www.ijrream.in Impact Factor: 2.9463

INTERNATIONAL JOURNAL OF RESEARCH REVIEW IN ENGINEERING AND MANAGEMENT (IJRREM)

Trust your Data - Enterprise Data Protection System using GeoFence Technology

M. Arunraj, K. Keerthiraj, T. Rubanraj, S. Sakthivel

Department of Information Technology

Paavai Engineering College, Namakkal

ABSTRACT:

A geo-fence is a virtual border for a true geographic zone. A geo-fence could be powerfully created as in a range around a point area, or a geofence can be a predefined defined of limits, and it includes an area mindful gadget of an area based administration (LBS) client entering or leaving a geofence. A system can be implemented for Enterprises against unauthorized access on secret files. It provides an authentication based on three types, such as Media Access Control (MAC), Internet Protocol (IP) and Geo-Fence Area or boundaries. A Malicious users are copy the secret files around the system within the geo-fence boundary, At the same time our system is automatically trigger and it generate the harmful virus for scrap the copied file. The users are insert the secondary device (Pen drive) into the outside of the geo-fence area, the virus file first check the GPS location , MAC Address and IP address of the current system, if it is mismatch the virus file wipe out the secret files and it also wipe out the whole system of malicious user's. Our system is also block the mail preview of the secret files.

Keywords: Media access control, GPS, LBS, Internet Protocol

1. INTRODUCTION

Geographical information is used in many fields such as ubiquitous computing, physical security, social networking services, and location aware marketing and advertisement, such as check-in and coupon delivery services .These geo-location aware technologies are triggered by a user’s presence in a given geographical area, which is called geofencing. The term geo-fence refers to a virtually fenced area. The services mentioned are provided in the geo-fenced area via wireless communications, thus wireless traffic is generated in the area. This context enables the development of new access control strategies in wireless communications. Previous works have investigated ways to couple geofencing with wireless access control. These can be roughly categorized into two approaches: power control and

localization based scheme. Proposed a power control based geo- fencing system which creates an area where the received signal strength (RSS) is high by using transmission power control and beam forming of directional antennas so that users can only access the network in the desired area. However, this approach requires beam-controllable APs and it is difficult to create an area with specific shapes, which needs cooperative control of multiple APs.

Localization based geo-fencing is a straight- forward approach that estimates the locations of users and conducts operations when a user enters/leaves a geographical area GPS-based localization is a promising way to estimate the locations of users in an outdoor environment while accurate indoor localization with low energy consumption and low operation cost remains a challenge. Indoor localization has been investigated extensively; many works use received signal information to estimate the user's locations. One promising technique uses the RSS of wireless signals However, the average estimation errors of RSS-based methods are larger than 1m even in simple environments which can increase fault/miss detection of user presence. We propose camera- based geo-fencing for WLANs, where the locations of STAs are estimated and tracked accurately using camera images.

In the proposed method, the setting of the geo-fenced area can be visualized on camera images, which is useful for operators because it allows intuitive operation to draw the geo-fenced area on the camera image. This system also realizes precise control of geo- fencing due to highly accurate localization by camera images. As an example of geo-location based wireless control, we also propose a WLAN activation control which allows STAs to pre-activate WLAN interface and associates with WLAN APs when STAs enter an area where the users tend to use their STA so that the power consumption is reduced by extending sleep time of WLAN chip set without increasing time to obtain contents. The contributions of this paper are summarized as i) a system design for a camera- based geo-fencing in WLANs, ii) a proof of- concept experiment using off-the-shelf devices to show the feasibility proposed system.

2. EXISTING SYSTEM

Spatial Temporal Provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed

setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non- transferability of the location proofs and protects users' privacy. A semi trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light- weight entropy-based trust evaluation approach.

- System Model
- Flow of Geo-Fencing for Wireless LANs with Camera
- Geo-Fencing Area Setting and Visualization
- Geo-Fencing Based Association Control

System Module:

Fig shows a model of the system. We consider an indoor environment, such as a museum, where multiple APs providing WLAN and Bluetooth are deployed. Cameras are placed in each room and corridor mainly for surveillance, but the images obtained by the cameras can also be used for geo-fencing. We assume that users in the area opt in the surveillance by our system and there are no blind spots for the wireless access networks or cameras. The equipment is connected to a control server which manages the geo-fencing control via wired networks such as Ethernet. Users walk around the environment with STAs rented by the museum, which display information about the exhibits. When the users operate the STAs to get information, the STAs send requests to a control server, the control server responds with the requested information. The STAs are connected to APs via WLAN, Bluetooth, or BLE, and these wireless networks the STAs connect to can be selected by the control server. The users are constantly captured by cameras and the pictures are sent to the control server to detect the users' positions.

