A PILOT SCENARIO OF SECURE LOCATION-BASED SERVICES IMPLEMENTATION IN A UNIFIED WIFI NETWORK

B. Radulović[1], J. Stergar[2]

[1] Cisco Systems, Bravničarjeva 13, 1000 Ljubljana, Slovenia
[2] University of Maribor, Faculty of Electrical Engineering and Computer Science, Maribor, Slovenia

Key words: RFID, Location-Based Services, IEEE 802.11 infrastructure, Wi-Fi.

Abstract: In this paper a pilot scenario of secure location-based services implementation in a unified Wi-Fi network based on Cisco networking devices and location aware appliances will be presented. Third party active RFID tags from AeroScout have been used for the location aware tracking of users. We will present an indoor scenario of RF location tracking system implementation based entirely on a unified wireless network IEEE 802.11 infrastructure. In an environment sparse with obstacles a precision accuracy of criteria 1m/50% was achieved.

Pilotni scenarij implementacije varovanih lokalizacijskih storitev v združenem WiFi omrežju

Kjučne besede: RFID, lokacijske storitve, infrastruktura IEEE 802.11, Wi-Fi

Izvleček: V tem članku bomo predstavili pilotski scenarij implementacije varovanih lokalizacijskih storitev v združenem Wi-Fi omrežju zasnovanem na Cisco omrežnih napravah in lokalizacijskih orodjih. Za sledenje položaja uporabnikov so bile uporabljene aktivne značke z radijsko identifikacijo (RFID) podjetja AeroScout. Predstavili bomo scenarij notranje postavitve sistema za sledenje z radijsko identifikacijo, ki temelji izključno na brezžični infrastrukturi IEEE 802.11. V okolju z razmeroma malo ovirami je bila dosežena zanesljivost lokalizacije po kriteriju 1m/50%.

1. Introduction

The term location-based services (LBS) are a recent concept that denotes applications integrating geographic location with the general notion of services /1/. 3GPP strictly distinguishes between location-based services and location services. The latter exclusively deals with the localization of target persons and objects and with making the resulting location data externally available. A location service does not imply the processing of location data in the sense of filtering or selecting location-dependent information or performing other high-level actions as in LBS; it is only responsible for the generation and delivery of location data /2/. Despite the strict definition we will use the term LBS as it appears in most of the literature including location-services based on IEEE 802.11 wireless technology.

The rapid increase in the adoption rate of Wi-Fi coupled with the availability of high quality infrastructure at reasonable cost are key factors behind the outbreak of commercial and academic activity regarding Wi-Fi location-based services. Research and development progress in Wi-Fi location prediction techniques based entirely on IEEE 802.11 infrastructure have facilitated the emergence of indoor RF location tracking systems /3/. With integrated location tracking, enterprise wireless LANs become much more valuable as a corporate business asset.

Maintaining accurate information about the location of individuals or valuable equipment is a complex and ongoing requirement for any large enterprise. To streamline asset tracking and improve workflows for equipment procurement and logistics, new technologies such as radio frequency identification (RFID) are the promising solution on the market /4/.

Offering end-to-end object visibility, the RFID technology seems to revolutionize the supply-chain industry, significantly reducing costs and helping to enable differentiation. With support from such major industry figures as IBM, Wal-Mart, and Procter & Gamble, the momentum is clearly behind this technology. Most deployments are in the pilot phase now, with companies learning about and preparing to use this technology and planning to face the funding issues and business process changes that it will bring.

RFID technology offers the following significant advantages over traditional barcode data collection, although RFID will probably never replace barcodes completely:

- As opposed to barcodes RFID tags identify each item separately
- While barcodes have to be properly oriented Line-of-sight for RFID tags is not necessary.
- Resistant to harsh environments—Barcode life is limited by how long the printed symbols remain readable.
- Can be reprogrammed and reused—New data cannot be written to barcodes.

- Can be read in groups—Barcodes must be read individually, whereas an RFID reader can scan multiple items simultaneously.
- Secures data—Tag memory can be programmed, optionally permanently locked, and can also be erased to protect privacy.

