ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Smart RFID for Smart Grid Network

Anjana Krishna

Final year PG student, Dept. of CSE(Cyber Security), SNGCE Kolenchery, M.G.University, Kerala, India

ABSTRACT: Smart grid network supplies electricity to consumers via two way digital communication. This system allows for monitoring, control and communication within the supply chain. One of the enabling communication technology used here is Radio Frequency IDentification(RFID). Here I propose a mutual authentication protocol for securing the smart grid network from cyber-attacks. It provides multiple RFID tag communication simultaneously. Use of simple cryptographic operations and ALOHA protocol make it simple and Elliptic curve cryptography (ECC) and zero knowledge protocol make it stronger. Here I deployed a conjoined verification method for minimizing the cost in such a network. The proposed mechanism has better performance than other existing mechanism.

KEYWORDS: ALOHA protocol; Authentication; RFID system; Smart grid network

I. Introduction

The electrical grid has both utilities and consumers with the capability of monitoring, controlling and predicting energy use. Smart grid networks include various communication technologies, among them, Radio Frequency Identification (RFID) is considered as an enabling technology for realizing ubiquitous environment. A RFID system, which consists of RFID tags, RFID reader, and server, provides automated identification and information gathering from objects.

RFID tags communicate with the reader through open air in an automated, wireless manner. They have a small microchip on board that offer functionality that can be used for security purposes. In order to be successful for these security purposes, RFID tags have to be resistant against many attacks like cloning of the tag, man in the middle attack, Reader Impersonation attack, replay attack and forward secrecy.With secure authentication mechanism RFID communication can be used in protected areas.

We have proposed comprehensive mutual authentication protocol (CMAP)that incorporates hashed authentication tags as well as zero knowledge protocol based identifications. Here integrated authenticationtechnique is introduced in order to achieve conjoined validations in all three entities of the RFID based Smart grid network. And we use the ALOHA protocol for multiple tag communication. Use of this protocol prevents multiple tag collision attack. The proposed method is simple and easy to implement. It reduces the computational complexity and authentication cost.

II. Related work

RFID system has been widely used for various applications from supply chain management to home energy management. It can be observed that a concept of Internet of Things (IoT) visualizes the vision for bringing the Internet to any objects [1]. Thus, it can be seen that RFID can be considered as one of the utmost enabler technologies for massive IoT deployment [2].The application of RFID technology in Smart grid systems is increasing. Most significantly RFID is integrated in smart meters (power meters) [3, 4].In Smart grid environment, RFID is used for smart metering that includes realtimedata access, personal energy management, pre-payment, sealing smartmeter [5], and outage recording system [3]. Furthermore, RFID can be used to track smart meters for asset management.In mobile RFID (mRFID) networks, mobile RFID reader is used rather than fixed one. RFID-enabled smartphones, tablets, phablets, and personal assistant device (PDAs) can be used as mobile RFID readers for various mobile RFID applications. In traditional RFID systems, a communication channel between fixed RFID reader and backend server is assumed to be secure. Nonetheless, in mRFIDsystem, the communication channel between them being wireless, it is assumed to be insecure. It can be seen that such insecure channel is vulnerable to various threats such as eavesdropping, masquerading, replay attack and other active attacks [6]. Consequently, security and privacy issues in the mRFID systemare more challenging than the conventional RFID system [7]. Predominantly, works on authentication and privacy in RFID systems emphasizeon nishing security between RFID reader and RFID tags.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

However, for mRFID systems, security and privacy properties have to be realized for tag-reader communication as well as for reader-server communication. In recent days, certain authentication protocols were proposed for secure mobile RFID networks [4, 8,9].Due to enormous potentials, integration of RFID technology in smart meter has been rapidly realizing, for instance, RFID-based power meter [3] and RFID based e-seals for smart meter [5]. However, they do not reflect security and privacy issues.The security and privacy issues in the conventional RFID systems are well addressed and significant amount of works have been conducted. However, security and privacy considerations in emerging mobile RFID systems have just commenced [4].In case of Smart grid network, J. Chao et al.[10] provided ubiquitous solution using standard RFID technology and a security protocol deploying one-time password for user authentication. Nevertheless, it has high communication overheads. In case of generalized mobile RFID systems, Zhou et al.[11] proposed mutual authentication protocol based on public key cryptography using elliptic curve cryptography (ECC),whereas W.T. Koetal.[12] proposed modified version of Zhouet al. scheme that is suitable for security patrolling application. However, shortcoming with these schemes is that RFID tags have to perform a large number of expensive ECC computations for the mutual authentication.

