A Fuzzy-Based Context-Aware Privacy Preserving Scheme for Mobile Computing Services

Eric Ke Wang and Yunming Ye

Abstract Currently privacy issues are challenging mobile computing services. We proposed a new privacy protection scheme for mobile computing services that is able to adapt to context. The accurate context is inferred by fuzzy reasoning. The experiment has been executed, and preliminary results have been encouraging.

Keywords Context aware · Privacy preserving · Fuzzy logic

1 Introduction

With the increasing availability of mobile devices, users enjoy more and more mobile services due to the users have much more mobilities than before. For example, when a user comes to a place, he can discover the nearest restaurant or ATM around his location, which is called location-based services. When users move, the environment changes. The original rules applied in one environment may not be applied in the other. For example, when users sit inside home, the environment is simple and gentle; the privacy protection can be home level. However, when users are in shopping mall, the environment becomes more complicated, the privacy protection should be high level.

Therefore, it is necessary to enforce different privacy policies according to context. That is called context-aware privacy preserving mobile computing that is different from the traditional privacy preserving computing. Traditionally, privacy

E. K. Wang (✉) · Y. Ye
Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen Key Laboratory of Internet Information Collaboration, HIT Campus, Shenzhen University Town, Shenzhen, China
e-mail: wk_hit@hitsz.edu.cn

Y. Ye
e-mail: yym@hitsz.edu.cn

S. Patnaik and X. Li (eds.), *Proceedings of International Conference on Soft Computing Techniques and Engineering Application*, Advances in Intelligent Systems and Computing 250, DOI: 10.1007/978-81-322-1695-7_14,

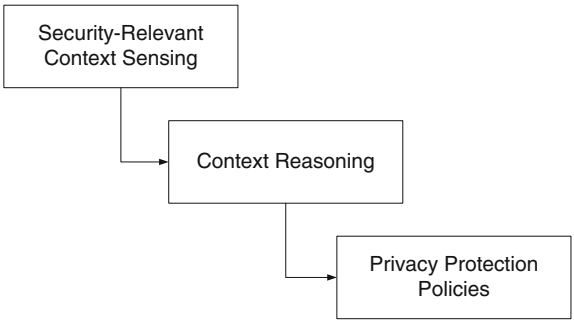


Fig. 1 Context-aware privacy protection model

protection can only solve problems in common scenario, or users should manually update protection policies. However, in context-aware privacy preserving mobile computing, the system enforces reasoning process based on the context data to get accurate inference result to adjust the privacy protection policies.

Context is the information that can determine an application's behavior or in which an application event occurs [1]. The context can be from various context information providers and can be in varying forms from temperature to user behavior. Besides, context-aware computing includes active context awareness that can automatically adapt the application to current context, and passive context awareness that can only give the users the context data to let users to decide the next step.

In our framework, we mainly tackle active context awareness and privacy-relevant context, which consists of the set of contextual attributes that can be used to characterize the situation of an entity, whose value affects the choice of the most appropriate controls (measures). Figure 1 shows the basic context-aware privacy protection model.

2 Privacy Challenge of Mobile Computing

Actually, many people besides friends and acquaintances are interested in the information that people post or exist on mobile services. Privacy issues for mobile computing are increasingly challenging users. Identity thieves, scam artists, debt collectors, stalkers, and corporations looking for a market advantage are using location-based applications to gather information about consumers [2]. Companies that provide mobile services are themselves collecting a variety of data about their users, both to personalize the services for the users and to sell to advertisers.

For example, more and more people are willing to use location-based services to make queries related to locations. As it is well known, the values at the core of services are precise and connecting [3]. However, the more precisely and convenient we become with these services, the more apt we are to share personal details about

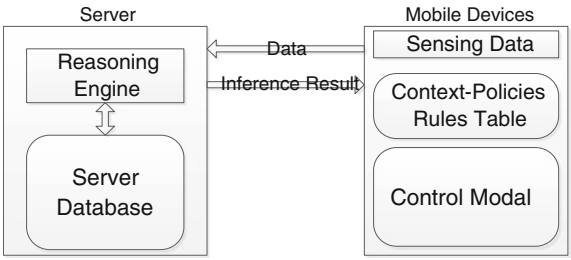


Fig. 2 System architecture

ourselves and let our guard down as we interact with others. Actually, the facts tell that the majority of mobile users post risky information online, without giving due diligence to privacy and security concerns. Unfortunately, the native core value of openness, connecting and sharing are the very aspects that allow cyber-criminals to use these services as a vector for various kinds of bad online behavior. At the same time, cyber-criminals are targeting location-based services with increasing amounts of malware and online scams, honing to this growing user base.

