International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-2, February 2016
ISSN: 2395-3470
www.ijseas.com

A Safe Period Approach for Supporting Location-Based Digital Right Management Services

Seokyoon Kim[1], Youngmo Kim[2], Ung Mo Kim[3]
[1] Soongsil University, Seoul, Republic of Korea
[2] Soongsil University, Seoul, Republic of Korea
[3] Sungkyunkwan University, Suwon, Republic of Korea

Abstract

This paper addresses the problem of the efficient supports of location-based digital right management (DRM) services. In location-based DRM services, users can access the documents only in the designated areas, but cannot access in the other areas. Existing methods for supporting location-based DRM services assume that users periodically send their current locations to the distributor and the distributor periodically checks whether the users are within their designated areas or not. However, such an assumption degrades the system performance, because the communication cost is huge and the workload at the distributor is increased. In this paper, we propose a safe period method to overcome this limitation. Through simulations, we verify the efficiency of the proposed method.

Keywords: *Digital Right Management, Location-Based Services, Location-Based DRM Services, Access Control.*

1. Intoroduction

With the technological advances in wireless networks and the wide deployment of mobile devices, equipped with location sensing technology (e.g., smart phones and pads), *location-based services* (*LBSs*) have attracted much attention as one of the most promising applications in recent years. LBSs are services, which provide the location-specific information to a user by taking the user's current location as an input.

A number of real-world LBS applications demand the access control model for constraining the access to documents to particular locations. For example, a doctor (in a hospital) should not access a patient's medical record unless he or she is in a designated area within the hospital. Similarly, a company may want to make sure that secret materials can be accessed only within the company's ground.

Location-based Digital Right Management (DRM) services allow information owners to control the use and dissemination of encrypted documents via a machine-readable *license*, which contains location constraints used to allow access to sensitive documents to only a designated area. Users can access the documents in the designated area, but cannot access in the other areas.

To support location-based DRM services, two aspects should be considered. The first aspect is that users' locations are very sensitive information that can pose privacy threats to the users, because adversaries could infer the personal sensitive information (e.g., medical conditions) by combining users' locations with publicly available information (e.g., telephone directories). The way to achieve users' privacy protection is beyond the scope of this paper and is presented in [1].

The second aspect is that the distributor, which is responsible for transmitting documents to the users, should keep track of the users' locations due to their *mobility*. For example, the user shown in Fig. 1 can access the sensitive documents at time t_0. A little later, at time t_1, let us assume that the user moves out of the designated area as shown in Fig. 1. Then, the user cannot access the sensitive documents.

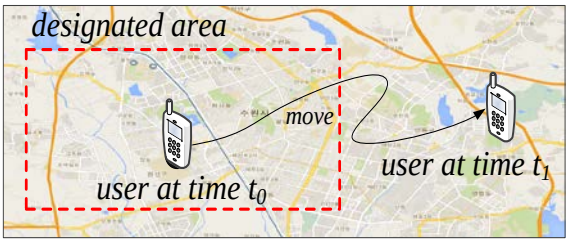

Fig. 1 An example of user's mobility.

The majority of existing methods for supporting location-based DRM services assume that users periodically send their current locations to the distributor through wireless connections, and the

distributor continuously checks whether the users are within their designated areas or not. However, excessive location-updates from users can not only cause significant energy waste of the battery powered handheld devices (carried by the users), but also significantly degrade the overall system performance due to the overwhelming workload at the distributor as well as the severe communication bottleneck.

In this paper, we propose a method for supporting location-based DRM services in an efficient manner in terms of the workload at the distributor and communication cost. The proposed method uses the concept of *safe period*, which utilizes the available computational resources of users' handheld devices (e.g., smart phones and pads) to improve the overall system performance. Through simulations, we verify the efficiency of the proposed method.

The remainder of this paper is organized as follows. In Section 2, background and related work are presented, and in Section 3, details of the proposed method are presented. In Section 4, the results of performance evaluation are presented. Finally, Section 5 concludes the paper.

2. Background and Related Work

2.1 Location-Based Services (LBSs)

Many current LBSs usually rely on the functionality of monitoring users' current locations (e.g., traffic condition monitoring and floating population monitoring) [2, 3]. Given a geographic region of interest, the majority of existing methods for location monitoring queries assume that the users periodically send location-updates to the server via wireless connections and the server continuously monitors the population in the region. However, excessive location-updates from users may not only cause significant energy waste of the battery powered handheld devices (carried by the users), but also significantly degrade the overall system performance.