RFID already has numerous commercial applications, such as automobile theft prevention, collecting drive-through tolls, managing traffic, gaining entrance to buildings, automating parking, dispensing goods and books tracking in libraries. As RFID technology solutions mature, companies everywhere will also experience unprecedented supply-chain visibility and information exchange. Currently, EPCglobal, Inc., based on a joint venture between the Uniform Code Council and EAN International, is responsible for developing a single industry standard worldwide to further enable adoption of RFID based on the Electronic Product Code (EPC). The EPC is the favored specification of both Wal-Mart and the U.S. Department of Defense (DoD). This positions EPC as the leader for large supply-chain implementations /5/.

2. RFID Tag Technology

RFID is a means of identifying a person or an object using radio transmissions. This is accomplished by using two primary components: the transponder – an RFID tag located on the object to be identified, which contains a microchip and miniature antenna; and the reader – also known as a detector or interrogator, which communicates with the tag and passes its information on to a controlling system or middleware host /5/.

The majority of RFID tags produced today are passive RFID tags, comprised basically of a microcircuit and an antenna. They are referred to as passive tags because the only time in which they are actively communicating is when they are within the RF field of a passive RFID tag reader.

Another type of common RFID tag is known as the active RFID tag, which usually includes a battery that directly powers RF communication. This onboard power source allows an active RFID tag to transmit information about itself at great range, either by constantly beaconing this information to a RFID tag reader or by transmitting only when it is prompted. Active tags are usually larger in size and can contain substantially more information (because of higher amounts of memory) than do pure passive tag designs /3/.

The combination of both technologies is combined into semi-passive tags which differ from passive tags in that they use an onboard battery to provide power to communication and ancillary support circuits such as temperature and shock monitoring. Although they employ an onboard power source, semi-passive RFID tags do not use it to directly generate RF electromagnetic energy as active RFID's do. Rather, these tags typically make use of backscatter modulation and reflect electromagnetic energy from the RFID reader to generate a tag response similar to that of standard passive tags.

2.1. Active RFID Tags

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). The relatively higher cost of assets tracked with active RFID tags (as compared to those typically tracked with passive RFID) usually justifies the higher cost of the active tag itself and presents strong motivation for tag re-use. Medical equipment, electronic test gear, computer equipment, reusable containers, and assembly line material-in-process are all excellent examples of applications for active tag technology. Active RFID tags can provide tracking in terms of presence (positive/negative indication of whether an asset is there/missing in a particular area) or real-time location. Active RFID tags are physically larger and typically more costly than passive RFID tags. Most Real Time Location Systems (RTLS) are based on the use of active RFID tag technology.

Active RFID tags can be sub-categorized into those that operate as transponders and those that operate as beacons. Of special interest are the active RFID tags that operate in the unlicensed ISM bands and abide by IEEE 802.11 protocols. These special active RFID tags are known as 802.11 (Wi-Fi) active RFID tags – this type was used for our pilot study.

Beaconing active RFID tags are used in many RTLS systems and are of primary use when the precise location of an asset needs to be tracked anywhere and anytime without the need for pre-positioned interrogators or tag exciters to trigger tag transmission. With a beaconing active RFID tag, a short message payload known as a "beacon" is emitted at pre-programmed intervals with the unique identifier of the RFID tag. This interval is programmed into the tag by the tag owner/user and can be set depending on the degree of criticality associated with tag location updates.

Any 802.11 Wi-Fi active RFID tag that is capable of successfully authenticating and associating with the underlying WLAN infrastructure (and issues probe requests regularly on all channels) should be recognizable by the Cisco LBS solution as a WLAN client (in WCS as a rectangular blue icon, Figure 2).

2.2. Implemented 802.11 Active RFID Tags

802.11 active RFID tags are designed to operate in the unlicensed ISM bands of 2.4 to 2.4835 GHz or 5.8 to 5.825 GHz. Currently manufactured 802.11 Wi-Fi active RFID tags available at publication are limited to 2.4 GHz.