Although people's attitudes of privacy protection are various, most people hope that privacy protection measures would be smarter to let human be free while, currently most privacy protections for mobile services have to be handled and updated manually.

Therefore, how to protect privacy in an intelligent way is the main problem need to be solved for privacy issues of mobile computing. In order to tackle the above privacy problems, we proposed a privacy protection framework that can be able to adapt privacy protection polices by current environment. In this framework, the most important part is context awareness. However, because most data captured are ambiguous and scattered, a precise context is very hard to be achieved. In order to solve the problem, we adopt a reasoning engine based on fuzzy-logic theory [4] to solve the uncertain and vague data collected by mobile devices.

3 System Overview

3.1 Architecture

Considering the constraint resources of mobile devices, we design Server-Mobile Client model. The complicated computing tasks are done by server while, Mobile Client only solves the data collections and devices controls.

Figure 2 shows the architecture of the fuzzy-based context-aware privacy preserving scheme. It mainly includes two parties, one is the server, which solves the reasoning procedures, the other is the client side, which collects context data and execute controls. After users' mobile devices collect the sensing data, data will be sent to the server. Inside the server, there is a reasoning engine that receives the

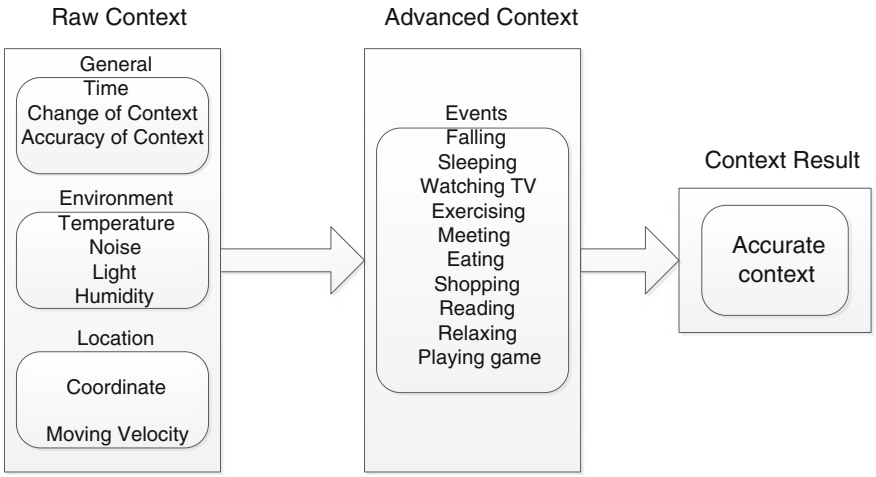


Fig. 3 Context modeling

data and executes reasoning process to send back the inference result to the users' mobile devices. After that, the mobile devices can read the inference result as context to adjust rules.

3.2 Context Modeling

Context is information that is used to describe the situation of an entity. However, how to model context is a crucial part in the system. Commonly, the context can be categorized into four types: system context (e.g., wireless network status, etc.), user context (e.g., location, emotion, medical history, etc.), physical environment context (e.g., lighting, temperature, weather, etc.), and time context (e.g., time) [5].

In our scheme, we model the context as raw model and advanced model. Raw context model includes some low-level data such as environment context data and user context data. Advanced context model includes high-level context such as behavior context. Figure 3 shows the context modeling.

All data collected by sensors in the mobile devices can be as the features of the context entities. In our scheme, we adopt <key, value> to map these features into individual fuzzy set in the fuzzy-logic framework. These fuzzy sets can be used for high-level context interpretation and further decision inference.

Some of the attributes associated with entities in our context model and their fuzzy sets are detailed as follows:

```
<Humidity, wet>
<Light, dark>
 <Location, Home>
```

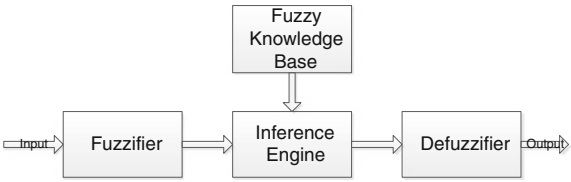


Fig. 4 Common fuzzy-logic system

```
<Temperature, cold>
```

3.3 Fuzzy-Reasoning Process

A fuzzy-logic system commonly includes three parts: fuzzy sets, rules and inference engine [6].