The safe region method, which helps users reduce the frequency of sending their location-updates, was introduced in [4]. A safe region, assigned to each user *u*, is the region that (i) contains *u* and (ii) guarantees that the current result of all the monitoring queries will remain valid if *u* moves only within this region. Therefore, *u* can move freely without sending his or her location-update to the server as long as he or she does not exit the safe region. On the other hand, the space partitioning query index method and the query region-tree method whose primary goal is to reduce the communication cost and the server workload by leveraging the available (memory and computational) capabilities of users, was introduced in [2,3], respectively.

2.2 Location-Based DRM services

Location-based DRM services allow information owners to control the use and dissemination of encrypted documents via a machine-readable license, which contains location constraints used to allow access to sensitive documents to only a designated area. Traditional location-based DRM services do not consider users' mobility. As a result, there is no option to control the users' mobility.

The naïve way to solve this problem is to let the users periodically send their current locations to the distributor through wireless connections, and the distributor continuously checks whether the users are within their designated areas or not. However, when the distributor involves a large number of users, the overall system performance may deteriorate drastically due to a severe communication bottleneck and overwhelming workload at the distributor. In the next section, in order to remedy this problem, we propose the concept of safe period that provides location-based DRM services in an efficient way in terms of the communication cost and the workload at the distributor.

3. The Proposed Method

3.1 The Overview of the Proposed System

Fig. 2 shows a high-level overview of the system model. Similar to the system model presented in the previous work [5, 6], the system model we consider consists of four major components: license issuer, document provider, distributor, and users.

- License issuer: The license issuer is responsible for handling financial transactions and issuing licenses.

- Document provider: The document provider is a digital rights owner.
- Distributor: The distributor is responsible for disseminating the provided documents. In addition, the distributor computes a safe period for each user and provides the safe period to the user.
- Users: Each user is identified by his or her unique identifier and carries a handheld device that has a capability of sensing its current location (e.g., equipped with a GPS receiver) and some available (memory and computational) capability. The user is assigned a safe period and only when the safe period expires, he or she send location-update to the distributor to receive a new safe period.

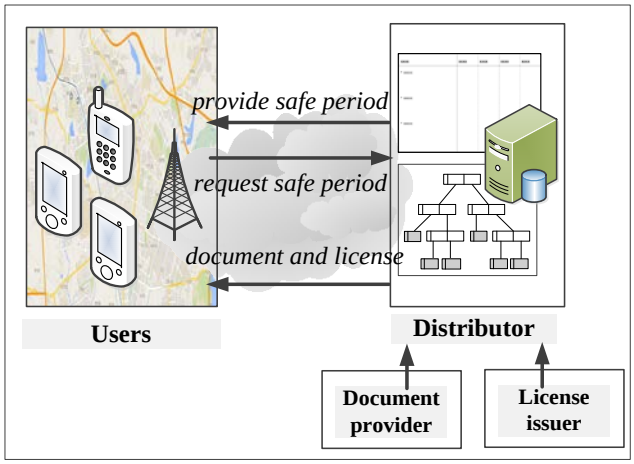

Fig. 2 System overview.

3.2 Safe Period Computation

A safe period assigned to each user is defined as a period of time in which the user can move freely without sending his or her current location. According to two cases of user's location, the safe period assigned to the user is computed as follows:

- **Case 1**: If the user u is within a certain designated area r, the safe period SP assigned to u is $mindist(u, r) / vmax(u)$, where $mindist(u, r)$ is the minimum distance from u to r (See Case 1 in Fig. 3) and $vmax(u)$ is the predefined maximum velocity of u.
- **Case 2**: If the user u is not within any of the set of designated areas $R = \{ r_1, r_2, \ldots, r_{|R|} \}$, the safe period SP assigned to u is $MIN(mindist(u, r_{i\ (1 \le i \le |R|)})) / vmax(u)$. Here, $MIN(mindist(u, r_{i\ (1 \le i \le |R|)}))$ is the minimum distance among $mindist(u, r_1)$, $mindist(u, r_2)$, …, and $mindist(u, r_{|R|})$ (See Case 2 in Fig 3).

