

Lightweight Three-factor Authentication and Key Agreement Protocol for Internet-integrated Wireless Sensor Networks

Dr. Prabhavathi S^[1], Hosapete Basavaraja^[2]

^[1] Professor, RYMEC Ballari, ^[2]M.Tech Student, RYMEC Ballari,

Abstract- *Wireless Sensor Networks (WSNs) will be integrated into the future Internet as one of the components of the Internet of Things, and will become globally addressable by any entity connected to the Internet. Despite the great potential of this integration, it also brings new threats, such as the exposure of sensor nodes to attacks originating from the Internet. In this context, lightweight authentication and key agreement protocols must be in place to enable end-to-end secure communication. Recently, Amin et al. proposed a three-factor mutual authentication protocol for WSN. However, we identified several flaws in their protocol. We found that their protocol suffers from smart card loss attack where the user identity and password can be guessed using offline brute force techniques. Moreover, the protocol suffers from known session-specific temporary information attack which leads to the disclosure of session keys in other sessions. Furthermore, the protocol is vulnerable to tracking attack and fails to fulfill user untraceability. To address these deficiencies, we present a lightweight and secure user authentication protocol based on the Rabin cryptosystem which has the characteristic of computational asymmetry. We conduct formal verification of our proposed. In order to demonstrate that our scheme fulfills the required security features. We also present a comprehensive heuristic security analysis to show that our protocol is secure against all the possible attacks and provides the desired security features. The results we obtained show that our new protocol is a secure and lightweight solution for authentication and key agreement for Internet integrated WSNs.*

KEYWORDS: Wireless Sensor Networks; Protocols etc.

1. INTRODUCTION

Wireless Sensor Networks will be the imminent part of the Internet of Things, will be targeted worldwide for any structure on the Internet. The power of this concatenation, conveys new dangers, such as sending sensors to attack news from the Internet. To provide secure communications, there should be a lightweight security policy and important agreements. One Internet thought for what's to come is that items and articles with the capacity to comprehend and convey will be coordinated into the Internet of Things (IoTs). As the Wireless Sensor Network (WSN) is one of the best advancements that bolsters basic abilities required for forthcoming applications, the coordination of WSN with the Internet will assume a significant job in the change of

future Internet reproduction. The Internet Force Task Force (IETF) has built up a stable of conventions and open measures for coordinating WSN into the Internet, for example, 6LoWPAN. As hub sensors (SNs) can be associated requiring little to no effort and remote innovation, for example, IEEE 802.15.4, and can likewise be associated with the Internet by means of the 6LoWPAN entryway. Consequently, sensors will be imparted worldwide to any Internet-associated association and in this manner empowered remote access to sensor information. Notwithstanding its extraordinary potential, the incorporation of WSN with the Internet likewise presents new dangers, for example, introduction to asset SNs and low remote connects to WSN in assaults utilized on the Internet. Given its affectability and affectability, tactile data in a hurry

ought to be ensured by a protected channel (E2E) in a safe channel among SN and a business outside WSN. The formation of such a channel requires legitimacy and key understanding components that permit two remote organizations to recognize and arrange classified keystrokes used to shield tangible information from different kinds of dynamic and virtual assaults. Note that in spite of the fact that WSN itself has lower safety efforts and system security administrations characterized by IEEE 802.15.4, Internet get to in any case requires affirmation and understanding arrangements to set up a protected E2E channel between these distributed correspondence frameworks.

2. OBJECTIVES

The lightweight and secure three-factor authentication protocol, based on the Robin crypto cyst, is subject to the official approval of the protocol proposed using ProVerif to demonstrate that it meets the required security features. In addition, a comprehensive security analysis to demonstrate this protocol can withstand all possible effective and deceptive attacks, including dealing with vulnerabilities identified in the protocol

3. SYSTEM DESIGN AND IMPLEMENTATION:

The system design and implementation involves different stages which include the brief description and step by step process.

LEVEL 1

The admin going to provide basic information about sensor like the sensor_id, name, port_no, system_name using this attribute create the sensor

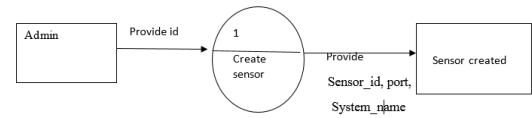


Figure 1: Admin login Diagram Level 1

LEVEL 2

In second level admin going to place the sensor based location latitude and longitude using sensor going fix that region.

