Security and Privacy Solution for I-RFID based Smart Infrastructure Health Monitoring

[1]Shailesh Kumar, [2] Byomakesh Mahapatra, [3]Rahul Kumar, [4]Ashok Kumar Turuk
Dept. of Computer Science and Engineering
National Institute of Technology, Rourkela
Rourkela, Odisha, India
Email: [[1]shaileshkumar478, [2] byomakesh22, [3]rahulchauhan533,[4]akturuk]@gmail.com

***Abstract*— The smart city and smart infrastructure is a new concept, for managing and controlling the different infrastructure of the city by integrating it with the internet and cellular network. The integration of Internet of Thing (IoT) with the cellular network again adds more scalability and reliability to the existing system. The recent development in the Integrated Radio Frequency Identification (I-RFID) sensor more securely sends sensor data to long distances through access point (AP) and base station (BS). This transmission needs some highly secure authentication and validation methods. In this paper we have present an I-RFID based cellular IoT (C-IoT) system and given its key security issue. We have proposed some algorithm for this system and the simulation result shows that this proposed algorithm is secure from various attacks and more useful in the practical scenario for C-IoT network communication in smart infrastructure health monitoring.**

Keywords—C-IoT, Radio Frequency Identification (RFID), Security, smart Infrastucture

I. INTRODUCTION

With the rapid growth of the world, population leads to an increase concert infrastructure, which needs a continuous monitoring and observation of this infrastructure in an intelligent way. A smart infrastructure can be pronounced as an infrastructure embedded with the sensor, actuator and some embedded digital devices. The sensor and actuators are connected through many communication protocols for real-time data acquisition and control application. Cambridge Centre for the smart infrastructure defines as an infrastructure which digitally enhances, and has potential to efficient use of the available resources. The smart infrastructure combines the existing physical infrastructure such as Transport, building, energy sources, waste and water with the new digital technology like sensor, IoT devices, core-networks, machine learning, big data, and GPS. Smart infrastructure gives a more cost-effective solution for the end user by improving intelligence and decision making at the service level. The smart infrastructure based on a feedback loop of data, and takes a decision based on this feedback information. The information collected from the sensor and different level of smart devices is analysed and processes them for the human operator to make a decision with or without human intervention. This collected data can be used in future, to design more accurate and efficient version of system architecture. As the number of smart devices increases, there is a rapid increase in the generated data which leads to network conjunction and increase in network delay. To overcome these limitations, the present network and cellular architecture required many changes from its present scenario. This paper focus on some solution for this limitation in term of the changes in the basic cellular architecture. At present cellular and wireless architecture, the base station (BS) is the key control unit for wireless and cellular communication. The increase in number IoT devices, V2V communication and mobile user leads to an increase in the number of BS. Study done by Cisco-VNI showed that the global data traffic has increased to 36EB in 2015 which is 0.24EB in 2010. At present around 4 million base stations serving worldwide to serve 100 million mobile users, [1] and expected to be increased to double its size till 2016. With the increase of data intensive operation in cellular network, power-consumption of each traditional BS reach up to 25MW with an estimated energy cost of $3,200, and emission of an 11 tones CO2 per annum. In most of the case the infrastructure maintenances of a smart city need a dedicated network, some smart people and some intelligent device. The continuous monitoring of an infrastructure like building, bridge and road by using a closed loop control monitoring system.

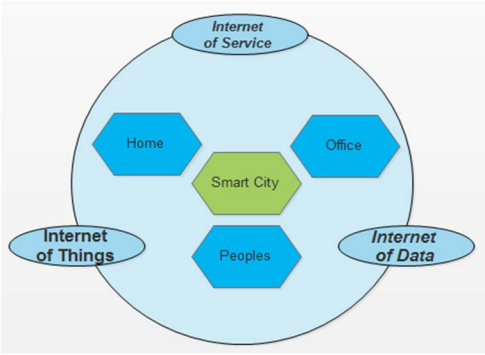

Fig. 1 Smart City concept and paradigm

Radio Frequency Identification (RFID) is a concept which enables an object or devices to recognize through radio

