Int. J. Advanced Networking and Applications 2484
Volume: 6 Issue: 5 Pages: 2484-2486 (2015) ISSN: 0975-0290

Internet of Things (IoT) Applicability in a Metropolitan City

Dr. D Mohammed
Associate Professor with Saint Leo University in Florida
Email: dmohammed@lake.ollusa.edu

----------ABSTRACT----------

Internet of Things (IoT)is defined here as a network of interconnected objects. These objects can include several technological systems. This paper examines the wireless communication systems and IoT sensors. IoT is technically feasible today, allowing people and things to be connected anytime, anyplace, with anything and anyone. IoT privacy is a concern but security solutions exist today to solve these issues. A proposal is made to use secure IoT solutions in supporting the metropolitan needs in San Antonio, Texas.

Key word: Internet of Things, Privacy, RFID, Sensors

Date of Submission: September 05, 2011 Date of Acceptance: October 20, 2011

1. Introduction

The Internet of Things (IoT) is a concept of globally interconnected devices, objects and things. Generally it is thought of as a wireless network of sensors whose purpose is interconnecting all things. This technology includes bar codes, sensors, smart cards, and voice recognition. The IoT is not very known, and we need to start where innovativeness and demand is common. The place chosen is the progressive city government of San Antonio, located in state of Texas. The San Antonio City Council mandated that the metropolitan area has a validated government need to provide cultural amenities to the occupants of the city [1]. These amenities can be provided by private and public organizations. Additionally, these amenities should enhance the downtown area through innovativetechnology. IoT is a solution in thatthrough technology (anytime) it can enhance downtown (anyplace)cultural amenities(anything) for its occupants (anyone). So, our object is clear, we have a stated need and we have a solution that will incorporate IoT systems and concepts.

2. Architecture

The San Antonio Metropolitan IoT Architecture end goal is to employ amesh network. This network could employ various devices and networks as shown in Figure 1.

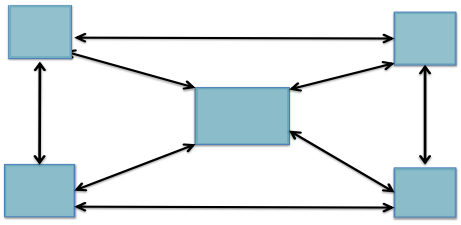
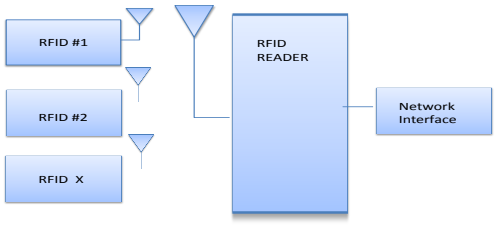


Figure 1 Mesh Network

Each entity, noted as a box in Figure 1, have a unique characteristics and each entity can be anything within the downtown San Antonio area. These entities can be public or private entities. This architecture seems simple enough but as of today IoT solutions has had limited success. The major obstacles of IoT are: entity sensor immature technology; limited internet addresses for all the places or things; and the availability of the wired internetin various cities [2]. Today's RFID IoTarchitecture as shown in Figure 2 is a simplistic today. Several components and standards will be required to insure privacy and implementation [3], [4], [5].



Current RFID Architectures
Figure 2

This architect entity requirement and their shortfalls include the following:

Volume: 6 Issue: 5 Pages: 2484-2486 (2015) ISSN: 0975-0290

Discovery - Entity or subcomponents of the entity can be discovered by any user. At a minimum, a user can be a tourist or a resident. Discovery shortfalls:

a. The sensor can be a Radio Frequency Identifier Device (RFID) which has no privacy.
b. Sensors can be cost prohibitive.

Any Object - Entity selected can be any object that promotes the downtown area. At a minimum this is any physical public or privately owned facility or object in the Riverwalk downtown area. Any object shortfalls:

a. The Internet Protocol 4 (IPv4) is the existing standard that limits IP addresses (2^{32}) which will be a grave systems issue forexpanding future sensors with IP addresses.
b. Investments can be delayed if addresses or objects are limited.

Communication - Entity must communicate with any user. Communication shortfall*s*:

a. The wired internet is not available to all citizens and has a direct impact in completing our mesh network using the network interface in Figure 1.
b. An unavailable internet limits the "anytime" definition.

Privacy -Any user data shall maintain a high level of privacy.The privacy shortfalladds more complexity, which at times is added after the fact, can be an overall architecture show stopper.

So if one look at an RIFD implementation issues and requirements addressed above, it will require extensive integration and design.

3.0 IoT Solutions

Below are the solutions for incorporating a future RFID architecture.

3.1. RFID Solution/Discovery

RFID's, also called tags can be active or passive. Passive is a tag without power and an active tag has a power source. The tag hardware consists if active, a battery, the integrated chip (IC), the antenna, and the enclosure. Since our application for the city includes pedestrians walking the Riverwalk, the tag requires a potential transmit range ofseveral feet. The passive tag hardware is a few inches in length which is ideal since this can be mounted in various cultural or commercial fixtures along the Riverwalk. Our RFID network in the Riverwalk downtown area would at a minimum consist of 100 RFID sites. The tag would require the maximum storage which is 512 bits, this equates to about 64 characters which can accommodate a short description of all current commercial or public points of interest. If a larger description is required then multiple tags can be daisy-chained.