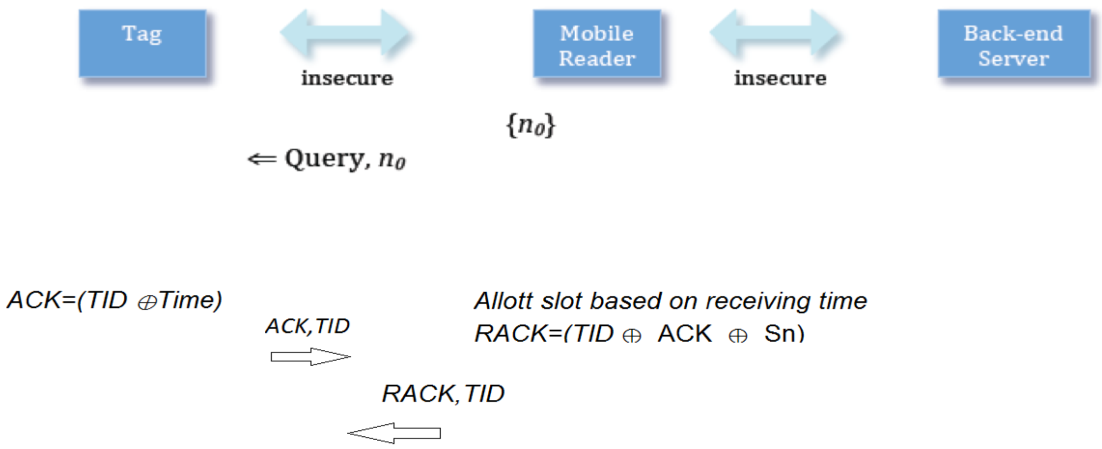
III. PROPOSED PROTOCOL

A. *Design Considerations:*

- Server is considered as authenticated.
- Wireless communication between tag, reader and server is insecure.
- RFID tag and Reader should be registered on the server prior to the communication.
- RFID Reader and server communication is based on public key cryptography.
- RFID tag share its original identity, secret information and secret key with the server at the registration time.
- Communication follows the ALOHA protocol.

B. *Description of the Proposed Protocol:*

Aim of the proposed protocol is minimize the computation and authentication cost along with increased security against wireless attack.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

RFID communication is initiated by RFID Tag, Which sendradio frequency signal to the surrounding. The passive RFID tag responds to the signal with some information. Reader finds the first replayed tag. And it gives priority number to each tag. Based on this priority we can avoid tag collision.

$$\{r_T, n_2\} \in Z_p$$
$$TID = h(ID||k_T)$$
$$\sigma_1 = r_T \oplus x \oplus k_T \oplus n_2$$
$$\Delta_T = h(ID||r_T||k_T||n_2)$$
$$TID, \Delta_T, \sigma_1, n_2 \Rightarrow$$
$$\{n_1, r_R\} \in Z_p$$
$$\kappa_S = \text{x-coord}(n_1 a_R . V_S)$$
$$Y_R = r_R.P$$
$$x_R = h(\Delta_T \oplus \kappa_S \oplus n_1)$$
$$g_R = r_R + x_R.a_R$$
$$TID, \sigma_1, n_2, Y_R, g_R, n_1 \Rightarrow$$
$$ID \in DB\ ?$$
$$\kappa_S = \text{x-coord}(n_1 a_S . V_R)$$
$$r_T = \sigma_1 \oplus x \oplus k_T \oplus n_2$$
$$\Delta_T = h(ID||r_T||k_T||n_2)$$
$$Y_R =?\ g_R.P - h(\Delta_T \oplus \kappa_S \oplus n_1).V_R$$
$$\{r_G, r_S, n_3\} \in Z_p$$
$$c_K = h(r_T \oplus r_G \oplus n_1)$$
$$Y_S = r_S.P$$
$$x_S = h(r_T \oplus c_K \oplus \kappa_S \oplus n_2)$$
$$g_S = r_S + x_S.a_S$$
$$\Delta_S = h(ID||c_K||k_T||n_2||n_3)$$
$$\mu_R = (r_T||r_G) \oplus \kappa_S$$
$$\mu_T = r_G \oplus k_T$$
$$\Leftarrow Y_S, g_S, \Delta_S, \mu_R, \mu_T, n_3$$
$$r_T||r_G = \mu \oplus \kappa_S$$
$$c_K = h(r_T \oplus r_G \oplus n_1)$$
$$Y_S =?\ g_S.P - h(r_T \oplus c_K \oplus \kappa_S \oplus n_2).V_S$$
$$\{r_A\} \in Z_p$$
$$\varepsilon_R = r_A \oplus h(c_K||n_0)$$
$$A_R = h(\Delta_S \oplus r_A \oplus n_2)$$
$$\Leftarrow A_R, \varepsilon_R, \mu_T, n_1, n_3$$
$$r_G = \mu_T \oplus k_T$$
$$c_K = h(r_T \oplus r_G \oplus n_1)$$
$$r_A = \varepsilon_R \oplus h(c_K||n_0)$$
$$A_R =?\ h(h(ID||c_K||k_T||n_2||n_3) \oplus r_A \oplus n_2)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