The procedure of fuzzy logic is as follows: (1) fuzzification: converts input data to a fuzzy set by fuzzy variables, membership functions, and fuzzy terms. (2) Inference: makes an inference based on a set of rules. (3) defuzzification: maps the fuzzy output to a crisp output. We adopt Takagi–Sugeno Fuzzy modeling [7] to realize the processes. The reason why we select T–S fuzzy modeling is because that it provides a simple method to achieve a definite conclusion based on imprecise, ambiguous data since it employs a linear combination of input variables as a rule-consequent variable.

The fuzzification process is as follows:

If x is the member of the physical context sets, $\tilde{A}$ and y are the members of the user behavior set $\tilde{B}$;

Then $z = f(x, y)$;

The physical context sets $\tilde{A}$ and the user behavior set $\tilde{B}$ are the fuzzy sets of modus ponens [8], and $z = f(x, y)$ is the precise function of modus tollens [9] and it is the fusion relation of the two contexts. $z = f(x, y)$ is the polynomial of the input variable x and y. Figure 5 is the fuzzification process.

Figure 6 shows the flow in the reasoning engine. The raw data collected by the mobile devices with context information is processed in build stage, which can produce context fuzzy sets. Then, fuzzy rules loaded from the inference rules database are utilized to generate advanced level context such as user activity. At last, the rule engine identifies the current state of the user based on the combination of advanced level context and gets the advanced result.

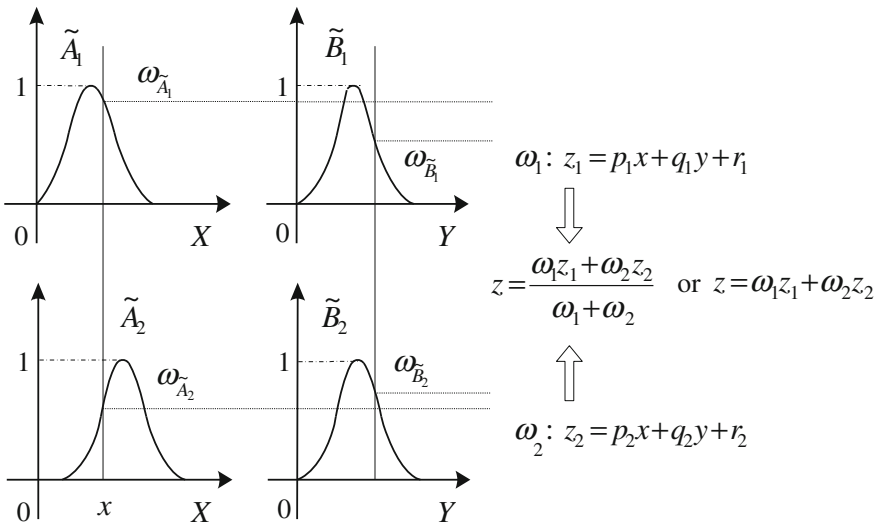
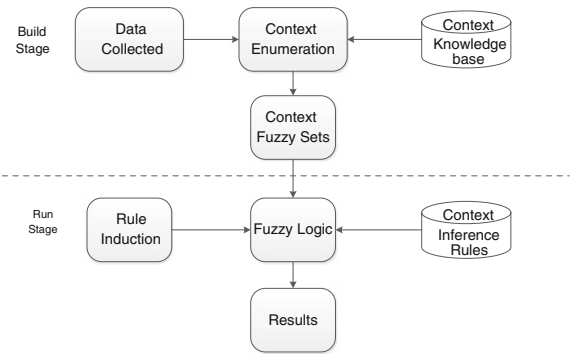


Fig. 5 Fuzzification process

Fig. 6 Reasoning engine



4 Evaluation

In order to evaluate the scheme, we implemented a prototype in a smart phone (Samsung Galaxy Note I with android 4.0) and made experiment. Figure 7 shows the implementation structure. The server runs a context acquire service that receives the GPS-location information, Wi-Fi connection information, and users'