frequency signals automatically. RFID communication is fast and convenient. In an RFID basically two parts consists one is tag and other is reader. In the tag, it consists of an antenna and a chip. Tag and the reader communicate each other by the concept of electromagnetic reflection. A reader reads the identity of targeted object [2][3]. A reader achieves this by scanning tag attached to the targeted object. An RFID tag is a device which can be incorporated on an animal, person or thing. A reader can scan multiple tags simultaneously and further transmit it to the server. Common applications of an RFID systems are supply chain management, highway toll collection, controlling building access, public transportation, developing smart home appliances, animal tracking etc .

The main focus of this paper is to design a frame work and security protocol for the smart city which secures a closed loop system. We have proposed a RFID based IoT architecture for the infrastructural health monitoring for smart city.

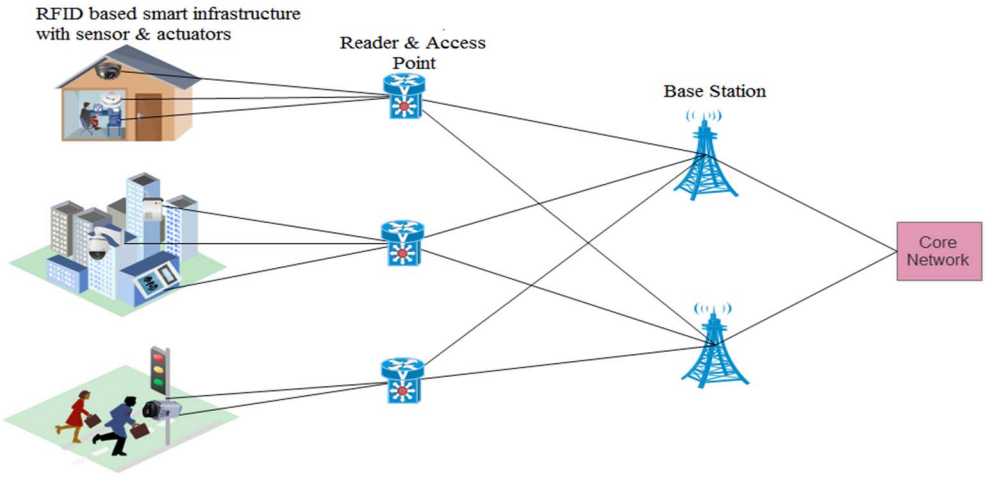

Fig.2. C-IoT network with its different functional units

Our contribution in this paper is summarized as below:

- We present a RFID based control system for the infrastructural health monitoring.
- We proposed a security protocol for this frame work for secure data access and transmission through the access point and communication link and core networks.
- We demonstrate the validation of this proposed method by using some simulation tools. This validation tools shows that this proposed method can be used in a practical scenario in an IoT based system.

The rest of the paper is organized as follows: Section II, describe detail architecture of the Cellular based IoT system. Section III, we have describe about the different challenges in RFID and C-IoT network. Section IV, descried about the proposed protocol and algorithm for RFID based cellular network. Validation of the proposed protocol and its simulation results is given in Section V, Finally a concluding remarks is given in the section VI.

A. *Prior works*

Smart city is a new concept comprising new and advance technology in term of smart infrastructure, delay aware communication networks and some automated monitoring and devices. Many researchers proposed and worked on smart city and smart infrastructure security. Authors in [5], the authors discussed about different security issues in the smart city and smart infrastructure which are generating huge amount of data. The paper focused about different capillary smart city solution for IoT and M2M connection. In [6], the authors describe about a future generation secure framework for smart city application, which is based on a multi-cloud and cloud federation approach. This used Elliptic Curve with a shorter key solution for security analysis. The advantage of this method is that it used very less memory space. A RFID based IoT system and its functionalities are described by the authors in [7]. In [8] and [9], the authors described about some mutual authentication procedure for a RFID system. They proposed new methods based on quadratic residue technique for RFID authentication. In [10] [11], authors proposed a light weight

and low-cost RFID authentication for RFID based for IoT system. In [12], authors proposed solution for hiding the information on the authentication and privacy process in the RFID system. In [13], authors proposed an authentication protocol for low-cost RFID system. In [14], authors describe the AVISPA tool for the automated validation of internet security protocols and applications. All the above papers well focused about the different security issue in RFID communication, but no one describe about the security issue in the integrated sensor based RFID communication properly. In this paper we have focus on some key issue and proposed solution for the IoT based RFID communication.