These tags exhibit the characteristics of active RFID tags, but also comply with applicable IEEE 802.11 standards and protocols. Wi-Fi RFID tags can readily communicate directly

with standard Wi-Fi infrastructure without any special hardware or firmware modifications and can co-exist alongside Wi-Fi clients such as laptops, VoWLAN phones, and so on. When powered on, assets equipped with 802.11 Wi-Fi client radios can be tracked natively without the need to have an asset tag attached. Other assets lacking an internal 802.11 Wi-Fi client radio can be tracked via a physically attached 802.11 active RFID tag. A physically attached 802.11 active RFID tag also makes it possible to use the location-aware Cisco UWN to track assets with integrated Wi-Fi client radios when those radios are powered off.

AeroScout T2 Tags were used for the presented scenario of secure LBS. The AeroScout T2 Tag is one of the, if not the leading Wi-Fi tag. The T2 Tag has proven usability, dependability, scalability and flexibility for a wide variety of industries and applications. The T2 messages can be received and processed by standard Cisco Systems wireless access points, keeping infrastructure costs low with a straightforward installation. The T2 is characterized by its long battery life, convenient small size, built-in choke point capabilities and telemetry functionality. T2 Tags enable separate transmission intervals when they are stationary or in motion, which additionally reduces unnecessary network traffic /8/.

3. Location Tracking Approaches

Location tracking and positioning systems can be classified by the measurement techniques they employ to determine mobile device location – localization. These approaches differ in terms of the specific technique used to sense and measure the position of the mobile device in the target environment under observation. Typically, RTLS can be grouped into four basic categories of systems that sense and measure position on the basis of the following:

- Cell of origin (nearest cell)
- Distance (lateration)
- Angle (angulation)
- Location patterning (pattern recognition)

An RTLS designer can choose to implement one or more of these techniques. This may be clearly seen in some approaches attempting to optimize performance in two or more environments with very different propagation characteristics. An example of this is an RTLS system attempting to yield optimal performance for both indoor and outdoor applications by using two different techniques. It is not unusual to hear arguments supporting the case that a fifth category should exist to include those RTLS systems that sense and measure position using a combination of at least two of the four techniques mentioned above. Regardless of the underlying positioning technology, the "real-time" nature of an RTLS is only as real-time as the most current timestamps, signal strengths, or angle-of-incidence measurements. The timing of probe responses, beaconing rates, and location server polling intervals can influence discrepancies seen between actual and reported device position from reporting interval to reporting interval /3/.

4. Accuracy and Precision of the Location Based Services Solution

With proper deployment according to the best practices /3/ the accuracy and precision of the tested LBS solution in indoor deployments is represented as follows:

- Accuracy of less than or equal to 10 meters, with 90 % precision
- Accuracy of less than or equal to 5 meters, with 50 % precision

In other words, given proper design and deployment of the system, the error distance between the reported device location and the actual location should, in 90 % of all reporting instances, be 10 meters or less. In the remaining 10 % of all reporting instances, the error distance may be expected to exceed 10 meters. Note that these specifications apply only to solutions using RF Fingerprinting; namely, the use of a WCS licensed for location usage (with or without a location appliance).

For applications that require better performance than an accuracy of 10 meters with 90 % precision, the Cisco LBS solution can deliver accuracy of 5 meters or less but with 50 % precision. Stated another way, in 50 % of all reporting instances, it can be reasonably expected that the error distance between the reported and the actual location exceeds 5 meters. The location inspection tool can display various levels of accuracy and precision from 2 m to 100 m along with which areas of the inspected environment can meet these accuracy levels.

5. The unified wireless network setup and configuration

The network infrastructure was build from scratch. No appropriate RFID capable or compatible equipment was previously available. The network environment was setup at the annual Cisco EXPO conference (2007). The proof of concept for wireless appliances was targeted for a small to medium enterprise (50-100 employees).