3.2. IP Solution/Any Object

IPv4 is the current IP standard that can handle 4.3 million IP addresses. But today the new emerging standard is IPv6 which can handle approximately 2^{95}addresses. This meets our IP gap for RFIDs for the entire planet and as long as the RFID architect plans his network with IPv6 compatible devices, RFID employment should not be a problem.

3.3Wired InternetSolution

This addresses the Communication and Privacyshortfalls.Thoughwireless internet is convenient, for most robust locations wired internet is a solid requirement. The RFID architecture requires some form of data management central office. This is mainly for configuration control of data and insures privacy compliance standards are adhered. San Antonio is a hub for AT&T and the wired internet is not a problem for the city. If we say the city is wired for the internet and then the city would need to take some form of RFID data management responsibility.

4.0 IOT Components

For the RFID Component one can consider a current IC is the MONZA 4® from the Impingcompany which is apassive tag and transmits at 860 to 960 MHz (Class 0)which is defined by Electronic Product Code (EPC) Global and International Standards Organization(ISO) agencies. These tags transmit if it receives a magnetic field, this transmission can be generated by a near-field transmitter. A key issue here, a magnetic field decreases quickly in respect to distance. This is a natural inherent security deterrent since tags cannot be changed from a distance. The tag transmission distance is approximately 6 feet if using a traveling wave antenna. This distance meets our Riverwalk criteria since the side walk is rather narrow. The traveling wave antenna is critical since it can use the entire UHF frequency range, it does not have to be tuned to the reader and from an IoT advantage can be daisy chained.

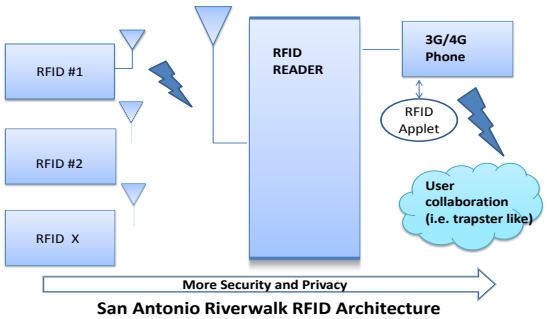
The tag that is required to insure privacy is defined in ISO 18000-6. This enables the owner to zerioze the tag bits structure, called the kill feature and is stated in part C of the ISO standard.A security issue for the San Antonio Riverwalk is individuals spoofing the tag. The countermeasure to this is killing the tag ifthe serial number has changed. Each tag has unique serial number. The tag owner would need to monitor the tag as needed to insure tag is valid. Identity theft is a grave concern these days with bad people doing bad things to other people but in terms of the tag information description, all this information is public information. So there is no risk in identify theft if the IC data or tag was stolen.

For the Internet Component, the issue on IP addresses is to make sure all devices connected to the RFID network follow an IPv6 standard. The protocol for RFIDs needs to be internet base which is defined by EPC Global.Currently, the RFID at the Physical layer uses a

Volume: 6 Issue: 5 Pages: 2484-2486 (2015) ISSN: 0975-0290

similar standard as the bar code industry. The main difference is that RFID's associate an object to a serial number and bar codes do not. At the datalink layer RFID's uses a tag protocol layer for HF or UHF Class 1 tags**.**

Considering the overall RFID components, figure 3 shows an RFID architecture that puts this in perspective. Figure 3 shows how a typical near field readercould be integrated with an IPhone. This particular reader works with active tags, in our example we used a passive tag. The IPhone would require an applet similar to Trapster. This would allows users to vote on speed traps. In our case, the user would click upon a tag intercept. The user can now annotate on a Riverwalk map the location and any other attributes defined by the applet.



San Antonio Riverwalk RFID Architecture
Figure 3

5.0 Conclusion

Data privacy and security with the IoT will be an ongoing challenge. However, based on the findings in this paper, a recommendation for a Riverwalk RFID Investment Plan should be drafted and presented to the San Antonio Planning Commission. After which one needs to obtain the City's approval to conduct an RFID demonstration along the Riverwalk in San Antonio, Texas. Upon a successful demonstration, recommendations should be made to consider the adoption of a long term implementation plan throughout theRiverwalk area in San Antonio, Texas.

References

[1]. San Antonio City Council, "San Antonio Master Plan Polices", City Council Minutes, May 1997.
[2]. Lamberth, L., "The Difference Engine: Chattering Boxes", The Economist, Aug 2010.
[3]. Gibbs, C., "Mobile Security and the Internet of Things", Gigaom, Aug 2010.
[4]. Webber, R., "Internet of Things – New security and privacy challenges", Computer Law & Security Review, Vol 26, 2010, pp. 23-30.
[5]. Mayer, C.P., "Security and Privacy Challenges in the Internet of Things", Electronic Communications of the EASST, Vol 17, 2009, pp. 1-17.

Author Biography

Dr. D Mohammed is currently employed as an Associate Professor with Saint Leo University in Florida. He currently teaches undergraduate and graduate level courses in Network Design, Information security, and Cyber security. He has worked extensively in both the public and private sectors to improve the security of their critical information systems. His research focuses on improving the security of network systems.