LOCATION AS A UNIQUE IDENTIFIER FOR WI-FI ACCESS

Anthony .C. Ijeh[1a], Ahmad Al Dahoud[2], Jean .G. Maurice[1b], Stephen .A. Reames[1c]

College of Business Administration, A'Sharqiyah University, Ibra, Sultanate of Oman[1]
Faculty of Information Technology, Jordan University of Science and Technology, Jordan[2]
aijeh@asu.edu.om[1a], black4online@yahoo.com[2], jgmaurice@asu.edu.om[1b], sreames@asu.edu.om[1c]

Abstract

This paper discusses the use of location as a unique identifier for Wireless Fidelity (Wi-Fi) Access. The architecture of the prototype draws upon Location Based Services (LBS) and Wi-Fi technology. A detailed discussion of the access variables, functionality, and security is conducted. The paper concludes that most LBS monitoring devices rely upon emissions to control devices. However, emission security has no commercial standard and if electromagnetic waves are going to be effective then commercial standards for emission security need to be developed.

Keywords - Location, Wi-Fi, Access, Unique, Identity Management, Model

1 LOCATION BASED SERVICES

The Location Based Service (LBS) model used to develop the prototype by this researcher(s) is similar to the Jokela model [1]. The model describes how usability is a key role in the development of user interfaces for mobile telephones. This researcher(s) adopted the Jokela model because the model incorporates the professional practice of designing usable products. The researchers identified the task of user which, in turn, formed the basis of the product usability. Previous research indicates that all new products were efficient in tasks management (once quantified) before the design stage begins [1]. Similarly, profiling behavior in groups (i.e.-grouping components and architecture) of LBS will insure both reliability and workability in mitigating the risks to privacy [2].

1.1 Access Variables

In Tables 1.0 and 1.1 denotes independent and dependent variables that are utilized to develop a threat and trust model for LBS. The threat model dependent variables in Table 1.0 and mitigates them in Table 1.1. The flow of information between the dependent variables in Table 1.0 links each variable together and defines their interdependencies. The researcher demonstrates how existing variables in LBS are embodied in the Wireless Fidelity (Wi-Fi). The aim of location estimation methods determines the location of mobile devices from signal matrices measured from a set of access points [3]. The method utilizes centralized Wi-Fi architecture that is a set of access points which acts is client server. The particular method was the choice of the researcher since this method is commonly utilized by LBS end users and is proven to be an accurate tracking of mobile devices such as laptops [4].

The dependent variables provides monitoring, detection, and prevention. The logical components of the prototype are Radio Frequency Identity Tag (RFIT), Wireless Communication System (WCS), light weight access points, antennas, and exciters. The data measure of the dependent variables provides monitoring, detection, prevention. Protective quality is cross-checked with the use of International Standard Organizations (ISO) Information Security Management System standards (ISO27001:2005). The standard verifies the overall security strategy (i.e. - the security risks that affect the logical components). This standard defines space for monitoring, detection, and prevention. This protective method instructs the Wi-Fi compatible mobile device with LBS to monitor, detect, prevent, and protect unauthorized access to the wireless network. Moreover, the user's unique profile is stored to a database server which drives the security policy of the organization.

Table 1.0: Dependent and Independent Variables of LBS Threat Model [4]

Dependent Variables	Measure of Dependent Variable	Independent Variables	Measure of Independent Variable
RFID Technology	Compliance with EU & ISO/IEC Standards	Signal corruption, data, software, spatial relationships, projection, scale, data format, metadata, radio transmission	RFID Infrastructure used for live test
Test bed	Compliance with ISO/IEC Metric Measurement standards	Volume of the floor of the library, Volume of the Ceiling of the library, Volume of the Walls of the library	Volume of Test bed during live test
Wireless Communication System	Compliance with ISO/IEC standards and IEEE Protocols	Direct or reflected signals, algorithms, software engines, Specification	WCS Infrastructure used for live test
Access Points	Compliance with ISO/IEC standards and IEEE protocols	Range, RSSI, RSS, Signal strength, radio waves, reach	Received Signal Strength Indicator
Mobile Wireless device	Compliance with ISO/IEC Manufacturing standards	Specification	Functionality of Laptop during live tests
Noise & Interference	Compliance with ISO/IEC & IEEE Recommendations	Interference	Noise during live tests