TABLE I. NOTATION USED IN PROPOSED MECHANISM

Symbol	Description
ID	Tag real identity
TID	Tag's pseudo-identity
P	EC base point
$\{a_I, V_I\}$	Private / public key pair of *I*; *R*- reader, and *S* –server
n_0, n_1, n_2, n_3	Nonce by reader, tag, and server
Δ_T, Δ_S	Partial commitment by tag and server respectively
r_T, r_G, r_A	Secret random by tag, server, and reader respectively
κ_S	Ephemeral shared key between reader and server
x	Secret information of a tag from server
k_T	Secret key of tag from server
h( )	One way hash function
c_K	Group secret
A_R	Integrated hashed authentication tag
g_R	Integrated zero knowledge protocol based authentication tag
g_S	Server-initiated zero knowledge protocol based authentication tag
x-coord(*k.P*)	x coordinate of *k.P*
||	Concatenation
$\oplus$	Exclusive-OR operation

IV. PSEUDO CODE

Step 1: Initial signal send by the RFID Reader
Step 2: Tag calculate ACK by XORing TID and Time. Then send ACK and TID to the reader
Step 3: Reader allot slot for each tag based on their response time. Securely send the slot number to the tag.
RACK is the XORed value of TID, ACK and slot number Sn.
Send RACK and TID to the Tag.
Step 4: Tag sends the pseudo identity along with other information for authentication.
Step 5: Reader collect these information and send it to the server and reader use public key cryptography for server side authentication.
Step 6: Server perform authentication process for both RFID tag and Reader.
Step 7: Upon receiving server message it validates both server and Tag.
Step 8: Finally the tag get message from reader and it validates both server and tag for secure communication.

V. SIMULATION RESULTS

The simulation of the above described protocol is done in the .Net framework. Protocol successfully executed in this environment. By analyzing this protocol we can understand it prevents many wireless attacks and it can provide higher security to the smart grid network.It can prevent man in the middle attack, replay attack, tag anonymity, reader impersonation attack, and multiple tag collision attack. Another advantage is reduced computation cost and authentication cost.

RFID communication protocol should be executes by the actual RFID system. But the lack of RFID tag with processing capability makes it difficult. Actual implementation work is in progress. In the simulation study we tried to perform Tag anonymity attack and reader impersonation attack. It results, the protocol successfully prevent these attacks.

