Smart Card Based Access Control System using RFID Via Location Sensing

C. Sarumathi
PG scholar
Oxford engineering college
Trichy

M. Vijayakumar. M.Tech.
Assistant professor
Oxford engineering college
Trichy

***Abstract*-Increasing number of user portable computing devices is embedded in vehicles, containers in order to provide a wide range of services to users. The location information or location related information can serve as a legitimate access context .The radio frequency identification system makes uses of tags and readers to communicate. Toll cards usually only communicate with toll readers in certain fixed locations at toll booths or when the car travels at a certain speed. Hence, location or location defined information can be used as a good means to establish a legitimate usage context. It is found that location information can be used to design selective unlocking mechanism so that tags can selectively respond to reader interrogations and also location information can be used as a basis for secure amount transaction.**

1. INTRODUCTION

Wireless communication is the transmission of information between two or more points that are not connected by an electrical conductor, through air. The most common wireless technology is the use of radio technology. Using a short distance radio waves communication, a few kilometers for television or as far as thousand kilometers for deep sea radio communication. It comprises of various types of fixed, mobile, and portable applications. Examples include wireless computer mice, keyboard, headset etc.

1.1NEAR FIELD COMMUNICATION

Near field communication is a form of short range wireless communication where the antenna used is much smaller than the wavelength of the carrier signal (thus preventing a standing wave from developing within the antenna). In the near-field (approximately one quarter of a wavelength) the antenna can produce either an electric field, or magnetic field, but not both fields. Thus NFC used

communicates by a modulated electric field, or a modulated magnetic field, but not by both radio waves. For example, a small loop antenna produces a magnetic field that can then be used up by another small loop antenna, if it is in the near field range for communication.

1.2. RFID TECHNOLOGY

Radio-frequency identification (RFID) is the wireless technology that uses electromagnetic fields to transfer data, for the process of automatically identifying and tracking tags attached to objects. Electronically stored data are contained in the tags. Some of these tags are powered by electromagnetic induction from magnetic fields that are produced near the reader. Some types of tags collect energy by interrogating the radio waves and acts as a passive transponder. The next types of the tag have a local power source such as a battery power and may operate at hundreds of meters from the reader. Some tags contains a barcode, these tag does not necessarily need to be within line of sight of the reader, and may be embedded in the objects to be tracked. Radio frequency identification (RFID) is used as one method for Automatic Identification and Data Capture (AIDC).RFID tags are used in many industries. In order to track the progress of an automobile during its production RFID tags are used through the assembly line. A radio-frequency identification system uses tags, or labels attached to the objects to be identified. A two-way radio transmitter-receivers known as interrogators or readers send a signal to the tag and read its response.

We can classify the RFID systems by the type of tag and reader used in the application. A Passive Reader Active Tag (PRAT) system has a passive reader that only receives radio signals from tags that are active (battery operated, transmit only). The range of reception of a PRAT system reader can be adjusted from 1–2,000 feet (0.30–609.60m) allowing flexibility and it is used in applications such as asset protection and supervision. Similarly an Active Reader Passive Tag (ARPT) system has an active reader that transmits the interrogator signals and also receives replies from passive tags. Likewise an Active Reader Active Tag (ARAT) system uses tags that are active and waken when an interrogator signal from the active reader reaches. A small variation of this system could use a Battery-Assisted Passive (BAP) tag which acts like a passive tag but has a small battery to power up the tags and then return the reported signal. Similarly fixed readers are used to create a specific interrogation zone that can be tightly controlled for accessing. This kind of system allows a highly defined reading area for reader when tags go in and out of the interrogation zone. Mobile readers can either be hand-held or mounted on vehicle for various purposes depending on its usage.

1. EXISTING SYSTEM

Hardware-based selective unlocking: A Hardware-based selective unlocking schemes were the previously proposed system. These include: Blocker Tag [15], RFID Enhancer Proxy, RFID Guardian [16], and Vibrate-to-Unlock.All of

these system approaches, however, require the users to carry an auxiliary device. A Blocker Tag is one of a special RFID tag, called "blocker, "that is used for the identification process by disrupting the reader to identify tags in proximity. RFID Enhancer Proxy and RFID Guardian are special RFID-enabled devices that could be implemented in a PDA or cell phone. They are assumed to come with greater computation capability and, thus, can perform more sophisticated interactions with readers, on behalf of tags, for various security purposes.