Table 1.1: Dependent and Independent Variables of LBS Trust Model [4]

Dependent Variables	Measure of Dependent Variable	Independent Variables	Measure of Independent Variable
Trust Model	Mitigation of Threat Model	Wireless Security Model	Ability to Secure Wi-Fi Network

2 WIRELESS FIDELITY

Experiential studies reveal that wireless network technology has not been able to restrict radio waves used to transmit data from one access point to another. That is, leaking through windows and doors of an organizations building [5]. This is because Wi-Fi is based upon radio communications technology, as an alternative to structured wiring and cables [6]. Transmission by air waves allows unauthorized persons to access wireless networks from outside a buildings physical wall who utilize specially configured laptops. This, in part, is due to the lack of physical control over the radio waves [7]. Furthermore, wireless can broadcast anyone within its range. And special large antennas can pick and chose the non-physical radio waves to monitor [8].

2.1 Wi-Fi Functionality

Research studies confirm that location privacy is critical to the security of data transmitted by wireless technology. In addition, studies confirm that the implementation of the purportedly secure standards for wireless systems such as the 802.11 requires a new framework to provide security to data being transmitted [23]. Until late, information in transit remains in a plain unprotected form for some seconds

before it is re-encrypted into another format for transmission and this allows information criminals to crack a variety of security holes [9] as noted in Figure 1.0.

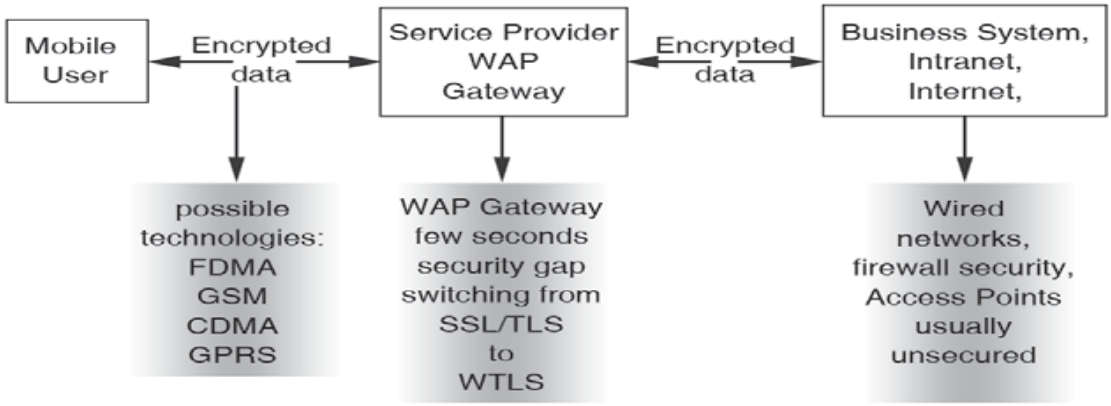

Figure 1.0: Overview of a wireless network security system [9]

3 UNIQUE IDENTITY

This paper does not suggest a new signal propagation model for location estimation or algorithms for the triangulation of locations. However, the researcher demonstrates a new method of securing Wi-Fi networks utilizing Location Based Services (LBS) with Geofencing [6, 10]. Experiential research reports that Radio Frequency Identity (RFID) technology is used in asset tracking, real time supply chain management, and telemetry based remote monitoring amongst others [11]. RFID technology was utilized in World War II by United Kingdom army aircraft to distinguish enemy aircraft from other aircraft through the use of radar. Research reveals that RFID and similar technologies can play a vital role in the future of Wi-Fi networks [11]. Unique identity can be monitored using SPSS statistical tools for data analysis in order to recognize human activity like walking [12, 13]. I.e. - walking speed is extracted using features from speed sensors attached to a user; the procedure allows monitoring technology such as RFID [14].