The WAN connection was firewalled with a software based IOS firewall on a Cisco 1800 Series Integrated Services Router. The integrated services routing architecture of the Cisco 1800 Series offers features that provide the complete functionality and flexibility to deliver secure Internet and intranet access. It is ideal for small to medium-sized businesses and small enterprise branch offices enable businesses to reduce costs by deploying a single, resilient system for fast, secure, delivery of multiple mission-critical business services. As aggregation switch a Cisco Series 3560 switch was implemented. The Cisco Catalyst 3560 Series are next-generation energy-efficient Layer 3 Fast

Ethernet switches. For the access switching nodes basic models L2 Cisco Catalyst Express 500 Series of switches were used. Cisco Catalyst Express 500 Series switches meet the needs of growing businesses with up to 250 employees. This family of Layer 2-managed Fast Ethernet and Gigabit Ethernet switches offers non-blocking, wire-speed performance and provides a secure network foundation optimized for data, wireless, and IP Communications (Figure 1,Table 1).

Table 1: Used equipment

Cisco1812	Router Series 1800	1
WS-C3560G	L3 switch with 24 10/100/1000 ports and 2GE SFP ports	1
WS-CE500	L2 switch with 24 ports and 24 PoE	2
AP1010	Lightweight Access Point	6
LOC2710	Location Appliance	1
WLC4402	Wireless Location Controller (12 AP)	1
WCS	Wireless Control System	1

Lightweight access points Cisco 1000 Series were implemented. The Aironet 1000 Series lightweight access points are specifically designed for operation with Cisco Wireless LAN Controllers and the Wireless Control System management tool. They provide dual band support for both 802.11a, 802.11b and 802.11g, simultaneous air monitoring for dynamic, real time RF management. In addition, the Lightweight Access Points handle time-sensitive functions, such as L2 encryption, that securely support voice, video, and data applications in wireless LANs.

The Cisco 4400 Series Wireless Controller for AP management was installed. The Wireless LAN Controllers is designed for medium-to-large enterprise facilities. The Cisco 4402 with two Gigabit Ethernet ports comes in configurations that support up to 12, 25, and 50 lightweight access points. It provides one expansion slot that can be used to add enhanced functionality, such as VPN termination and other future capabilities.

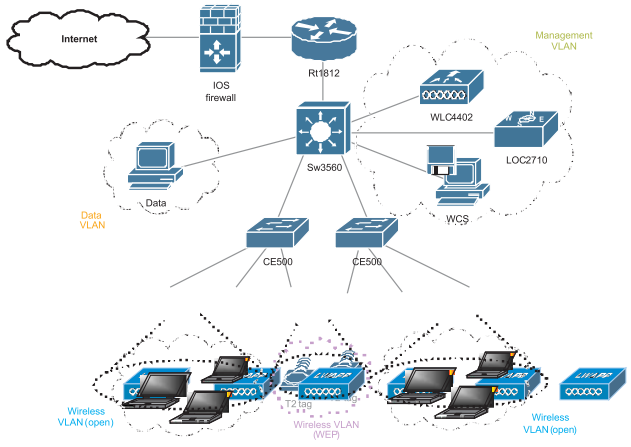

Fig. 1: The implemented location-aware unified wireless network architecture.

Next the Cisco Wireless Location Appliance was integrated. The 2710 Wireless Location Appliance simultaneously tracks thousands of 802.11 wireless devices from directly within a WLAN infrastructure, increasing asset visibility and control of the RF environment. Additionally, the appliance provides location-based alerts for business policy enforcement and records rich historical location information that can be used for location trending, rapid problem resolution, and RF capacity management.

Finally the Wireless Control System was installed on a Windows 2003 server. The Cisco Wireless Control System (WCS) is a Cisco Unified Wireless Network Solution management tool that adds to the capabilities of the web user interface and command line interface (CLI), moving from individual controllers to a network of controllers. WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

Light-Weight Access points forward information to WLAN controller (WLC) regarding the detected signal strength of any WLAN clients (Wireless VLAN) and asset tags (Wireless WEP VLAN). At least three access points detect the asset tag's transmission. It is forwarded to the WLC to which the detecting access points are registered. In normal operation, access points focus their collection activities for this information on their primary channel of operation, going off-channel and scanning the other channels in their regulatory channel set periodically. The collected signal strength information is forwarded to the WLC to which the access point is currently registered, which aggregates the information such as battery status and tag or asset telemetry. The location appliance (LOC) uses SNMP to poll the controller (or controllers if there are many) for the latest signal strength information for each tracked category of device /6/.

