© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Novel Approach for Authentication of RFID Devices

Suthar Monali, Prof. Alka J Patel
IT Department, LDCE, Ahmedabad, Gujarat, India

ABSTRACT

RFID is a wireless technology for automatic identification and data capture and it's the core technology to implement the internet of things. Because of that, the security issue of RFID is becoming more important. In past , simple mathematical and logical method, hash based schemas and simple PKI schemas are introduce RFID authentication . In this paper we illustrate about the possible security attack on RFID and introduce a novel approach using pre computing function and also discuss security analysis.

Keywords: RFID, Reader, Tag, Backend Sever , Authentication , Security , ECC.

I. INTRODUCTION

RFID system is composed of tags, readers, backend sever, and antennas. RFID tags are available in affordable charges, wireless devices which can be communicate with RFID readers [1].RFID architecture shown in **figure 1** which consist tag, reader and back-end server. Tag consist EPC (electronic product code) which store details about tag. Reader is responsible for reading and writing tag information. Back end sever will save all data about tag which are in one group .Communication in RFID network will start on reader broadcast message or query. Communication between tag-reader and reader-server is in insecure channel.

In this paper we first analyse security attack possible on RFID and discuss RFID device performance measurement in section II, literature survey discuss in section III, proposed schema discussed in section IV. Security analysis discussed in section V. Comparison shown in section VI.

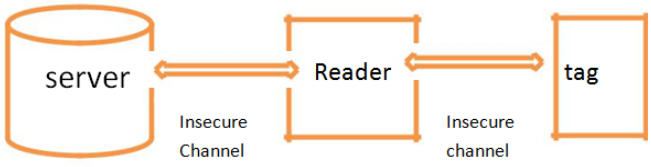

Figure 1

II. SECURITY ATTCK ON RFID AND PERFORMANCE MEASUREMENT

Denial of Service (DOS) : In both of wireless and wired communication, there are Denial of Service (DOS) . Once attackers control a large number of fake readers and tags, they can make the data connection to abuse computational resources, and even use up the resources and network bandwidth.[1]

Eavesdropping: The communication channel between the tag and the reader can be eavesdropped, because the radio frequency channel is not secure communication channel .[2]

User privacy : The attacker can monitor the tag using the tag identifier in order to know the user's behaviour, when the user identity is linked to a certain tag. Also, the attacker can trace the user location with the tag identifier, when the output of the tag such as the tag identifier is unchangeable.[2]
Replay attack : The attacker obtains messages between the tag and the reader by eavesdropping and reuses the message in order to impersonate a legitimate tag or a legitimate reader.[2]

Spoofing attack : The attacker impersonates a reader, sends a query to a tag, and then obtains the response of the tag. When the legitimate reader queries the tag, the attacker will send the obtained response to reader in order to impersonate the tag.[2]

Cloning attack : An attacker can build a cloned tag which will be interpreted by the reader as the legitimate tag, due to the fact that most tags are not tamper-proof.[2]

PERFORMANCE MEASUREMENT

RFID schemes cannot use computationally intensive cryptographic algorithms for privacy and security because tight tag cost requirements make tag-side resources (such as processing power and storage) scarce .[3]

Capacity minimisation: The volume of data stored in a tag should be minimised because of the limited size of tag memory

Computation minimization: Tag-side computations should be minimized because of the very limited power available to a tag.

Communication compression: The volume of data that each tag can transmit per second is limited by the bandwidth available for RFID tags [3]

Scalability: The server should be able to handle growing amounts of work in a large tag population. It should be able to identify multiple tags using the same radio channel [3] Performing an exhaustive search to identify individual tags could be difficult when the tag population is large [3]. Conclusion and future work discuss in section VII.