3.1 Identity Management

RFID technology is classified as a wireless automatic identification and data capture technology [15]. The technology employs radio waves for detecting objects [11]. The use of RFID is described as the effective and efficient tracking of assets [16]. Since Radio Frequency Identification (RFID) technology requires no visibility, which leads to the reduction of human intervention, the ability to successfully track, locate, identify, and trace objects is an asset [17]. In addition RFID assigns individual identification numbers to each product thereby lending itself to item level traceability [4, 10]. Research reveals that the majority of RFID tags produced today are passive RFID tags, comprised basically of a micro-circuit and an antenna [18]. They are referred to as passive tags because the only time at which they are actively communicating is when they are within close proximity of a passive RFID tag reader or interrogator [18].

In addition, research identified another type of common RFID tag in the marketplace today. It is known as the active RFID tag, which usually contains a battery that directly powers RF communication [18]. This onboard power source allows an active RFID tag to transmit information about itself at great range, either by constantly communicating this information to a RFID tag reader which is responsible for the transmission of an electromagnetic wave into the detection field via its antenna [18]. Research studies show that active RFID tags can transmit only when prompted to do so [19]. This is because active tags are usually larger in size than passive tags and can contain substantially more information because of higher amounts of memory than do pure passive tag designs [19]. Active tags are typically used in real-time tracking of high-value assets in closed-loop systems that is, systems in which the tags are not intended to physically leave the control premises of the tag owner or originator [19].

Active RFID tags can provide tracking if a positive or negative indication when an asset is present in a real-time location [20]. Most Real Time Location Systems (RTLS) are based on the use of active RFID tag technology. The intensities of radio signals emitted from Wi-Fi networks can be used to detect the position of a mobile device since there is a functional dependence between the signal strength received from an access point (AP) and the physical position of the mobile device [4].

Additional research reveals that accurate models of radio transmission patterns are important for protocol design and simulation [21]. A research report presented results from an experiment using Radio Frequency test equipment which precisely measured sensor node transmission and signal strength in order to accurately determine transmission patterns [21]. The study led to a proposed methodology to optimize the design of an asset tracking system that was constrained by a limited number of RFID readers [16]. The active and passive RFID applications and comparison is noted in Table 1.2. This table compares the two types of tags and the applications. The researcher(s) utilized a tag to monitor the movement of a laptop during the experiment. [22].

Table 1.2: Active and Passive RFID Applications & Comparisons [4]

Application	**Active RFID**	**Passive RFID**
Tag Power Source	Internal to Tag	Energy transferred from the reader via RF
Tag Battery	Yes	No
Availability of Tag Power	Continuous	Only within field of reader
Required Signal Strength from Reader to Tag	Very Low	Very High (Must power the tag)
Available Signal Strength from Tag to Reader	High	Very Low
Communication Range	Long range (100m or more)	Short or very short range (3m or less)
Sensor Capability	Ability to continuously monitor and record sensor input, data/time stamp for sensor events	Ability to read and transfer sensor values only when tag is powered by reader, no date/time stamp
Data Storage	Large read/write data storage (128kb) with sophisticated data search and access capabilities available	Small read/write data storage (e.g. 128 bytes)

4 SUMMARY

The architecture, introduced herein, was utilized while developing a framework for location as a unique identifier and the concepts relevant to the framework. The researcher(s) then examined areas of research and practice currently using location as a unique identifier for access control. The purpose was to better understand tested concepts and determine how the framework can securely combine both the Wi-Fi components and architecture to secure Wi-Fi networks. Future research is centric to the rarely explored area of emission security. That is, most LBS monitoring devices rely on emissions to control devices such as RFID technology but little is known about emission security and its technology which, until late, date has been the reserved for several governmental agencies without a commercial standard. If electromagnetic waves are to be utilized effectively then a commercial standard for emission requires development.