All implemented hardware was appropriately configured using /9/, /10/, /11/, /12/, /13/, /14/.

6. Inspecting Location Quality and Precision

A new capability introduced with the latest Wireless Control System (Cisco WCS) and using the location appliance is Location Inspection.

Location inspection is the ability to directly validate the performance of the created path loss models via the calibration process. Unlike the location planner or location readiness tools, which are purely predictive in nature, when location quality is inspected, predicted locations to actual physical locations are directly compared and graphically expressed using the accuracy of the path loss model. With the use of the calibration model and the *location inspection tool*, it can be quantified whether achieving the 10 m/90 % performance metric in the environment and if so, whether it has been uniformly achieved throughout the area. Location inspection allows a topography preview of areas where the location performance may be below the performance

expectations as well as those where it is clearly exceeding them (Figure 2).

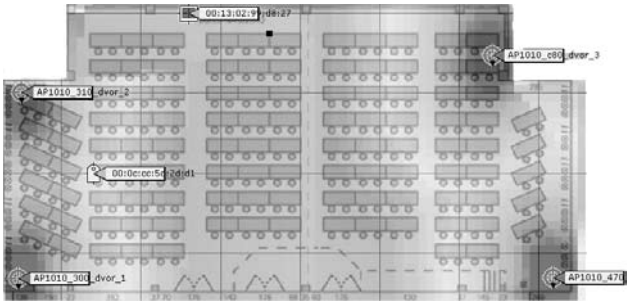

Fig. 2: On-Demand WLAN Client Localization using WCS (clients are depicted with blue whereas RFID tags with yellow).

Location inspection uses the signal strength information recorded during data collection and the path loss model to compute estimated location. It does this for each data collection point that was recorded. These estimated locations are then compared against the actual location coordinates (also recorded during data collection). The results of the comparison are displayed in a graphical format indicating the level of precision available throughout the environment for various selected accuracy levels.

The performance metric often used having the most familiarity and significance is accuracy. Accuracy typically refers to the value of the received information. Location accuracy refers particularly to the quantifiable error distance between the estimated location and the actual location of the mobile device.

In most real-world applications, however, a statement of location accuracy has little value without the ability of the solution to repeatedly and reliably perform at this level. Precision is a direct measure reflecting on the reproducibility of the stated location accuracy. Any indication of location accuracy should therefore include an indication of the confidence interval or percentage of successful location detection as well, otherwise known as the location precision /7/.

Measurements have been performed to estimate the deviation of reported and actual position of targets compared to measurement accuracy as regarding the 10 m/90 % performance metric criteria in the environment under observation and whether it has been uniformly achieved throughout the area.

For the precision estimation of measurements a straightforward arithmetic mean with mean absolute error (MAE) estimation was used. Additionally all measurements in column 2 (Table 2) were rounded up, thus the actual error is even lesser.

$$\overline{x} = \frac{1}{n}\sum_{1}^{n} x_i \qquad \varepsilon_i = \left|\overline{x} - x_i\right| \tag{1}$$

where x_i is the actual measurement and ε_i the absolute error.

Table 2: Accuracy measurements of objects reported by the LBS System compared to a reference grid.

Measurement Nr.	Distance (m)	Error (m)
1	2	-0,79
2	3	0,21
3	4,5	1,71
4	2	-0,79
5	2	-0,79
6	0,5	-2,29
7	4	1,21
8	2,5	-0,29
9	3	0,21
10	3,5	0,71
11	2,5	-0,29
12	4	1,21
13	3	0,21
14	1,5	-1,29
15	2,5	-0,29
16	3	0,21
17	4	1,21
MAE (m)	2,79	

It is evident that all predicted measurements in the environment under inspection were clearly within the guaranteed 10m/90% criteria. In our case with an area including very little obstacles even the 1m/50% criteria could be met. Also measurements have been performed repeatedly to estimate the confidence interval (Figure 3).