II. SYSTEM MODEL

The smart city consist of many smart infrastructure like smart building, smart road and other control and manage by millions of sensor and actuators connected by some highly dedicated network. Fig.2 shows a complete diagram for a C-IoT based smart city, which consist of different smart infrastructure like smart home with automated functioning device, smart road with real time traffic and road condition monitoring system, smart industries and offices with automated controller and data acquisition system.

The main functional unit of the C-IoT based structural health monitoring are divided into three main units such as.

A. *Sensor and data acquisition devices:* This unit consist of a number of sensor/ transducer along with the signal conditioning devices for the measurement of physical parameters in the smart infrastructure.

B. *Local access Points:* The localized sensor node connected to a local access point (AP) or a gateway with the help of low power communication links such as: Wi-Fi, RFID and long range Bluetooth links. This local access point/Reader work as a routing unit and made a bridge between the local sensor unit and base station (BS).

C. *Base station and core networks:* This unit consist of a large scale macro BS which operates in different band like, GSM, CDMA or LTE network. The controlling, data handling and data processing part are carried out by central unit. This central unit can be known as Main Switching Centre (MSC) or Evolved packet Core (EPC) unit in GSM and LTE network respectively.

D. *Interconnected Backhaul link:* The BS is connected to the MSC or EPC through a high speed core network known as backhaul link. This backhaul link generally designed by a dedicated large bandwidth optical cable or a high speed microwave link.

In this system model given in [4], which consist of an integrated sensor with an active RFID tag, a RFID reader which connected to a BS through a wireless link. Each sensor integrated with a thin-film RFID tag and measures a different physical parameter like small motion, vibration, proximity etc. This signal is integrated tag work as a general RFID tag having a unique IDs. The tag data is transfer to RFID reader which is connected to a DAQ system. The reader is control by a local controller and output is either storage in a local memory for references or sends to distances places by using cellular network.

III. CHALLENGES REGARDING PRIVACY AND SECURITY ISSUE IN C-IoT COMMUNICATION

As the number of wireless devices and connection increases the corresponding security challenges are increase at each and every level of the system. A well-designed system still having some common technical issues in a RFID tag based communication system like:

i. *Counterfeit reader attack tag*: This type of an illegal attacker's act as a legal tag. By using an unauthorized reader the attacker tries to retrieve different sensitive information from the source device.

ii. *Man-in-middle attacks*: This Type of attack generally occurs at the communication links, which exist between the tag and the reader. An unauthorized attacker randomly generates some raw signal and tries to jam the communication links and try to interpret the necessary message. The attacker can modify or temporarily holds message which is generally transformed from tag and reader.

iii. *Denial-of-Service (DoS) attack:* This is the most common attack found in any type of communication system where, an illegal attacker holds a fake tag IDs. He tries to send wrong and improper message to the RFID reader. Due to the illegal authentication a legal reader unable to connect to its corresponding device.

iv. *Impersonation attack:* In this type of attack an unauthorized reader who does not have the secret key and try to prove himself as a legal reader (tag) for accessing necessary information.

IV. WORKING MODEL FOR A INTEGARED RFID (I- RFID) SECURITY PROTOCOL

The objective of this proposed protocol is to preserve the privacy of the system as well as perform mutual authentication between RFID-reader and RFID-tag. The proposed scheme is divided into two phases: in the first phase, key-generation is performed and the second phase deals with identification and mutual authentication of tag and reader are performing.