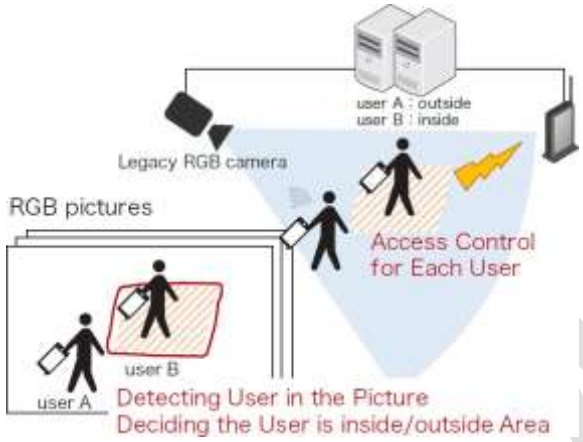


Fig.1 Existing System Module

Flow of Geo-Fencing for Wireless LANs with Camera:

Fig shows a flow chart of the proposed system. The control server first sets the geo-fenced area. At the same time, cameras capture images of the view, APs obtain STAs information such as MAC address and acceleration data which is required to STA localization, and they send the data to the control server. Next, the control server detects and localizes STAs in the camera images. Considering information such as the geo-fenced area and the location of the STA, wireless control strategy is decided and a control message is sent to the APs to execute the wireless control. This control scheme is done repeatedly, every time the condition of the user or the area changes.

Geo-Fencing Area Setting and Visualization:

Our existing method provides an easier way of defining the geo-fenced area using the camera images. Assuming that the geo-fenced area is included in images, the administrator can easily recognize the size and shape of the geo-fenced area, even if its shape is complicated. Thus, the system administrator can set the geo-fenced area directly on the camera image using graphical interfaces that provides intuitive operations, such as drawing or erasing lines. Moreover, the system monitors the area and can track dynamics of the area, e.g. mobility of pedestrians. Therefore, the proposed system has capability to adaptive control responding changes in the user distribution.

STA Detection and Localization

Since it is difficult to detect STAs in camera images, the proposed scheme first localize humans in the field of view (FoV) of camera and then match STAs to the humans. Such a

localization approach has been studied in [10]. User detection and tracking are well investigated on the computer vision. For example, proposed a lightweight object detection method which enables 3Dimensional positioning with single camera with an estimation error of less than 50 cm. A method to track multiple persons with multiple cameras was proposed in. We exploit such existing methods to detect and localize humans. Matching between STAs and users in the FoV of camera has also been studied in. These works leverage the movement of STAs and users for matching. The movement of STAs is captured by using acceleration data from STAs, and that of user is captured from camera images. The proposed system employs these matching schemes.

3. PROPOSED SYSTEM

This project will provide an introduction to Geo Server own authentication and authorization subsystems. such as from basic/digest authentication and CAS support, check through the various identity providers, such as Geo fence boundaries, MAC (Media Access Control), IP (Internet Protocol), as well as providing examples of custom authentication plug-in for Geo Server, integrating it in a home grown security architecture. This system create the victim file for wipe out the data, when the data is attempted to open outside of the geo fence. Modules Description:

1. Geo - Fencing Boundary Fixing
2. Attacker Module
3. Malware Injection
4. Wipe out System
5. Performance Evaluation

Geo - Fencing Boundary Fixing

Geo-fencing allow an administrator to set up triggers so when a device enters (or exits) the boundaries defined by the administrator, an alert is issued. Many geo-fencing applications incorporate Google Earth, allowing administrators to define boundaries on top of a satellite view of a specific geographical area. Like that we do in our project to implement the in our enterprise small startup company its very help full one.