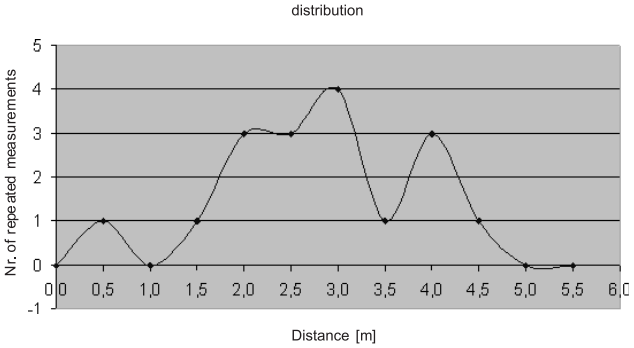

Fig. 3: The confidence interval estimation.

In addition measurements not fulfilling the triangle AP criteria were checked. As expected the measured position of the targets and their actual position were nondeterministic using implemented distance based or TDoA (Time Difference of Arrival) lateration techniques. Nevertheless rude estimation with RSS (Received Signal Strength) with appropriate path loss model is still possible /3/.

7. Conclusion

A Pilot Scenario of Secure Location-Based Services Implementation in a Unified WiFi Network was presented. State of-the-art hardware with the unified wireless Cisco network architecture with IEEE 802.11 infrastructure was used. The benefits of such an implementation are in using the existent

wireless environment extending it with additional hardware for implementation of new services for localization. Localization of targets well beyond the guaranteed 10m/90% criteria was achieved.

Pilot scenarios as the one presented or simple deployments can perform well with standard IP networks without complete upgrades. Localization results even much below the criteria 10m/90% can be achieved in environments sparse with obstacles. An accuracy of 1m/50% was demonstrated. However, network features can be used to optimize RFID deployments. Functionality such as network availability and scalability, simplified network provisioning, network security, and network quality of service are enhancements that advanced deployments will require. Choosing the correct network infrastructure in the beginning of the design will help to ensure the investment protection of RFID networks.

Aknowledgements

The authors thankfully acknowledge the assistance of Cisco Slovenia supporting this study with state-of-the-art equipment.

References

/1./ J. Schiller and A. Voisard Eds., Location-Based Services, Morgan Kaufmann, 2004.

/2./ Küpper, Location-based Services, John Willey & Sons, 2005.

/3./ Cisco Systems, *Wi-Fi Location-Based Services - Design and Deployment Considerations*, 2006.

/4./ Cisco Systems, Cisco Tracks Corporate Assets with RFID and Wireless LAN Solutions http://www.cisco.com/web/about/ciscoitatwork/news/082420061.html

/5./ Cisco Systems, *Cisco Systems and RFID Technology*, White Paper, 2004.

/6./ Cisco Systems, *Wi-Fi Location-Based Services 4.1 Design Guide,* 2008

/7./ C Yeh, H Lim; RSSI Measurements, IEEE 802.16 Broadband Wireless Access Working Group, 2004.

/8./ AeroScout T2 tags - http://www.aeroscout.com/content/T2, accessed January 2008.

/9./ Cisco Systems, Cisco 1800 Series Integrated Services Routers (Fixed) Software Configuration Guide, 2005.

/10./ Cisco Systems, Catalyst 3560 Switch Software Configuration Guide, 2004.

/11./ Cisco Systems, Catalyst Express 500 Series Switches Configuration Example, www.cisco.com, 2008.

/12./ Cisco Systems, Cisco Location Appliance Configuration Guide, 2007.

/13./ Cisco Systems, Cisco Wireless LAN Controller Configuration Guide, 2006.

/14./ Cisco Systems, Cisco Wireless Control System Configuration Guide, 2007.

Bojan Radulović
NIL d.o.o., Tivolska cesta 48, 1000 Ljubljana, Slovenija

(Former) Cisco Systems Slovenija,
Bravničarjeva ulica 13, SI-1000 Ljubljana, Slovenia

doc. dr. Janez Stergar
University of Maribor, Faculty of Electrical Engineering and Computer Science,
Smetanova ulica 17, 2000 Maribor
e-mail: janez.stergar@uni-mb.s

Prispelo: 21.04.2010 *Sprejeto: 03.03.2011i*