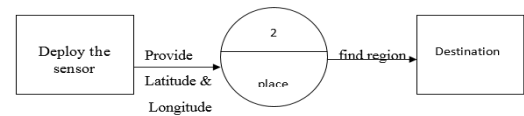


Figure 2: Data Flow Diagram Level-2

LEVEL 3

In this level admin will predict the gateway node based on all nodes latitude and longitude

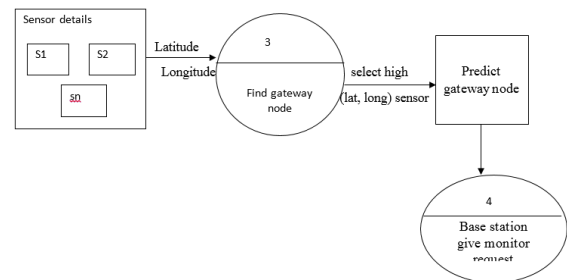


Figure 3: Data Flow Diagram Level-3

LEVEL 4

Sensor will update the monitored value to the gateway node and gateway will update to base station.

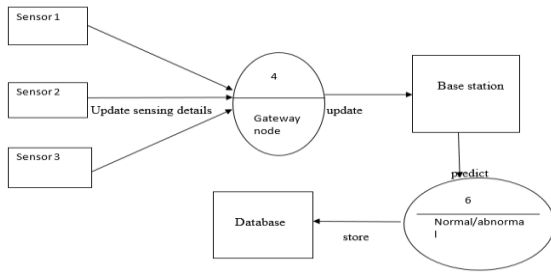


Figure 4: Data Flow Diagram Level-4

LEVEL 5

Registration:

User can be registered to the database and appropriate security level is provided by the admin to view sensor information.

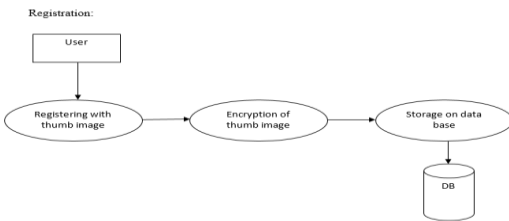


Figure 5: Data Flow Diagram Level-5

Thumb image is read from the thumb reader while registering the user, encrypted the thumb image for the valid registered user and then stored. When user want to login into system, thumb image is read from the thumb reader and compared with the stored image in the system already while registering the user. If it matches with the registered user and then user able to login to system.

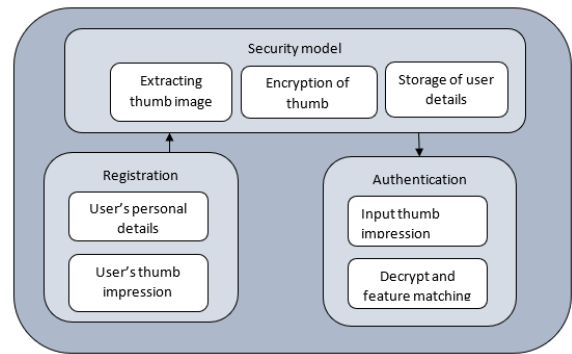


Figure 6: Thumb reading block Architecture

Authentication:

User needs to be logged into database with valid user credentials. These credentials are validated against the user credentials stored in the database. Once user authentication is validated, then user can able to view the sensor information based users security level provided by the admin at the time user creation.

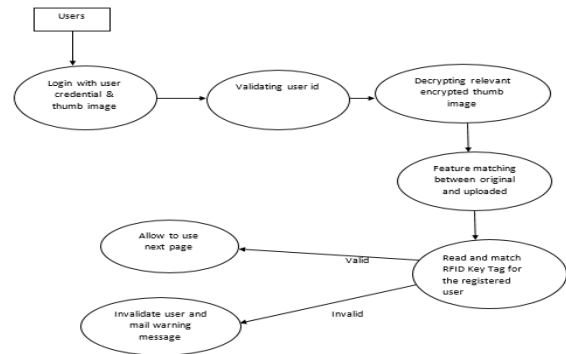


Figure 7: User Authentication diagram

4. HARDWARE AND SOFTWARE SPECIFICATION

Hardware requirements

Processor, Hard Drive, Monitor, RAM

Software requirements

Operating system : Windows XP/7.

Coding Language : JAVA, J2ee

Tool : NETBEANS 8.1

Database : MYSQL

5. RESULT AND ANALYSIS:

Result will be exhibited as below

Sensor creation: the admin going to create sensor using sensor_id, port_no, system_name using this parameter sensor created successfully. Based on place latitude and longitude, can be deployed the sensor based on people personal use or commercial use.

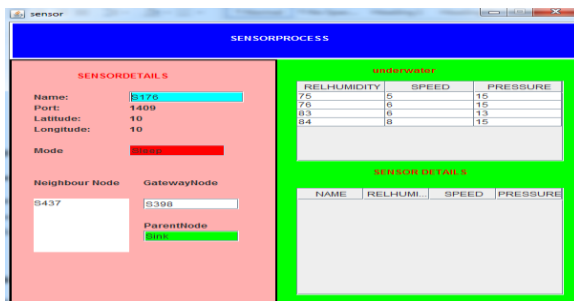


Figure 8: Sensor Creation

Neighbors Discovery: This module discover the neighbor sensor using have sine formula it take input of node latitude and longitude and neighbor sensor latitude, longitude. Compare to find distance between neighbor sensor and base sensor. Then check user mobility region when it is less than for source sensor mobility region discover the sensor as neighbour.