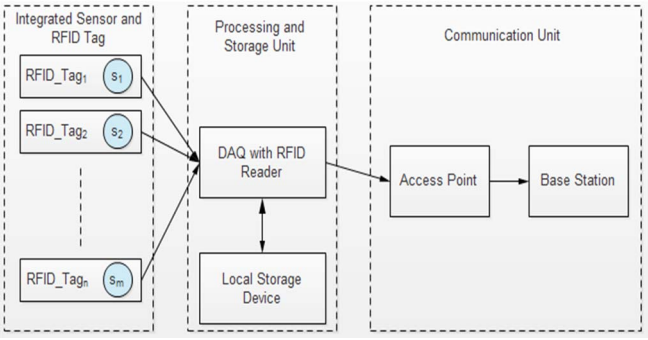

Fig.3. System block diagram for integrated-RFID communication process

a) Key Generation Process: In key generation process certain secret and encrypted key is generated for pairing and authentication purpose. The step by step algorithm represents the total key generation process in the RFID system.

***Algorithm*.1** RFID Key Generation

1. Generate Public-key ***(Pk)*** and Privet-key ***(Sk)***
2. Assign the tag to a unique id **IDs**
3. Set the status word ***(SW)*** to Zero [SW= "00000000"]
4. Generate random number for each privet tag **(T_i)** and are added to the system
5. For the tag **Ti** with **IDi** compute **Si**

$$S_i = \{\alpha_1, \alpha_2, \alpha_3 .....\} \quad \textbf{and} \quad \alpha_j = E_{pk}(ID_i \| random_i)$$

6. Random key **K_i** is chosen for the tag **T_i**
7. The pair **(Si, Ki)** is stored in the tag **Ti**
8. The pair **(IDi, Ki)** is stored in the database of the system

b) Identification and Mutual Authentication: First of all the reader identify each tag in its vicinity. The reader performs interrogating based on a walking tree singularity protocol.

Algorithm.2: Tag Identification Algorithm

1. Select a I-bit Identifier and use a leave of a binary tree of depth **I**
2. Select a node ***S***
3. The left child is ***S*||*'0'*** And right child ***S*||*'1'***
4. IF responses ***(r == 0)*** tag identifier is a left child
5. IF responses ***(r == 1)*** tag identifier is a right child
6. Continue searching for tag up to tag n^{th}
7. End process

c) Authentication: After identifying the proper tag, the second part is to authenticate the tag. Since the reader has the ID of each tag, the reader can exchange data with each tag avoiding a collision from another tag, the reader can exchange data with each tag avoiding a collision from each other tags in its vicinity. The reader and tag authenticate each other by using the following algorithm.

Algorithm.3 Reader and Tag Authentication Algorithm

1. Using the **α** value the reader sends a nonce value **Rr**
2. Tag compute **$Auth_T = f_k(\alpha||Rr)$** where **f_k** is a OWF
3. Tag generates a random nonce value **R_T** and send **<$Auth_T$, R_T>** back to reader
4. Reader computes **$Auth'_T = f_k(\alpha||Rr)$** and compares with **<$Auth_T$>** send the tag if doesn't match then halt (fake tag).
5. If match then both authenticate to each other, now the tag can shear its information with the reader

V. RESULT AND DISCUSSION

The above three algorithms represent a complete identification and authentication process in a small IoT application. We simulate the proposed RFID protocol using Automated Validation of Internet Security Protocols and Applications (AVISPA v 1.1) on a Linux OS environment on a system with ACPI X86 based with intel-i7 processor with 8GB RAM .