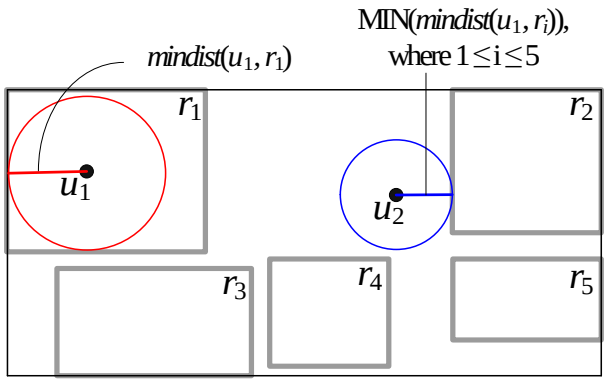

Fig. 3 Exmaples of *mindist* computation.

4. Performance Evaluation

In this section, we evaluate and compare the performance of the proposed safe period method, denoted by SP with the naïve method [5, 6] in terms of the workload at the distributor and communication cost. The workload at the distributor was measured in terms of the CPU-time. On the other hand, the communication cost was measured by the total number of messages transmitted between the distributor and users. The simulations were conducted on Intel Xeon E5-2620 6-core Processor with 8GB RAM running on the Linux system.

4.1 Simulation Setup

Our simulations were based on a set of rectangular designated areas, with the workspace fixed at 50 km × 50 km square. The designated areas on the workspace are uniformly distributed. The movements of users that we generated follow the random waypoint model, which is one of the most widely used mobility models: each user chooses a random point of destination on the workspace and moves to the destination at a constant speed distributed uniformly from 0 to maximum speed, which we set to 50 km/h. Upon reaching the destination, he or she

remains stationary for a certain period of time. When this period expires, the user chooses a new destination and repeats the same process during the simulation time steps.

4.2 Simulation Results

In the first simulation, we varied the number of designated areas from 1000 to 10,000 and studied the effect of the number of designated areas on the workload at the distributor and communication cost. The purpose of this simulation was to show the scalability of SP with regard to the number of number of designated areas. Fig. 4 shows the effect of the number of designated areas on the CPU-time the distributor takes for the location-based DRM service. As shown in the figure performs much better than the naïve method.

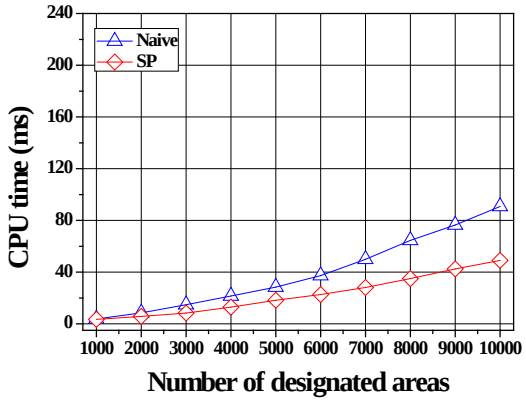

Fig. 4 CPU-time vs. # of designated areas.

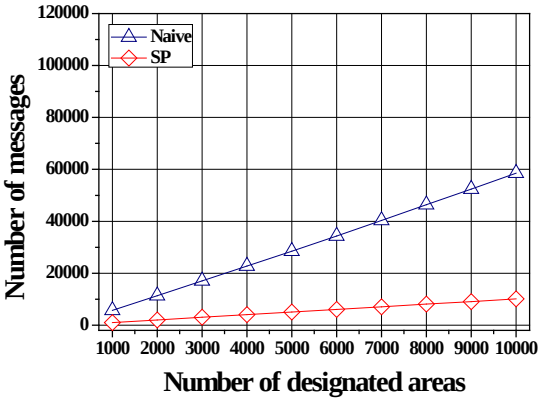

Fig. 5 # of messages vs. # of designated areas.

Fig. 5 shows the effect of the number of designated areas on the total number of messages communicated between the distributor and users. As the number of designated area increases, the performances of both methods degrade. However, SP outperform the naïve method.

In the next simulation, we increased the number of users from 10,000 to 100,000 to study how the number of users affects the performances of SP and the naïve method. As shown in Fig. 6 and Fig. 7, as the number of users increases, the overhead of both methods increases in terms of the CPU-time and the total number of messages. However, in all cases, SP outperforms the naïve method.