In Vibrate-to-Unlock, a user unlocks the RFID tags by identifying the tags that are used through vibrating the phone. Similarly, this kind of an auxiliary device may not be available at the time of accessing RFID tags, and therefore users may not be always interested to carry these devices. A Faraday cage can also be used to prevent an RFID tag from responding by preventing its transmission that is in the range. However, a special-purpose cage (a foil envelope or a wallet) could be needed and the tag would need to be removed from the cage in order to be read. This greatly decreases the usability of such solutions because users may not be always interested to put up any changes to the model that are used traditionally. However by, building a true Faraday Cage that prevents all communication which is known to be a significant challenge in the system. An example is a crumpled sleeve that is found to be not effective for shielding purposes .In contrast to above mentioned work, our work does not require the user to carry an auxiliary device or there does not exists any necessary to carry additional devices.

"Secret Handshakes" is another proposed method, were the selective unlocking method that is used based on context awareness. In order to unlock an accelerometer-equipped RFID tag using Secret Handshakes, the user must move or shake the tag (or its container) in a particular pattern. An example for this kind is that, the user should move the tag in parallel to the surface of the RFID reader's antenna in a circular manner. A number of unlocking patterns were studied and shown to exhibit low error rates. The major drawback to Secret Handshakes is that a particular movement pattern is required to unlock the tag. This kind of system makes changes to the existing RFID usage model. Similarly for a standard, insecure RFID setup requires users to bring their RFID tags within range of a reader, the Secret Handshakes method requires the users to consciously move the tag in a certain pattern. This clearly determines the usability of this approach.

Another proposed method is the use of distance bounding protocol that is a cryptographic challenge-response protocol. However, it requires shared key(s) between tags and readers as other cryptographic protocols. It allows the user to measure the upper bound distance that limits the user for accessing the tag. Using this protocol, a valid RFID reader can verify whether the valid tag is within the range or not. Modern cars or vehicles are embedded with complex electronic systems in order to improve driver safety and convenience. There arises a significant area for public and private manufacturer interest to include access control to the car, so that we can incorporate the system that helps to avoid duplication of cards by using RFID tags and readers.

All these existing system had some drawbacks either in its mechanism or in its application. In order to overcome this, a new system was proposed based on utilising the location information. GPS is used as the main source for location information.

2. PROPOSED SYSTEM

In this paper, we report on our work on utilizing location information for selective unlocking of tag and secure amount transaction on tags. Toll card is a card that can be bought with pre-defined values for tolls payment for a given vehicle used exclusively on motorways without manual tolls payment. Privacy of users is very important in RFID applications but at the same an objective and realistic definition of privacy is needed. In the real world, a vehicle or an automobile can be identified by using its number plate and then it is tracked by road authorities using video cameras as in the practice nowadays. Similarly, a toll card can be tracked by its issuing bank when it is used or whenever a transaction is made.

PROJECT OVERVIEW

3.1. IMPLEMENTATION

A typical RFID system consists of tags, readers. Tags are miniaturized wireless radio devices that store information about their corresponding subject. Such information is usually sensitive and personally identifiable. Toll cards will need to store a long list of toll booth locations. We notice that vehicles mounted with RFID toll tags are usually required to travel at a certain speed when they approach a toll booth. So we placed the RF Tag before certain distance from toll booth. RFID reader which is placed inside the car it reads the tag when it crossed the location. RF tag will contain the details about the speed of the car. If the driver did not reduce the speed it will automatically reduce the speed using the controller.

When the car entered the toll booth, user shows the tag over the RFID reader. The RF tag contains vehicle details whether it is small, medium or large vehicle and location of toll booth is identified by using GPS. If vehicle belongs to toll booth area it won't charge amount. If vehicle from other area the amount will be automatically credited depends on the size of the vehicle. This kind of payment is made by the bank to the user, by ensuring the authentication to the user.

3.2. LOCATION SENSING

For locating information a number of positioning technologies can be used to get accurate location information. The most popular positioning technologies to get location information include the satellite based-GPS, Wi-Fi-based positioning system, and cellular network-

based positioning system. All of these positioning systems have its own advantage and their performances also vary from the others in terms of its location information estimation accuracy. In many situations a combination of them does not make any sense to improve the overall accuracy. GPS is generally used as the main source of location information and the major enabler for location-based services. It has world-wide availability and an accuracy of a few meters in location estimation. It is adequately enough for most of the civilian applications. However, the accuracy of GPS gets faded inside the buildings and in arrow urban areas. Unlike GPS, Wi-Fi positioning can also be used to give good positioning results even indoors. Since, it is prone to interference of signal and hence not be always available due to its coverage limitations.

Cellular network positioning is almost available both outside and indoors. However, it has lowest accuracy of 50-100 meters in location estimation. Since location is used as a security control parameter in our approach, accuracy of location estimation can affect the security level. For example, poor accuracy can leads to large false unlocking rate in selective unlocking and gives more area for the adversary to cheat in proximity in transaction server verification. For this reason, the cellular network positioning technology is not believed as a good candidate to use to get location information for security purpose.

A GPS receiver gets its location information by timing the signals sent by GPS satellites that is located high above the Earth surface.

