Classification and Handling of Anonymity in Pervasive Middleware

Dr.G.Radhamani
School of IT and Science
Dr.GRD College of Science
Coimbatore, Tamilnadu, India

K.Vanitha
School of IT and Science
Dr.GRD College of Science
Coimbatore, Tamilnadu, India

D.Rajeswari
School of IT and Science
Dr. GRD College of Science
Coimbatore, Tamilnadu, India

ABSTRACT

Pervasive devices are deployed in the world anywhere at any time that makes an adaption to the changes in the dynamic environment based on the user mobility. New device enquiry, registration and adaption are major issues in such pervasive devices. As well as handling unacknowledged communication that causes anonymity is also a considerable issue. Above aspects referred as anonymity in pervasive computing. Middleware is an intermediate software application that connects pervasive devices. Therefore in this paper we define the presence of anonymity in pervasive environments using the said issues. We also analyze and compare few middleware applications for handling anonymity.

Keywords

Pervasive device; Anonymity; Middleware; Adaptation;

1. INTRODUCTION

The advances in wireless technologies growth and information processing services at everywhere created a new computing area called Pervasive computing. Pervasive computing is the idea that almost any type of device can be embedded with chips to connect the device to an infinite network of other devices to provide a convenient access to relevant information when and where it is needed. With respect to the development of applications for pervasive environments, a middleware can be used to bridge the gap between the application and the underlying operating systems and networks. One of the basic purposes of any middleware is to satisfy the application requirements and also it is required to support the challenges and issues in the computing devices on the pervasive environments. An environment consists of large number of embedded devices which coordinately works to perform some useful tasks to adapt to the users behavior. Since the devices are invisible and kept across the users computing environment, there may be possibility of unknown devices or unknown user could join in the existing computing environment and access the resources in it. This possibility makes the anonymous situation for the pervasive environments.

2. LITERATURE REVIEW

There are several middleware's are available for pervasive system. Some of the most representative are described in this section.[1]focused on Some important middleware categories and technologies suitable for today's mobile middleware and discussed about how the middleware is connected to pervasive environment.[2]Presented the concept and design of BASE, a flexible middleware supporting the additional requirements of pervasive computing environments. design implementation of BASE middleware shields applications from the multitude of different communication technologies and interoperability protocols by separating the communication model of the application and the interoperability protocols used.[3] discussed a privacy-aware solution for service discovery in heterogeneous networks, based on the MUSDAC platform and privacy issues that arise during service discovery and mechanisms to control disclosure of private information contained in service related data. [4] Discussed about the privacy threats identified in a pervasive environment and presented a set of principles for ensuring privacy. Number of privacy protection mechanisms for pervasive systems were examined with the focus on the level of anonymity offered to the end user. Also Stelios Dritsas et al concluded by presenting a set of essential actions one should take into account, in order to ensure users anonymity in a pervasive computing environment. [5] Provides an object-based framework for supporting context-sensitive applications. [6] Presented the Sensor Enablement for the Average Programmer (SEAP) middleware, which lowers the barrier to entry for programming pervasive computing applications with existing languages.

3. ANONYMITY IN PERVASIVE SYSTEM

Anonymity can be defined as a subject who is not identifiable or unacknowledged among the set of subject. In Pervasive computing it can be classified into two main categories (Fig1) and one sub category. It can be of any device or user which is unidentifiable by other devices among them. Information can also be anonymity in pervasive environments.

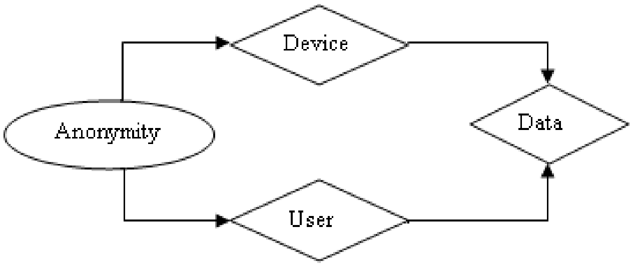


Fig 1: Classification of Anonymity

3.1 Device Anonymity

Ubiquitous and pervasive devices are becoming very popular and less expensive these days with which different devices like mobiles, smart phones and PDA etc has been dynamically adding into the computing environment to interact and coordinate easily with other existing devices in the pervasive environment .due to this dynamism any device entering into the existing pervasive environment may be a malicious one to abuse the service or resources available there or anonymously interact with all the devices in the computing environment to access the resources .Since the pervasive computing is exists everywhere and dynamism in addition and removal of devices makes the misidentification or anonymity in Pervasive computing.