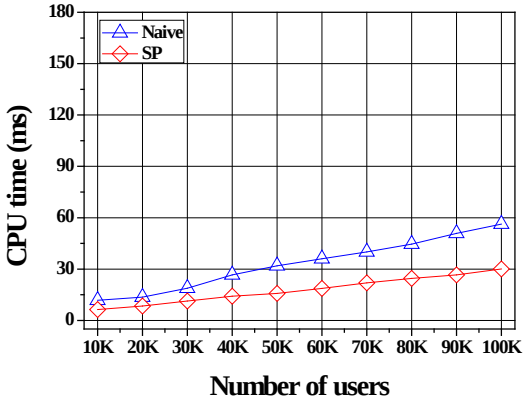

Fig. 6 CPU-time vs. # of users.

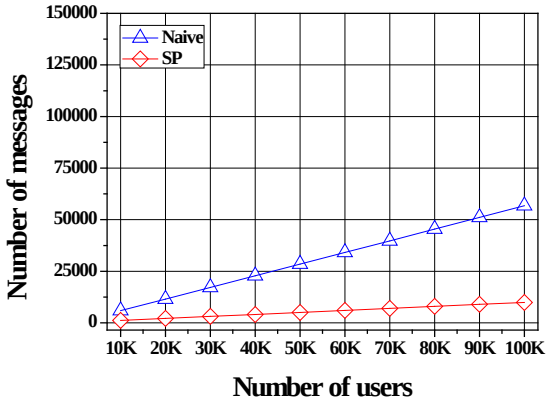

Fig. 7 # of messages vs. # of users.

5. Conclusions

In this paper, we addressed the problem of the efficient and scalable supports of location-based DRM services. Given a set of geographically distributed users, the primary goal of our study is to allow the users to access the sensitive documents to only designated areas in an efficient way. To achieve this, we proposed the safe period method. A safe period assigned to each user is defined as a period of time in which the user can move freely without sending his or her current location. We carried out a set of simulations and demonstrated that the proposed method outperform the existing naïve method. .

Acknowledgments

This research project was supported by Ministry of Culture, Sports and Tourism (MCST) and from Korea Copyright Commission in 2015.

References

[1] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection ", Computer, Vol. 36, 2003, pp. 135-137.

[2] H. Jung, Y.S. Kim, and Y.D. Chung, "SPQI: An Efficient Index for Continuous Range Queries in Mobile Environments", Journal of Information Science and Engineering, Vol. 29, 2013, pp. 557-578.

[3] H. Jung, Y.S. Kim, and Y.D. Chung, "An efficient and scalable method for evaluation of continuous range queries ", Information Sciences, Vol. 274, 2014, pp. 156-176.

[4] M.A. Cheema, L. Brankovic, X. Lin, W. Zhang, and W. Wang, "Continuous monitoring of distance-based range queries", IEEE Trans. Knowl. Data Eng., Vol. 23, 2011, pp. 1182-1199.

[5] A. Muhlbauer, R. Safavi-Naini, F. Salim, N. Sheppard, and M. Surminen, "Location constraints in digital rights management", Computer Communication, Vol. 31, 2008, pp. 1173–1180.

[6] J.S. Erickson, "Fair use, DRM, and trusted computing", Commun. ACM, Vol. 46, 2003, pp. 34–39.

Seokyoon Kim Seokyoon Kim received his Ph.D degree in Electric and Computer Engineering from University of Texas at Austin in 1993. He is currently professor in Soongsil University and dean of school of computer science & engineering. His research interests are embedded system, VLSI, SoC, design automation.

Youngmo Kim Youngmo Kim received his Ph.D. degree in Computer Engineering from Daejeon University, Daejeon, Korea in 2011. He is currently adjunct professor in Soongsil University and senior researcher Korea Copyright Commission. He is also working on several standardization activities and national project. His research interests are security, computer forensics, DRM (Digital Right Management), and fingerprint.

Ung Mo Kim Ung Mo Kim received his Ph.D degree in Computer Science from Northwestern University in 1990. He is currently professor at Dept. of Computer Engineering, Sungkyunkwan University. His research interests are databases, data mining, big data processing.