III. LITURATURE SURVEY

RFID has various advantages over EPC code. However, it has various security risks. To avoid cloning attack[11], proposed authentication protocols for RFID system based on PUF (Physical Unclonable Function) which is innovative circuit primitive to derive a secret from complex physical characteristics of ICs rather than storing the secret in memory. It has drawback that this algorithm has to compute HMAC for five times , therefore back end server should more powerful[2]. More recently Hash base authentication[2],[3] are studied this algorithms provide security against several attacks and have advantage that there is no worry about key security. Authentication algorithm for low cost RFID tag[4] is not secure against cloning attack. Authentication algorithm using elliptic curve cryptography [4],[5],[6],[7],[8] which introduce PKI system in RFID . elliptic curve cryptography is more suitable PKI because security level with key size 160bit in ECC is equal to key size with 1024 bit in RSA . ECC-based RFID authentication scheme integrated with ID-verifier[4] which will work on two point function , one is point function on elliptic and other one is random number function. there are several algorithms which is more powerful ten ID verifier [4]. The total computation of the improved protocol seems to be high for a RFID system. Therefore, reducing the computational cast especially for tag side is our future work. It can be achieved by using pre-computing technics[5].

This paper proposes a novel approach based on pre computing technique. The proposed approach is divided in two phase one setup phase and authentication phase. In setup phase this proposed algorithm use certificate authority as new entity which will generates certificate_id using identification of reader and identification of tag. Authentication phase will only compute a point function and search operation in list of certificate , therefore computation will decrease.

IV. PROPOSED SCHEMA

Proposed algorithm perform in two phase, setup phase and authentication phase. Flowchart is define in below figure. The step of algorithm is define as follow:

Algorithm :

Setup phase :

Step 1: reader will send its ID to CA

Step 2 : tag will send tag ID to CA

Step 3 : CA generate CA_ID using tag Id and reader ID

Step 4 : CA will send CA_ID to tag

Step 5 : CA will send list of certificate to reader

Authentication phase :

Step 1 : reader send request message with random number R1

Step 2 : tag generate =P($CA_{tag} \oplus$ (R1||R2))

Step 3 : tag send reader n_{tag} , reader check n_{tag} for all list , if found then tag is authenticated.

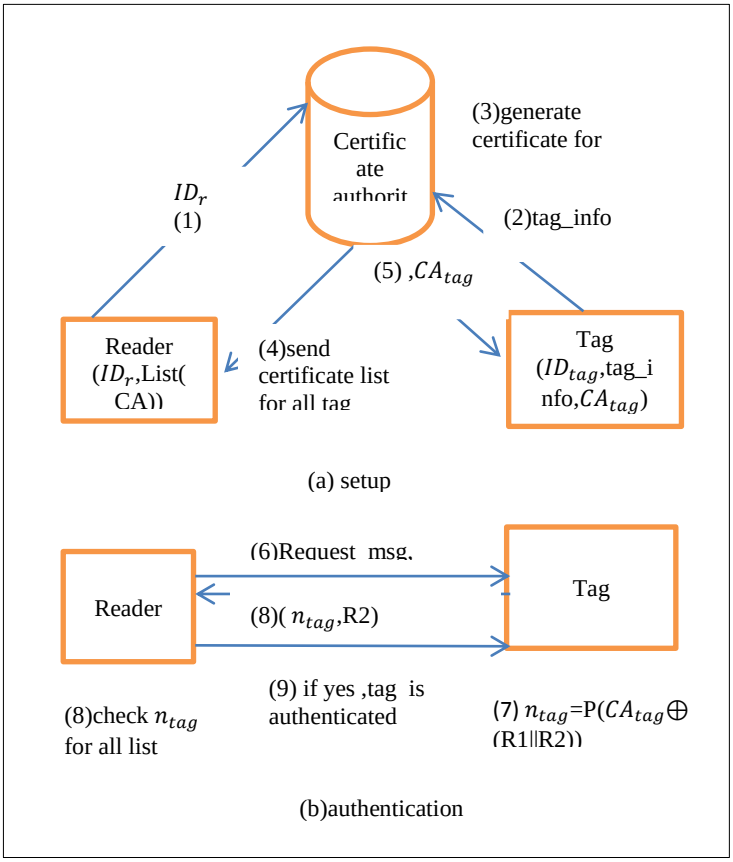

Table 1. Notation

Symbol	Meaning
ID_r	Reader identification
CA_{tag}	Certificate of tag H(ID_r||ID_{tag})
ID_{tag}	tag identification
List(CA)	List of certificate for group of tag
n_{tag}	
R1,R2	Random number
$\oplus$	XOR
CA	Certificate authority

V. SECURITY ANALYSIS

privacy protection : a tag never sends its own id to anyone, not even to the authorized reader. It sends its reply in disguise so that only an authorized reader can identify itself. Moreover no one is able to infer or learn the id of the tag by simply looking at the tag replies or by simply querying the tag.