GPS receiver uses the contents of the messages it receives from the satellites to determine the travel time of each message and thus measures the distance to respective satellite. These distances along with the satellites' own locations are used with the possible trilateration technique, to compute the position of the receiver. For estimating location information, we make use of the well-known global positioning system (GPS).For that we first need to fuse a low-cost GPS receiver with a RFID tag, and then conduct relevant experiments to acquire location and speed information from GPS readings. Using these contents from satellite we can estimate the location information.

4. RESULTS AND DISCUSSIONS

SIMULATION RESULTS

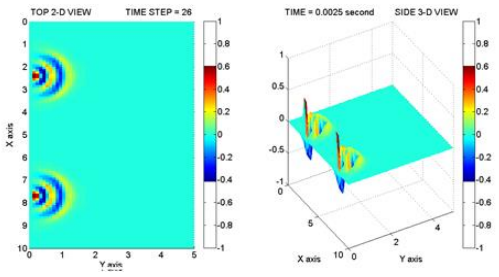

Fig 4.1 shows the process of signal transmission in 2D and 3D view.

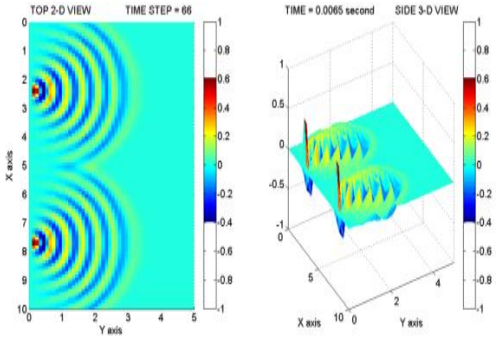

Fig 4.2 shows the process of transmission for locating the information for secure amount transaction to takes place.

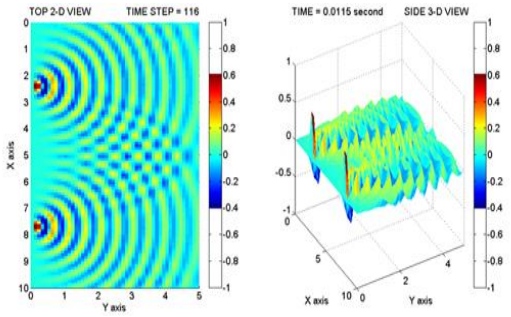

Fig 4.3 complete signal transmission in estimating location information for secure amount transaction.

EXPERIMENTAL RESULT

In this experiment, we used both location as well as speed as important parameters together to unlock the tag. Here, the tolerance of error for the location has to be set sufficiently high since the car is moving at a certain speed and the update rate of the GPS is 1 sample per second. Hence, it is also necessary to consider the fact that the car moves a certain distance within that span of 1 second. For example, a car moving at a speed of 45 mph can travel around 20 meters in 1 second. So, an error tolerance of 20 meters has to be provided. This would not affect applications like car toll systems because most of the toll booths are located far away from other places, and, hence, the area under consideration for the toll cards can be large. In other words, using a higher error tolerance for such a system would not affect the system performance. In previous experiments, an LED indicator was used for successful identification, which was later on used for unlocking the tag. It is also observed that we were successfully able to unlock the tag based on the location and speed, and our accuracies are improved when the location error tolerance was increased.

5. RELATED WORK

Modern cars embed complex electronic systems in order to improve driver safety and convenience. Areas of significant public and manufacturer interest include access to the car and authorization to drive. Traditionally, access and authorization have been achieved. In the last decade, this system has been augmented with remote access in which

users are able to open their car remotely by pressing a button on their key fobs.

6. CONCLUSION AND FUTURE WORK

Our toll cards based on speed and position information works only when a vehicle passes the toll gates at the suggested or particular speed. Hence when the car does not pass toll gates at that speed, toll card will be kept in locked state. The toll reader, hence, cannot read the information of the car and the corresponding user account, thus, cannot be charged successfully. So we also need consider with the reading failure due to user not driving at the suggested speed accidentally or intentionally. However, there exists a previously defined mechanism, which deals with failure reading in current RFID toll card system. Currently, appropriate position information rely on a camera equipped in toll gate, which takes a picture of the vehicle, and a RFID reader, which searches for a vehicles window/bumper mounted transponder to verify and collect payment. This kind of camera equipped RFID system sends a notice and fine to vehicles that pass through without having an active account or paying on the toll. Our work together with the existing camera-based mechanism and drivers are obligated to drive at the suggested speed by the government to avoid fines.