3.2 User Anonymity

Each device in pervasive computing environment performs their role for a user to satisfy their requirements and makes adaptable to the changes in the physical world. Anonymous user is a user who is unknowingly enters into its computing world. An unacknowledged user may provide some malicious access to the other devices to destroy in it. Also the anonymous user can steal the personal information such as user personal data (trusted entity in the pervasive environment) device identity, location etc among other user in the pervasive systems.

3.3 Data Anonymity

The pervasive applications may need the user's static or dynamic data to provide access to the services. Static data may include age, group, education level, etc. Dynamic data refers to contextual information like location, activity state, etc. The static profile and contextual information are exchanged often among devices in the dynamic environment. The owner of the information desires control of what goes out of the system. On the other hand, the service provider requires a certain level of quality of the information disclosed in order to provide the service. The greater the amount of information disclosed, the higher the chance of re -identification of the user even if the identity of the user is not disclosed. The balance hinges between the user's desire to control the anonymity level of the information disclosed and the provider's requirement of meeting a quality level of that information.

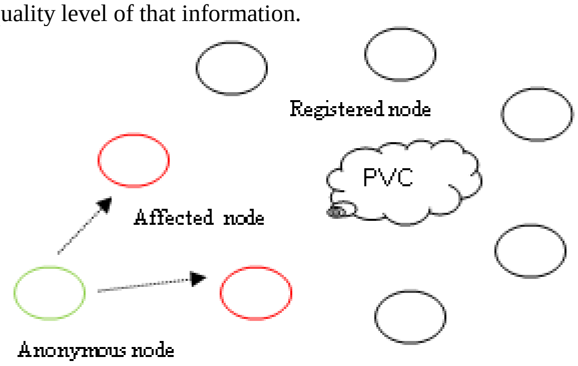


Fig 2: Representation of anonymity in Pervasive Environment

(Fig 2) describes the pictorial representation of anonymous device entering into the pervasive computing environment. Registered node (black) is a node which is authorized by a service provider and deployed in the computing world. An anonymous node (green) is a new node which is a non-identifiable or non registered node among other nodes on the Pervasive systems enters into it when using a service or resources from the trusted environment. Affected node (Red) is a node which is accessed by an anonymous node. When a new node enters into the computing environment it shares all the information of neighbor nodes to perform a tasks assigned to it. It has to be identified by existing nodes to coordinately work together. So these types of unknown nodes do not have a unique identity like other registered nodes in the Pervasive environment. Such a case of nodes may be a malicious one to abuse the nodes which is deployed by authorization.

4. MIDDLEWARE FOR PERVASIVE COMPUTING

Middleware is a software layer which sits below the applications and above the operating system to provide the common programming abstraction across all the distributed systems. Context-awareness, dynamism and heterogeneity are some of the properties that differentiate pervasive computing from traditional distributed systems. Most traditional distributed systems are unaware of context, are static, and are composed of homogeneous devices. Furthermore, different devices might be connected to different networks, with different latency and bandwidth. As a result, the middleware must provide mechanisms for handling disconnections, addressing fault tolerance, and adapting to a number of issues related to diversity including heterogeneous device resources.

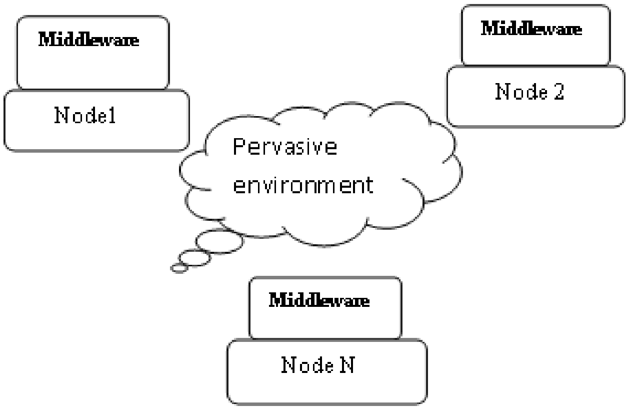
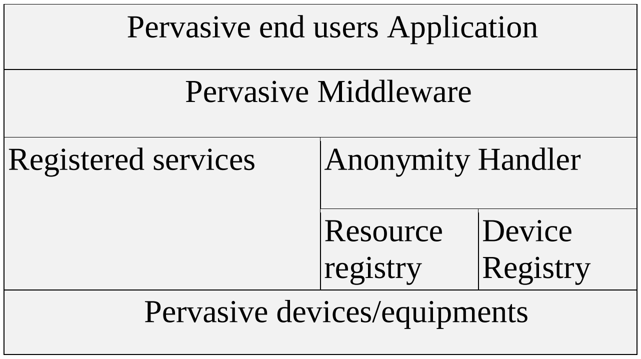