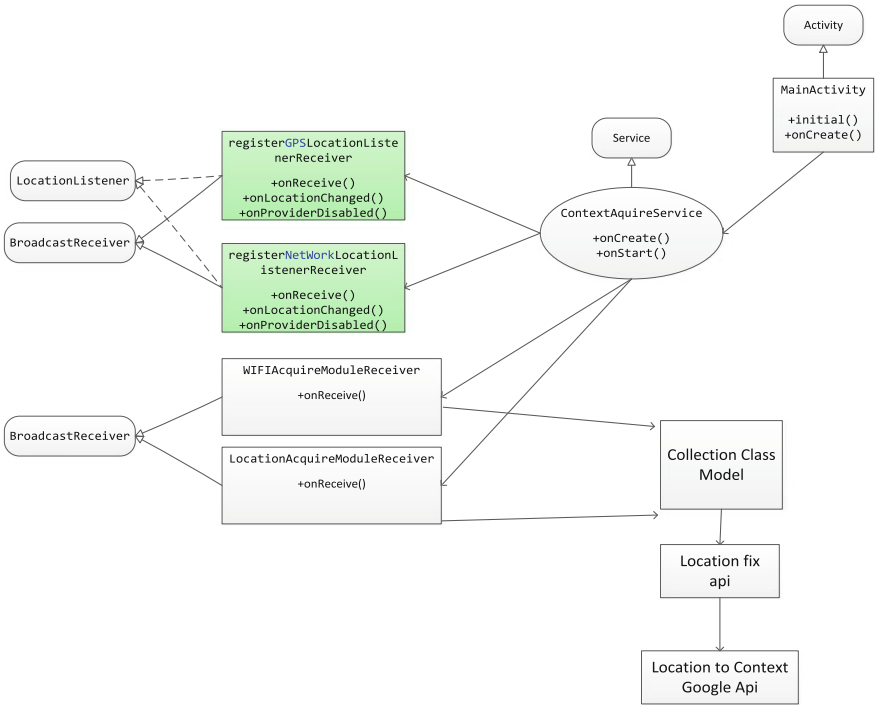


Fig. 7 Implementation modules

activities. The class (register GPS-location listener receiver) is used to get the GPS information, the class (Wi-Fi acquire module receiver) functions to get the Wi-Fi hotspot location information.

5 Conclusions

We proposed a fuzzy-based context-aware privacy preserving scheme that can dynamically adapt privacy protection policies to current scenario. It enforces fuzzy-reasoning based on context data to achieve accurate scenario. We built an experiment prototype to evaluate the scheme. The results show to be encouraging.

Acknowledgments This research was supported by National Natural Science Foundation of China (No. 61100192), Research Fund for the Doctoral Program of Higher Education of China (No. 20112302120074), and was partially supported by Shenzhen Strategic Emerging Industry

Development Foundation (No. JCYJ20120613151032592 and ZDSY20120613125016389), National Key Technology R&D Program of MOST China under grant no. 2012BAK17B08, and National Commonweal Technology R&D Program of AQSIQ China under grant no. 201310087. The authors thank the reviewers for their comments.

References

1. Dey, A.K.: Understanding and using context. Pers. Ubiquit. Comput **5**(1), 4–7 (2001)
2. Gong, Z., Sun, G.-Z., Xie, X.: Protecting privacy in location-based services using K-anonymity without cloaked region. In: 11th International Conference on Mobile Data Management, pp. 366–371, New York (2010)
3. Zhang, W., Cui, X., Li, D., Yuan, D., Wang, M.: 2010 18th International Conference on Geoinformatics. Beijing, China (2010)
4. Zadeh, L.A.: Fuzzy logic. Computer **21**(4), 83–93 (1988)
5. Hong, J., Suh, E., Kim, S.J.: Context-aware systems: a literature review and classification. Expert Syst. Appl. **36**(4), 8509–8522 (2009)
6. Liang, Q., Mendel, M.: Interval type-2 fuzzy logic systems: theory and design. IEEE Trans. Fuzzy Syst. **8**(5), 535–550 (2000)
7. Su, X., Wu, L., Shi, P., Song, Y.D.: H∞ model reduction of Takagi–Sugeno fuzzy stochastic systems. IEEE Trans. Syst. Man Cybern. B Cybern. **42**, 1574–1585 (2012)
8. Zardini, E.: Naive modus ponens. J. Philos. Logic **42**(4), 575–593 (2013)
9. Yalcin, S.: A counterexample to modus tollens. J. Philos. Logic **41**(6), 1001–1024 (2012)