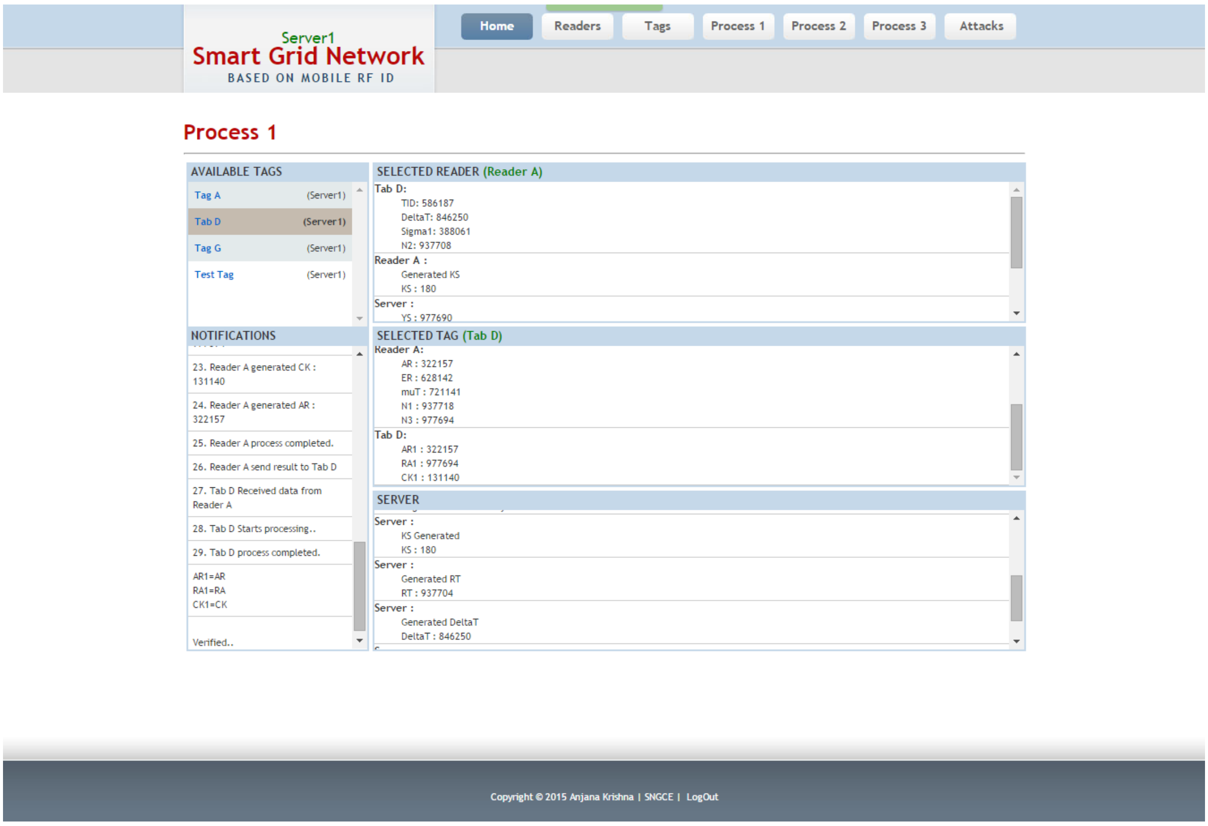


Fig1: Single tag communication with reader under same server

Fig.1 shows the protocol communication of different RFID tags under the same RFID server. Here we should select an RFID reader for reading the tags under its range. The selected reader sends signal and the tags under its range responds to the signal. It displays all tags and we can select any of the tag for communication. If the tag and reader are valid entities communication will be a success. Here we can't perform multiple tag communication. To overcome this problem I suggest a new solution, that is the use of ALOHA protocol. That helps to perform multiple tag communication. Fig.2 shows multiple tag communication.

Fig.2 is the execution of same protocol but it takes the advantages of ALOHA protocol. It prevents the multiple tag collision attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