Fig 3: Middleware in Pervasive Environment

(Fig 3) Shows pervasive computing environments where the middleware lies between end user application and the underlying hardware. A node may be any device like user, laptop, Pc etc which is involved in the computing environment via middleware to communicate with the applications. Many of the existing middleware's addresses the pervasive computing environment issues such as mobility, disconnection, dynamic introduction, removal of devices and merging of the physical environment with the computational infrastructure etc to provide a convenient interaction among the application and the pervasive devices. Even though middleware's which provides service such as privacy they can only protect the personal details. Due to the anonymity issues in pervasive systems may get into the risks such as personal information healing, memory destruction, routing failure can be occurred. (Fig 4) is our proposed middleware architecture which tackles the anonymity issues in pervasive systems. Our middleware architecture for handling anonymity deals with three components such as anonymity handler, Resource registry and device registry. Device registry contains the details about trusted devices (managing by the provider) and also it updates the device which is new to its computing environment. Resource Registry holds the details about the resources available for the devices in its local region. Anonymity handler is used to validate the equipments in pervasive systems to identify whether it can be acknowledgeable one or unknown one. It allows the registry to update the record if it is a valid device otherwise the handler will reject the entered one. Service registry maintains the services which is allowed by the anonymity handler and updates the record.

Fig 4: Anonymity Handler for Pervasive Middleware

4.1 Existing Middleware's in Pervasive Computing



4.1.1 BASE middleware

Base middleware is mainly developed to support the requirements of heterogeneity devices in Pervasive computing. Base serves as a foundation for applications as well as component systems. [2] Key features of BASE are the uniform access to remote services and device-specific capabilities, the decoupling of the application communication model and the underlying interoperability protocols, and its dynamic extensibility supporting the range of devices from sensors to full-fledged computers. It provides the services as an API. Middleware delivers requests to either device services in the middleware or transport protocols. Since the devices and services are dynamic according to the network changes the anonymity level also increases. The information collected is shared by all the devices participated in the environment. The base middleware only addresses the heterogeneity portability and scalability issues in Pervasive computing.

4.1.2 SEAP middleware

SEAP middleware provides a middleware layer between the developer and the customized hardware, publishing sensor and actuation data using the standard HTTP protocol.[6] It is designed specifically to reduce the complexities in developing middleware for Pervasive computing using existing technologies. It is mainly developed to request and receive the data between application of the end user and the several objects in the environment using standard Http protocol. Since the SEAP component is placed in the devices participating in Pervasive computing it provides the high level of mobility. Since the information is shared through the web, the personal information about the user is only shared among the local space. So the quality of data collected is not so accurate due to the high level of anonymity. SEAP middleware allows people to interact with sensors and actuators without learning new languages or procedures.

4.1.3 MUSDAC middleware

The MUlti-protocol Service Discovery and ACcess (MUSDAC) [3] middleware a platform introduced to provide context-aware service discovery and access in pervasive environments by combining well-established patterns to address protocol interoperability (i.e., common representation) and multi-network discovery (i.e., ad hoc network composition).This middleware deals with the privacy issues in service discovery when the information is shared among the set of entities. Protocol used by MUSDAC component provides the anonymity for a sender entity to share information in a service discovery. MUSDAC uses the lighter weight version of the protocol to transmit the service among the entities it offers only a high level of anonymity since it uses the end to end encrypted service discovery.