5 REFERENCES

[1] Jokela, T. Koivumaa, J. Pirkola, J. Salminen, P. Kantola, N. (2006): Methods for quantitative usability requirements: a case study on the development of the user interface of a mobile phone. In Personal Ubiquitous Computing, 10(6), p345-355. [Online] Available at: http://dx.doi.org/10.1007/s00779-005-0050-7 (login required) [Accessed 20th of July 2011].

[2] Wealands, K. Banda, P. Cartwright, W. E. (2007): User Assessment as Input for Useful Geospatial Representations within Mobile Location-Based Services, 11 (2), p283-309

[3] Roos, T. Myllymaki, P. Tirri, H. Misikangas P. Sievanen, J. (2002): A Probabilistic Approach to WLAN User Location Estimation International Journal of Wireless Information Networks (9)3, p155-164. ISBN: 1068-9605-02-0700-0155-0

[4] Ijeh, A.C. Preston, D.S. Imafidon, C.O. Watmon, T.B. Uwaechie, A.O. Nwadube, A.R. Kujabi, E. (2010): Geofencing Components and Existing Models: IAENG International Conference on Communication Systems and Applications (ICCSA). Royal Garden Hotel, 17th-19th March, 2010 3(3), p823-828, ISBN: 978-988-18210-4-1 [Online] Available at: http://www.iaeng.org/publication/IMECS2010/IMECS2010_pp823-828.pdf [Accessed 20/7/11]

[5] Curran, K and Smyth, E. (2005): Exposing the Wired Equivalent Privacy Protocol Weaknesses in Wireless Networks. International Journal of Business Data Communications and Networking Vol. 1, No. 3, p: 59-83. ISSN: 1548-0631

[6] Ijeh, A.C. Brimicombe, A.J. Preston, D.S. and Imafidon, C.O. (2009): Geofencing in a security strategy model. In Global Security, Safety and Sustainability (eds. Jahankhani, H., Hassami, A. & Hsu, F.), Springer, Berlin: p104-111. ISBN: 978-3-642-04061-0. [Online] Available at: http://www.springerlink.com/content/p85j16w581444106/ (login required) [Accessed 20th of July 2011].

[7] Everett, C (2008): Financial Exposure, Infosecurity Volume 5, Issue 1, January-February 2008, Elsevier B.V. p34-37.[Online] Available at: http://dx.doi.org/10.1016/S1754-4548(08)70013-5 [Accessed 20th of July 2011].

[8] Lashkari, A.H. Danesh, M.M.S. Samadi, B. (2009): A survey on wireless security protocols (WEP, WPA and WPA2/802.11i) Proceedings 2nd IEEE International Conference on Computer Science and Information Technology 2009, p1-5. ISBN: 978-1-4244-4519-6

[9] Mnkandla, E. Dwolatsky, B. and Nleya, B.M. (2006): A model for an effective security strategy on wireless technologies. Computing & Software Technical Engineer IT, (August 2006 Edition), p1-3. [Online] Available at: http://www.eepublishers.co.za/images/upload/Security%20strategy.pdf [Accessed 20th of July 2011].

[10] Ijeh, A.C., Brimicombe, A.J., Preston, D.S., Imafidon, C.O. (2009): Security Measures in Wired and Wireless Networks. In Proceedings of the Third International Conference on Innovation and Information and Communication Technology (ISIICT'09) held at the Philadelphia University, Amman, Jordan, 15th – 17th December, 2009: Published by the British Computer Society, Swindon, UK, p1-10. [Online] Available at: http://dl.acm.org/citation.cfm?id=2228043 [Accessed 20/02/13]

[11] Pathak, R. Joshi, S. (2009): Java based software framework and its integration in mobile phones using RFID technologies. Proceedings of the 3rd IEEE international conference on Internet multimedia services architecture and applications (IMSAA'09), IEEE Press, Piscataway, NJ, USA, p153-158, ISBN: 978-1-4244-4570-7.