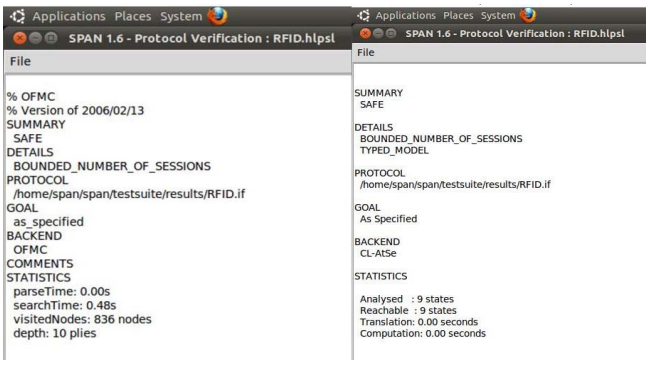

Fig.4. AVISPA result by the OFMC back-end and the CL-AtSe Back-end

We have used the OFMC and CL-AtSe back-ends of the AVISPA framework. Both the OFMC and CL-AtSe back-ends support analyzing protocols with XOR properties. They do it for a bounded number of sessions. The back-ends are called with the default options. Results have reported the protocol as safe, meaning that the stated security goals are verified by the OFMC and CL-AtSe back-ends for a bounded number of sessions and it clearly shows that there are no attacks possible on the I-RFID IoT system. We can thus deduct that the diagnosis of AVISPA security tools for this protocol is secure.

VI. CONCLUSION

The integration of I-RFID with C-IoT technology extends the range and scalability of IoT communication. The integration leads to different security issues at each level of the system architecture. This security issues can be overcome by proper design of the authentication system. The validation result give in this paper shows that the

proposed security protocol present in the paper is able to secure an I-RFID IoT network which is used in smart city environment.

REFERENCES

[1] A. Juels, "RFID security and privacy: a research survey," in *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, Feb. 2006.

[2] P. Ghosh, and T. R. Mahesh. "A privacy preserving mutual authentication protocol for RFID based automated toll collection system," *ICT in Business Industry & Government (ICTBIG), International Conference on. IEEE*, 2016.

[3] A. Shah, A. Pal, and H. B. Acharya, "The Internet of Things: Perspectives on Security from RFID and WSN," *arXiv preprint arXiv:1604.00389,* vol.12, pp.121-145, 2016.

[4] A. Mitrokotsa, and C. Douligeris, "Integrated RFID and sensor networks: architectures and applications," *RFID and sensor networks: Architectures, protocols, security and integrations*, pp. 512-514, 2009

[5] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, & D. Barthel, "Security and privacy in your smart city," *Proceedings of the Barcelona smart cities congress*, vol. 292, 2011.

[6] H. Djigal, F. Jun, and J. Lu, "Secure Framework for Future Smart City," *Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on. IEEE,* 2017.

[7] Lo, Nai-Wei, and Kuo-Hui Yeh. "Mutual RFID Authentication Scheme for Resource-constrained Tags," *Journal of Information Science & Engineering,* vol.26, pp.233-243, 2010.

[8] T. C. Yeh, Y. J. Wang, T. C Kuo, and S. S. Wang, "Securing RFID systems conforming to EPC class 1 generation 2 standard," Expert Systems with Applications, vol.37, pp. 7678-7683, 2010.

[9] Y. Chen, J. S. Chou, and H. M. Sun, "A novel mutual authentication scheme based on quadratic residues for RFID systems," *Computer Networks,* vol.5, pp.2373-2380, 2008.

[10] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Tapiador and J. C. van der Lubbe, "Security flaws in a recent ultra-light-weight RFID protocol*," arXiv preprint arXiv: 0910.2115*, 2009.

[11] Y. Tian, G. Chen, and J. Li, "A new ultralightweight RFID authentication protocol with permutation," *IEEE Communications Letters,* vol. 16.5, pp.702-705, 2012.

[12] R. Doss, W. Zhou, S. Sundaresan, S. Yu, and L. Gao, "A minimum disclosure approach to authentication and privacy in RFID systems," *Computer Networks*, vol. 56.15, pp.3401-3416, 2012.

[13] S. M. Lee, Y. J. Hwang, D. H. Lee and J. I. Lim, "Efficient authentication for low-cost RFID systems," *International Conference on Computational Science and Its Applications. Springer, Berlin, Heidelberg*, pp. 619-627, 2005.

[14] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P. C. Héam, O. Kouchnarenko, M. Mantovani, and S. Mödersheim, " The AVISPA tool for the automated validation of internet security protocols and applications," *International conference on computer aided verification,* pp. 281-285, 2005.