7. REFERENCES

[1] RFID Toll Collection Systems, http://www.securitysa.com/news.aspx?pklnewsid=25591, 2007.
[2] 66-Channel LS20031 GPS module http://www.megachip.ru/pdf/POLOLU/66_CHANNEL.pdf, 2011.
[3] GM-101 Cost Effective GPS Module http://www.alibaba.com/products/435104168/GM_101_CostEffective_GPS_Module.html, 2011.
[4] S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc.Int'l Conf. Theory and Applications of Cryptographic Techniques Advances in Cryptology (EUROCRYPT), 1993.
[5] J. Bringer, H. Chabanne, and E. Dottax, "HB++: A Light weight Authentication Protocol Secure against Some Attacks," Proc.Second Int'l Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006.
[6] M. Buckner, R. Crutcher, M.R. Moore, and S.F. Smith, "GPS and Sensor-Enabled Tags,"http://www.ornl.gov/webworks/cppr/y2001/pres/118169.pdf, 2013.
[7] M. Buettner, R. Prasad, M. Philipose, and D. Wetherall,"Recognizing Daily Activities with RFID-Based Sensors," Proc.Int'l Conf. Ubiquitous Computing (UbiComp), 2009.
[8] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In Proceedings of the European Workshop on Security and Privacy in Ad-hoc and Sensor Networks (ESAS), 2006.
[9] B. Danev, H. Luecken, S. Capkun, and K. Defrawy. Attacks on physical-layer identification. In Proc. of the 3th ACM Conference on Wireless Network Security (WiSec), pages 89–98. ACM, 2010.
[10] Y.Desmedt, C. Goutier, and S. Bagnio. Special uses and abuses of the Fiat-Shamir passport protocol. In CRYPTO, pages 21–39, 1987.
[11] S. Drimer and S. J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In Proceedings of 16th USENIX Security Symposium, Berkeley, CA, USA, 2007. USENIX Association.
[12] M.Flury, M.Poturalski, P.Papadimitrato,J, J.P.Hubux, Effectiveness of Distance-Decreasing Attacks against Impulse Radio Ranging. In 3rd ACM Conference on Wireless Network Security (WiSec), 2010.
[13] F.-L. W. Frank Stajano and B. Christianson. Multichannel protocols to prevent relay attacks. In Financial Cryptography, 2010.
[14] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch,H. Poor, and Z. Sahinoglu. Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks. Signal Processing Magazine.
[15] A. Juels and R. Rivets' and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," in Conference on Computer and Communications Security, 2003.
[16] M. Rieback and B. Crispo and A. Tanenbaum, "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management," in Australasian Conference on Information Security and Privacy, 2005.
[17] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," in Pervasive, 2007.
[18] A.Rabkin, "Personal knowledge questions for fall back authentication: Security questions in the era of Facebook," in Symposium on Usable Privacy and Security, 2008.
[19] A. Sample and D. Yeager and J. Smith, "A Capacitive Touch Interface for Passive RFID Tags," in Conference on RFID, 2009.
[20] D. Halperin and T. Heydt-Benjamin and B. Ransford and S. Clark and B. Defend and W. Morgan and K. Fu and T. Kohno and W. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defences," in Symposium on Security and Privacy, 2008.
[21] E.D. Kaplan and C.J.Hegarty, Understanding GPS-Principles and Applications, Artech House, 1996.
[22] M. Kuhn, An asymmetric Security Mechanism for Navigation Signals, 6th Information Hiding Workshop, Toronto, Canada, 2004
[23] J.A. Volpe, Vulnerability Assessment of the transportation infrastructure relying on GPS, NTSC NAVCEN draft re20. M. R. Rieback, B. Crispo, and A. S. Tanenbaum. Rfid guardian: A battery-powered mobile device for privacy management. In Australasian Conference on Information Security and Privacy (ACISP), 2005.
[24] A. Sample, D. Yeager, P. Powledge, and J. Smith. Design of a Passively-Powered, Programmable Sensing Platform for UHF RFID Systems. In IEEE International Conference on RFID, 2007.
[25] N. Segawa. Behaviour Evaluation of Sika Deer (Cervus Nippon) by RFID System. In WISP Summit, 2009.
[26] A. Sample, D. Yeager, and J. Smith. A capacitive touch interface for passive RFID tags. In Proceedings of the 2009 IEEE RFID Conference, 2009.
[27] J. Smith, A. Sample, P. Powledge, A. Mamishev, and S. Roy. A Wirelessly-Powered Platform for Sensing and Computation.In 8th International Conference on Ubiquitous Computing (Ubicomp), 2006.
[28] N. Bertelsen, K. Borre, the GPS Code Software Receiver, Aalborg University, Birkhauser, 2007.
[29] W. Franz and H. Hartenstein, Inter-Vehicle Communications, FleetNet project, University Karlsruhe, 2005.
[30] S. Godha, Performance Evaluation of Low Cost MEMS-Based IMU Integrated with GPS for Land Vehicle Navigation Application, University of Calgary, 2006.