[12] Ijeh, A.C. Ali-Alao, B. Preston, D.S. Imafidon, C.O. (2011) Quantitative Analysis of ISO/IEC 27001 Security Policies: The 1st IEEE Conference on Communication, Science & Information Engineering, (CCSIE). Middlesex University, London 25th – 27th, 2011: p183-186, ISBN**:** 978-0-9556254-5-9 [CD-ROM] Available at: http://www.ccsie.org/Contact.htm [Accessed 20/7/11].

[13] Ijeh, A.C. Ali-Alao, B. Preston, D.S. Imafidon, C.O. (2011) Simulating Euclidean Distances using Location Based Services: The 1st IEEE Conference on Communication, Science & Information Engineering, (CCSIE). Middlesex University, London 25th – 27th, 2011: p180-182, ISBN: 978-0-9556254-5-9 [CD-ROM] Available at: http://www.ccsie.org/Contact.htm [Accessed 20/7/11].

[14] Mantyjarvi, J. Himberg, J. and Seppanen, T. (2001): Recognizing Human Motion with Multiple Acceleration Sensors. Systems, Man, and Cybernetics, 2001 IEEE International Conference, 2 (1), p747 – 752, ISBN: 0-78003-7087-2

[15] Irani, Z. Gunasekaran, A. and Dwivedi, Y. (2010): Radio frequency identification (RFID): Research trends and framework. International Journal of Production Research, Taylor and Francis 49(9): 1-27. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/00207540903564900 (login required) [Accessed 20th of July 2011].

[16] Oztekin, A. Pajouh, F.M. Delen, D. Swim, L.K. (2010): An RFID network design methodology for asset tracking in healthcare, in Science Direct. Decision Support Systems. 49(1) p100-109

[17] Theisse, F. and Michahelles, F. (2006): An overview of EPC technology, Sensor Review, Emerald Group Publishing Limited, 26 (2), p101–105. ISSN: 0260-2288. [Online] Available at: http://www.emeraldinsight.com/journals.htm?articleid=1549954 (login required) [Accessed 20th of July 2011].

[18] Glover, B. and Himanshu, B. (2006): RFID Essentials, 1st edition. O'Reilly Media Inc., Cambridge, UK, ISBN: 0-596-00944-5

[19] Domdouzis, K. Kumar, B. Anumba, C. (2007): Radio-frequency identification (RFID) applications: A brief introduction, [Online] Available at: http://dx.doi.org/10.1016/j.aei.2006.09.001 (login required) [Accessed 20th of July 2011].

[20] Ijeh A.C. Brimicombe, A.J. Preston, D.S. Imafidon, C.O. Uwaechie, A.O. (2009): Using Geofencing to Overcome Security Challenges in Wireless Networks: Proof of Concept: In the proceedings of the Information Society 12th international multi-conference 12th-16th October 2009. Ljubljana, Slovenia. (1), p311-314. ISSN: 15819973 [Online] Available at: http://is.ijs.si/is/is2009/zborniki/Zbornik_A.pdf [Accessed 20/7/11].

[21] Scott, T. Wu, K. Hoffman, D. (2006): Radio propagation patterns in wireless sensor networks, new experimental results. Proceedings of the 2006 international conference on Wireless communications and mobile computing, ACM, New York, USA, p857-862, ISBN: 1-59593-306-9

[22] Ijeh, A.C. Brimicombe, A.J. Preston, D.S. Imafidon, C.O. (2009): Evaluating Ethical and Productivity Issues in Geofencing: Symposium on Progress in Information & Communication Technology, Kuala Lumpur, Malaysia, 7th-8th December 2009: University of Utah 1(1), p1-6. ISBN: 978-983-41743-1-6 [Online] Available at: http://spict.utar.edu.my/SPICT-09CD/contents/pdf/SPICT09_A-1_1.pdf [Accessed 20/7/11].

[23] Tutanescu, I. Sofron, E. Ali, M. (2010): Security of internet-connected computer networks, International Journal Internet Technology and Secured Transactions, 2(13), p.109–121.

ACKNOWLEDGEMENT: Presentation of this paper was made possible by funds provided by the College of Business Administration (COBA) and Vice Chancellors Office (VCO) at A'Sharqiyah University.