Tracking: By incorporating R2, our protocol become secured against tracking as attacker can not predict R2. Consequently Tj will reply a new pseudorandom number each time it is queried.

Cloning : whenever the adversary queries Tj, it gets a different response because of R1 and R2. Now ifplaces this response in T, it will never be able to fool a valid R. When T is queried by R, T cannot generate the actual response. This is because, for each query, R will now transmit a new R1 that attacker cannot predict.

DoS : eliminates the need of a back-end server. So synchronization between the server and the tag is not required and a reader has to communicate with the back-end server only to get its contact list.

Eavesdropping : Attacker cannot launch privacy attack as the protocol does not reveal any sort of private information of the tag and the reader. Even attacker fails to track T because each time T is queried, it replies with a new pseudo-random number. Thus attacker can not figure out any signature to follow T.

Physical attack : tag use random number at every time to generate n so its not possible to get tag info by physical attack.

Server spoofing : this approach is server less approach, here only certificate authority which is trusted third party , so server spoofing is not feasible.

VI. COMPARISSION OF SECURITY ATTACKS

Attacks	Jung's [2]	Boyeon's [3]	Liao's [4]	Farash's [5]	God or's [8]	Ours
Replay	Yes	Yes	Yes	Yes	-	Yes
Dos	-	Yes	Yes	-	No	Yes
Server Spoofing	Yes	-	Yes	-	-	yes
Mutual Authentication	Yes	-	Yes	-	Yes	Yes
Cloning	Yes	-	Yes	-	-	Yes
Physical Attack	Yes	-	-	-	-	yes
Eavesdropping	-	-	-	-	yes	yes

VII. CONCLUSION AND FUTURE WORK

In the literature we discussed authentication based on simple PKI, simple HASH, AES and RSA and ECC . PKI is not suitable to RFID system because of key size and key management .HASH and HMAC need more computation[3]. AES is quite complicated . In our proposed schema we divide authentication process in two phase setup phase and authentication phase which will reduce computational power and time by occupying only one hash function at setup phase and simple random number and bitwise XOR at authentication phase. In future we implement this algorithm with RFID application.

VIII. REFERENCES

[1]. Xiao Nie, Xiong Zhong "Security In the Internet of Things Based on RFID: Issues and Current Countermeasures" Proceedings of the Published by Atlantis Press, Paris, France.

[2]. Seung Wook Jung , Souhwan Jung " HRP : A HMAC-based RFID mutual authentication protocol using PUF" , ICOIN 2013, IEEE publication , pp 578-582.

[3]. Boyeon Song , Chris J Mitchell " RFID AuthenticationProtocolfor Low-cost Tags" WiSec'08, March 31–April 2,2008,Alexandria, Virginia, USA

[4]. Yi-Pin Liao , Chih-Ming Hsiao "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol " Department of computer science and information engineering , St.John's university,Taipei,ROC (2013), published by ELSEVIER, http://dx.doi.org/10.1016/j.adhoc.2013.02.004

[5]. Mohammad Sabzinejad Farash " Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptograph" published by Springer Science+Business Media New York 2014, DOI: 10.1007/s11227-014-1272-0

[6]. C.P. Schnorr," Efficient identification and signatures for smart cards", in: Gilles Brassard (Ed.), Advances in Cryptology – CRYPTO'89, Lecture Notes in Computer Science, 435, Springer-Verlag, 1989, pp. 239–252.

[7]. ChouJS(2013)" An efficient mutual authentication RFID scheme based on elliptic curve cryptography" .J Supercomput. doi:10.1007/s11227-013-1073-x

[8]. Gy6z6 Godor, Norbert Giczi, Sandor Imre Dr."Elliptic Curve Cryptography Based Mutual Authentication Protocol for Low Computational Capacity RFID Systems -Performance Analysis by Simulations", Department of Telecommunications, Budapest University of Technology and Economics Magyar Tud6sok korutja 2., Budapest, Hungary H-ll17, 978-1-4244-5849-3/10/$26.00 ©2010 IEEE