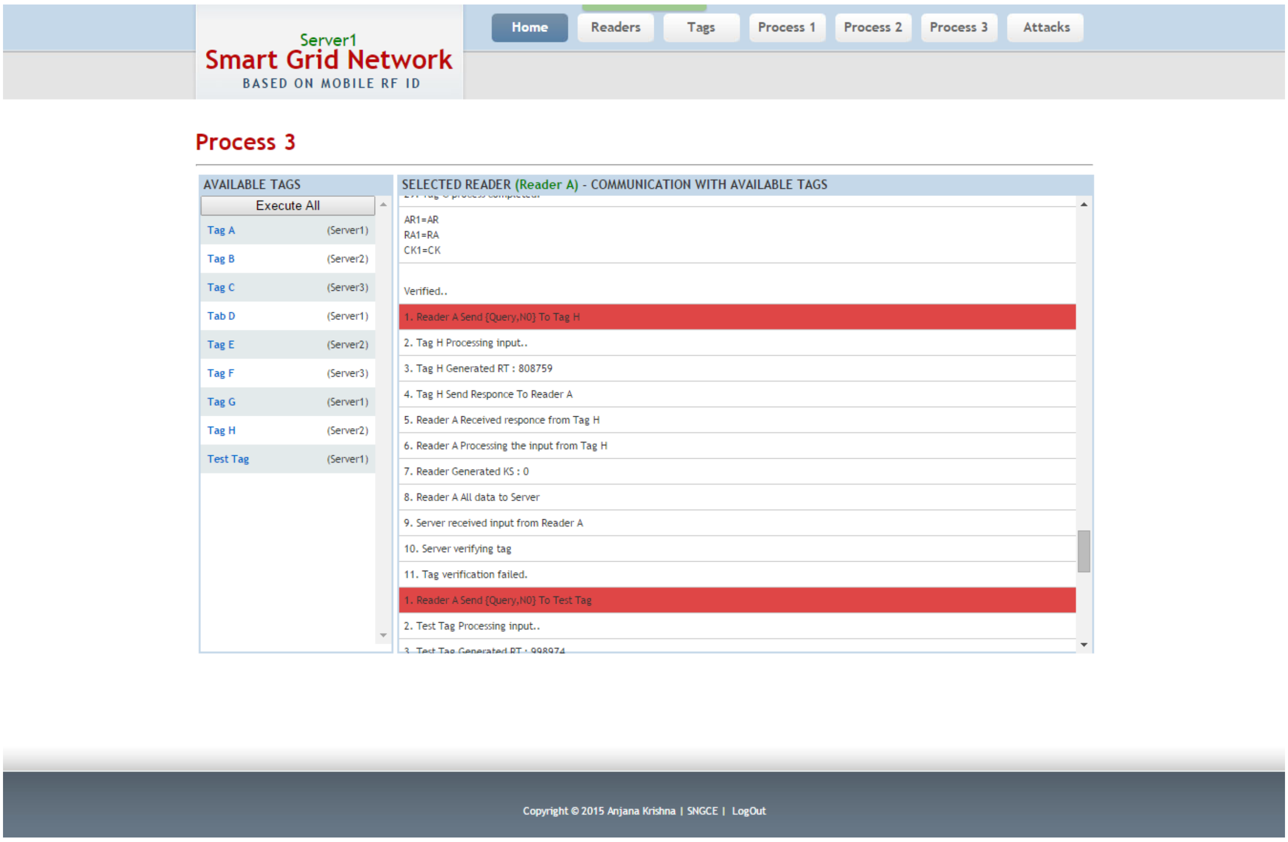


Fig2: Multiple tag communication without any collision

VI. CONCLUSION AND FUTURE WORK

The simulation results shows that the proposed mechanism have better performance in preventing wireless attacks. And it is suitable for smart grid communication. The use of simple cryptographic operations, ECC (Elliptic Curve Cryptography),zero knowledge protocol, ALOHA protocol are made it secure and simple. It should be applicable in high security needed areas. Real time implementation of this work is our future plan.

REFERENCES

1. J M. Darianian, M.P. Michael, "Smart Home Mobile RFID-based Internet-Of-Things Systems and Services", In Proc. of International Conference on Advanced Computer Theory and Engineering (2008) 116-120.
2. T.Y. Wu, G.H. Liaw, S.W. Huang, W.T. Lee, C.C. Wu, "A GA-based mobile RFID localization scheme for internet of things", Personal and Ubiquitous Computing 16 (2012) 245–258.
3. S.W. Luan, J.H. Teng, S.Y. Chan, M.C. Tsai, "An RFID-based power meter and outage recording system", Journal of the Chinese Institute of Engineers 35:7 (2012) 909-919.
4. R. Doss, S. Sundaresan, W. Zhou. “A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems”, Ad Hoc Networks 11 (2013) 383–396.
5. J.C. Lu, Y.Y. Chen, J.M. Wang, J.K. Jan, C.C. Chen, Y.L. Lai, "Study and Implementation of RFID Eseals for Power Meters", In Proc. Of International Conference on Innovations in Bio-inspired Computing and Applications (IBICA) (2011) 352-355.
6. A.K. Bashir, S.H. Chauhdary, S.C. Shah, M.S. Park, "Mobile RFID and its design security issues", IEEE Potentials 30:4 (2011) 34-38.
7. M.H. Yang, "Lightweight authentication protocol for mobile RFID networks", International Journal of Security and Networks 5:1 (2010) 53-62.
8. H.C. Lee, T.Y. Eom, J.H. Yi, "Secure and Lightweight Authentication Protocol for Mobile RFID Privacy", International Journal on Applied Mathematics & Information Sciences 7:1 (2013) 421-426.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

9. J. Zhuo, Y. Zhuo, F. Xiao, X. Niu, "Mutual Authentication Protocol for Mobile RFID Systems", Journal of Computational Information Systems 8: 8 (2012) 3261-3268.
10. J. Cho, M. Chung, K. Choi, Y. Lee, J. Moon, "Enhanced Security Protocols for EPC Global Gen2 on Smart Grid Network", In Proc. Of International Conference on Ubiquitous Information Technologies and Applications (CUTE) (2010).
11. J. Zhuo, Y. Zhuo, F. Xiao, X. Niu, "Mutual Authentication Protocol for Mobile RFID Systems", Journal of Computational Information Systems 8: 8 (2012) 3261-3268.
12. W.T. Ko, E.H. Lu, S.Y. Chiou, H.K.C. Chang, "A Mobile RFID-based Mutual Authentication Protocol using Elliptic Curve Cryptography for Security Patrolling Application", Cryptology and Information Security Series 8 (2012) 63-71.

BIOGRAPHY

Anjana Krishna is final year M.Tech student of Sree NarayanaGurukulam College of Engineering, Kolenchery, Ernakulam. She received B.Tech degree in 2013 from M.G.University, Ernakulam, Kerala, India. Her research interests are Security protocols, Cyber forensics, Ethical Hacking etc.