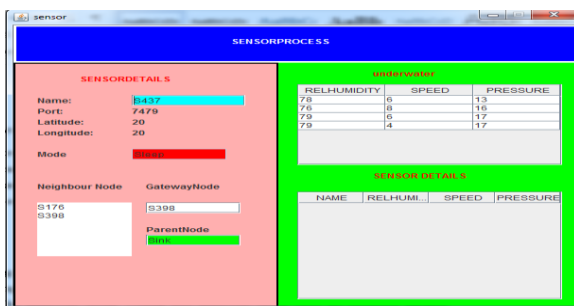


Figure 9: Neighbors Discovery

Gateway node: this module, creating the gateway node. First need to collect all the sensor details like each sensor latitude and longitude after collecting all sensor find highest latitude and longitude sensor that sensor elect as the gateway node. Using this gateway node only all monitor details update to base station

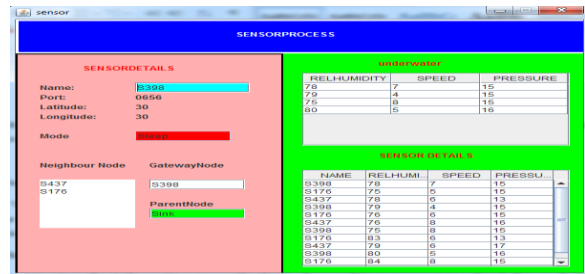


Figure 10: Gateway Node

User registration: With this module user want to register their own id after sending, user need to check whether that id is already exist or not. If not, consider as new id then user want to submit the thump impression and tag value, using that user can register.

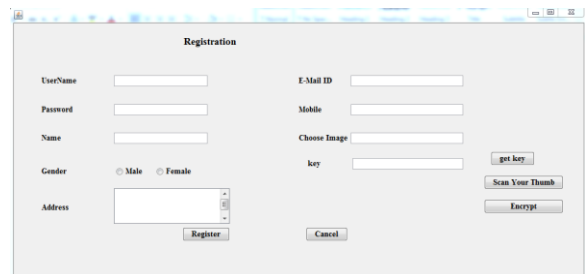


Figure 10: User Registration

View the information: User want to view the information mean the login. Logged in user want to submit the card id and their thumb using that thump, validate the existing database weather that is matched means allow to view the information otherwise invalid user like that system can block that particular request

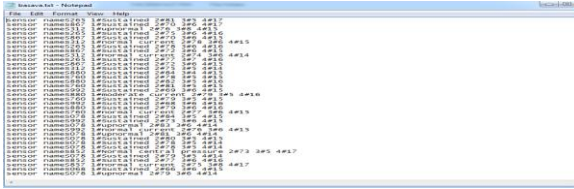


Figure 10: User Registration

6. CONCLUSION:

A three-pronged approach endorsed by Amin et al. It is pointed out that the security issues are affected by Type I & II SCLA. The user ID and password are fully encrypted with secrets deposited on the filched smart phone card and messages. In addition, there is a KSSTIA problem with the protocol, where temporary parameters are defined in the authentication system. Finally, the sixth law often detects an attack and fails to achieve user betrayal. Three-dimensional security and security system based on the Robin system. We demonstrate that the official confirmation of the suggested protocol using Pro Verification meets the required security features.

REFERENCES:

[1] B. Tang, Z. Chen, G. Hefferman, T. Wei, H. He, and Q. Yang, "A hierarchical distributed fog computing architecture for big data analysis in smart cities," Proceedings of the ASE BigData & SocialInformatics 2015, pp. 28:1—28:6, 2015.

[2] L. Sanchez, L. Muñoz, J. A. Galache, P. Sotres, J. R. Santana, V. Gutier-rez, Ramdhany, A. Gluhak, S. Krco, E. Theodoridis et al., "Smart-santander: Iot experimentation over a smart city testbed," Computer Networks, vol. 61, pp. 217–238, 2014.

[3] T. Ojala, "Open urban testbed for ubiquitous computing," in Communications and Mobile Computing (CMC), 2010 International Conference on, vol. 1. IEEE, 2010, pp. 442–447.

[4] R. N. Murty, G. Mainland, I. Rose, A. R. Chowdhury, A. Gosain, J. Bers, and M. Welsh, "Citysense: An urban-

scale wireless sensor network and testbed," in Technologies for Homeland Security, 2008 IEEE Conference on. IEEE, 2008, pp. 583–588.

[5] R. Clarke, Smart Cities and the Internet of Everything: The Foundation for Delivering Next-Generation Citizen Services, Cisco 2013