Table 1: Comparison of Middleware

Middleware	Supported Features	Unsupported Features
BASE	Uniform access to heterogeneous device Interoperability Context-aware service	Resource discovery Device discovery Security Privacy
SEAP	Stable infrastructure Supports coordination among devices	Ad-hoc networks Device discovery Resource discovery
MUSDAC	Context-aware Device discovery Resource discovery Supports ad-hoc	Security Privacy
RCSM	Context-aware service Device discovery Privacy	Service discovery Fault tolerance

4.1.4 RCSM middleware

Reconfigurable context sensitive middleware is designed to facilitate applications that require context- awareness or spontaneous and ad hoc communication. RCSM provides an object based framework for supporting context-sensitive applications. [4] RCSM models context-sensitive application software as context-sensitive objects, which consist of two parts: a context-sensitive interface and a context independent implementation. The interface encapsulates the description of the application's context awareness, whereas the implementation remains context free. RCSM a context-sensitive object request broker (R-ORB) as the key mechanism for providing communication transparency for context-sensitive application software. R-ORB hides the intricacies of ad hoc networking. It also performs device and service discovery on the behalf of the context-sensitive objects. Since the context of the computing entities such as location, identity of the device, data and resources available for that device are shared among themselves. The level of anonymity is low in sharing of resource.

4.2 Comparison of Pervasive Middleware using Anonymity Factor

Handling anonymity is observed in the following (Table 2) middleware and an anonymity factor (AF) is devised in three levels such as low factor refers unawareness of anonymity, Medium factor refers partial handling, High factor refers satisfactory handling.

Table 2: Level of Anonymity in middleware's

Middleware	Comments	Level of device Anonymity	Level of service Anonymity
BASE	Level of anonymity offered is highly situational depended	Low	Low
SEAP	Anonymity level depend on each proposed implementation	Low	Low
MUSDAC	Level of anonymity is based on situation awareness	Low	Medium
RCSM	Anonymity level depends on uncontrolled environments	Medium	High

Satisfaction factor is measured as follows: (a) Consideration of pervasive computing characteristics by each proposed middleware (b) Privacy Mechanism supported by each middleware approach (c) Mechanism which supports to identify devices for trusted system (d) Scalability of proposed middleware.

5. CONCLUSION AND FUTURE WORK

We attempt to define anonymity for pervasive computing and the middleware level. We also classify the presence of anonymity pervasive systems to identify the unknown scenarios. A detailed study on few Middleware prescribed for a pervasive application is presented. The Key research issue is to handle unknown and unauthorized entities into the pervasive networks. Even for the first time enquiry or missing registrations are to be focused for future avenues. We are working to devise a mathematical model for handling anonymity using theories such as Game theory. Future work will be focused on the implementation of the anonymity handler and to evaluate based on the performance in an application level.

6. REFERENCES

[1] Vesa Kautto, "Middleware for Pervasive Computing", HUT, Telecommunications Software and Multimedia Laboratory, 2001.

[2] Christian Becker, Gregor Schiele, Holger Gubbels and Kurt Rotherme, "BASE -A Micro broker- Based Middleware for Pervasive Computing " University of Stuttgart Institute of Parallel and Distributed Systems (IPVS), Breitwiesenstr. 20-22, 70565 Stuttgart, Germany.

[3] Roberto Speicys Cardoso, Pierre-Guillaume Raverdy and Valeŕie Issarny, "A Privacy-Aware Service Discovery Middleware for Pervasive Environments", Inria Rocquencourt 78153 Le Chesnay, France.

[4] Stelios Dritsas, Dimitris Gritzalisa, Costas Lambrinoudakis, "Protecting privacy and anonymity in pervasive computing: trends and perspectives", Volume 23 Issue 3, August 2006.

[5] Stephen S. Yau, Fariaz Karim, YuWang, Bin Wang and Sandeep K.S. Gupta, "Reconfigurable Context Sensitive Middleware for Pervasive Computing", Arizona State Arizona State Volume 1 Issue 3, July 2002.

[6] Seth Holloway, Drew Stovall, Jorge Lara-Garduno and Christine Julien, "Opening Pervasive Computing to the Masses Using the SEAP Middleware", Mobile and Pervasive Computing Group, The University of Texas at Austin , March 2009.

[7] R. Jason Weiss and J. Philip Craiger, "Ubiquitous Computing", University of Nebraska–Omaha, Volume 39 Number 4 April 2002.

[8] Wassim Masri, Zoubir Mammeri, "Middleware for Wireless Sensor Networks: A Comparative Analysis," IFIP International Conference on Network and Parallel Computing Workshops, September 2007.

[9] Václav Slováček, Miroslav Macík and Martin Klíma "Development Framework for Pervasive Computing Applications", Czech Technical University in Prague, Faculty of Electrical Engineering, Department of Computer Graphics and Interaction, September 2009.

[10] Md.Atiqur Rahman, "Middleware for wireless sensor networks: Challenges and Approaches", April 2009.