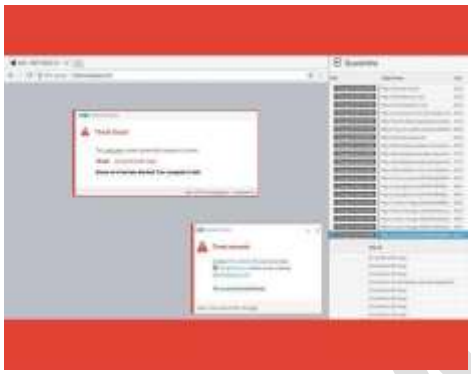


Fig. 2 Geo fencing Boundary Fixing

Attacker Module:

In Adversary module, the user can use the data on outside of the geo-fence area. It contains two types of attacker involves the system one is the attacker can be used an external device for copy the data in defense area, and another one is sending the data to the email. It is an one type of cyber-attacks, because an attempt to hackers to damage or destroy whole computer networks or system. We can use both two method of attacker module is like that external device attacker module like pen drive or any other physical device to get copy the data and use or insert the other systems. And the method we files share through the online like e mail to send the data. It's also a one of types of attacker modules.

Fig.3 Attacker

Malware Injection:

In this module is used to automatically inject the malware file to the original file. The victim file, is perform the main role of our system, it is an .exe file format. Auto exe is automatically

copy the external devices. Suppose the user attach file to the mail, it automatically convert the file to .zip format for preview blocking. Malware injection create the application.

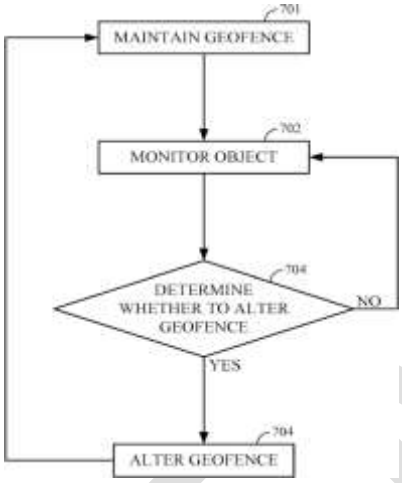


Fig. 4 Malware Injection

Wipe out System

In the wipe out module, is wipeout the files and destroy the system when an exe find the system is adversary system. Auto exe is first check the adversary system having internet connection, if it is having a internet connection, victim file reading the current system MAC , IP and Geo Location and compare with the server it doesn't match to send the adversary system information to the mail and wipeout the files and system. Otherwise it does not care of anything scrap the system and data.

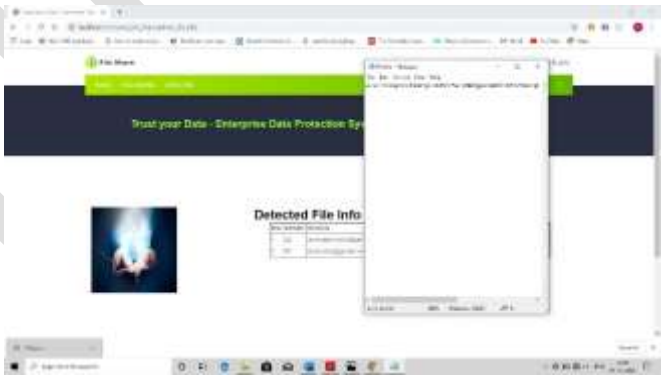
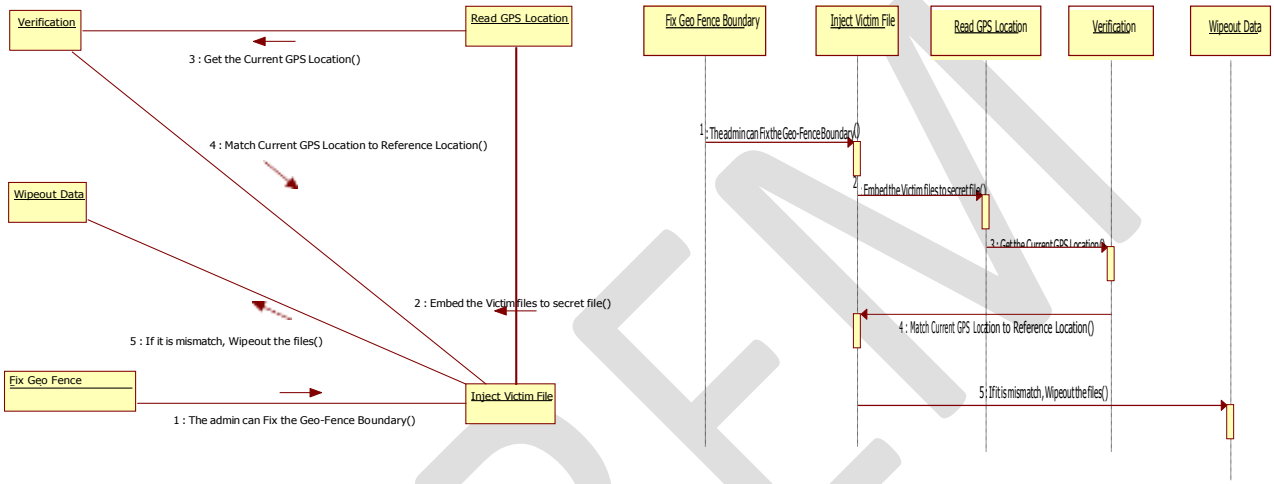


Fig. 5 Victim File Injection

Process of Proposed System

A geo- fencing system is usually used for location based service. First time we will used the Data security in defense. This system provides the more security for an essential data. A process of performed system to the step by step process each and every process make more security process.



4. CONCLUSION

In this paper, we introduced a novel privacy-aware framework for provide data security, which enables the participation of workers without compromising their location privacy. We identified geo fencing as a needed step to ensure that privacy is protected prior to workers consenting to a task. We provided heuristics and optimizations for determining effective geo fencing regions that achieve high task assignment rate with low overhead. It also generate the victim files, it automatically checks the geo - fencing boundary values and wipeout the system and files when geo-fencing and MAC Address is mismatch.

References:

1. Information Provision Improvement with a geo- fencing Event-Based System.
2. Enhanced Functionality for Tracing Places, Weather Forecasting and Geo-fencing using Android.
3. Ravindra B. Sathe and A.S. Bhide "GPS-based soldier tracking and health monitoring system" World Journal of Science and Technology 2012, 2(4):97-99 ISSN: 2231 – 2587

4. VChadil, N.; Russameesawang, A.; Keeratiwintakorn, P., "Real-time tracking management system using GPS, GPRS and Google earth," Electrical Engineering / Electronics, Computer, Telecommunications and Information Technology, 2008. ECTI-CON 2008. 5th International Conference, pp.393,396, 14-17 May 2008.
5. A Noulas, S. Scellato, C. Mascolo, and M. Pontil, "An empirical study of geographic user activity patterns in foursquare." in Proc. ICwSM, Barcelona, July 17–21 2011.
6. D. Namiot and M. Sneps-Sneppe, "Proximity as a service," in Proc. BCFIC, Vilnius, Lithuania, Apr. 25–27 2012, pp. 199–205.
7. A Sheth, S. Seshan, and D. Wetherall, "Geo- fencing: Confining wi-fi coverage to physical boundaries," in Proc. ICPC, Berlin, May 11–14 2009, pp. 274–290.
8. J. J. Roese, R. W. Graham, D. Frattura, and D. Harrington, "Locationbased access control in a data network," Mar. 3 2015, US Patent 8,972,589.
9. H. Rahimi, A. N. Zincir-Heywood, and B. Gadher, "Indoor geo-fencing and access control for wireless networks," in Proc. IEEE CICS, Singapore, Apr. 16-19 2013.
10. E. Cassano, F. Florio, F. De Rango, and S. Marano, "A performance comparison between roc-rssi and trilateration localization techniques for wpan sensor networks in a real outdoor testbed." in Proc. WTS 2009, Prague, Czech Republic, Apr. 22–24 2009.
11. F. Reclus and K. Drouard, "Geofencing for fleet & freight management," in Proc. IEEE ITST, Lille, France, Oct. 20-22 2009, pp. 353–356.
12. F. Zafari and I. Papapanagiotou, "Enhancing ibeacon based microlocation with particle filtering," in Proc. IEEE GLOBECOM, San Diego, CA, USA, Dec. 6–10 2015, pp. 1–7.
13. M. S. Aman, H. Jiang, C. Quint, K. Yelamarthi, and A. Abdelgawad, "Reliability evaluation of ibeacon for micro- localization," in Proc. IEEE UEMCON, New York, USA, Oct. 20–22 2016, pp. 1–5.