# Mutual Authentication Protocol Using a Low Power in the Ubiquitous Computing Environment

*Young-bok Cho, Dong-myung Kim, Sang-ho Lee

Dept. of Network Security Laboratory Chungbuk National Univ.

Email : {bogi0118@netsec.cbnu.ac, dmkim@mail.ddc.ac.kr, shlee@netsec.cbnu.ac.kr }

**Abstract**: Ubiquitous sensor network is to manage and collect information autonomously by communicating user around device. Security requirements in Ubiquitous based on sensor network are as follows: a location of sensor, a restriction of performance by low electric power, communication by broadcasting, etc. We propose new mutual authentication protocol using a low power of sensor node. This protocol solved a low power problem by reducing calculation overload of sensor node using two steps, *RM(Register Manager)* and *AM(Authentication Manager)*. Many operations performing the sensor node itself have a big overload in low power node. Our protocol reduces the operation number from sensor node. Also it is mutual authentication protocol in Ubiquitous network, which satisfies mutual authentication, session key establishment, user and device authentication, MITM attack, confidentiality, integrity, and is safe the security enemy with solving low electric power problem.

**Keywords**: Ubiquitous Computing, Authentication.

## 1. Introduction

Ubiquitous computing is a diverse and convenient approach to serve human beings with an innovative technology. Also its sensor network technology including perception and control of human's external environment is actively under development. This report provides LPMA(Low Power Mutual Authentication) Protocol, considering low power which is saved in the batteries of each sensor node in Ubiquitous computing environment. LPMA Protocol which consists of RM and AM enables us to have the safe communications by conducting the minimum calculation process under a limited sensor node and also by issuing secured session key with mutual authentication. The rest of this paper is organized as flows. We describe the related work in section 2. we discuss our approach of *LPMA* Protocol in section 3. the evaluation *LPMA* Protocol in section 4. our conclusions in section 5.

## 2. Related Work

Ubiquitous computing consists of the technologies such as Ubiquitous Flexible Broadband, Ubiquitous Teleportation, Ubiquitous Agent, contents, Ubiquitous Platform, and Ubiquitous sensor network. Among them, Ubiquitous sensor network is the components that collect and manage information by having the user's peripheral communication with others.

### *1) Ubiquitous Sensor Network*

The sensor network consists of a lot of micro-devices and each device is called the sensor node. These sensor nodes are powered by battery connection and are able to do data-processing and a short-range wireless communications. As the range of applications of the sensor network has been increased, the importance of its security also has been emphasized. Communications must be encrypted and authenticated to provide a certain level of securities in the sensor network. This can be solved by installing a session key between the sensor nodes for better communications. However, the sensor node is operated by limited electrical power in a battery, so it is not appropriate for a sensor node to use unnecessary power to secure a higher level of securities.

### *2) Ultra Light, and Low Power Encryption Technology*

There have already been a lot of ultra light, and low power encryption research fields focusing on low power of sensor mode. [5,6] is one of the most representative technologies in ultra light, and low power encryption research fields which evaluated the speed of various hard platforms these studies tried to solve the low power of the sensor node by using the faster encryption algorism.

However, doing a lot of operations affects the overload and power over-consumption of the sensor node, although we use the faster encryption algorism. [5,6] is symmetric key way and fits well on ultra light, and low power settings such as motes of 'Smartdust' or RFID. [7] implemented Rabin Ntru with low powered public key encryption which can be loaded in the sense node Robin scheme is one of the forms of RSA which was suggested by Robin in 1979 and gave a solution to the difficulties of understanding in factorization. Also Ntruencrypt was suggested and gave an solution to

SVP(Shortest Vector Problem) by Hoffestein, Pipher, Silverman in 1996.

### *3) Security Protocol*

SPINS(Security Protocols for sensor networks) developed by UC Berkely consists of μTESLA and SENP where there is a limited access to resources in wireless communications. SPINS which is one of the symmetric functions provides encryption, access code, random number generation and has a lower communication overhead due to the allocation of 8Bytes messages for MAC. Also, it focused on improving the efficiency of data algorism and issued a node when master key was saved in the sensor node.

SPINS uses a one way hash chain of μTESLA. Even though SPIN also makes MAC key by separating time and broadcasts, hash chain is consumed quickly, when there is a short period making Mac key. Also, separating time zone brings out big power consumption in a whole network.

### *4) Home Network based on the Sensor Node*

Home network is one of the crucial parts of Ubiquitous computing, One of the studies revealed in Korea shows the efficiency of home network based on the sensor node and the protocol which uses Feige-Fiat-Shamir authentication. This protocol consists of 5 steps; service registration, the initial sensor registration for temporary group installation, installation of temporary group, service request for temporary group, and deletion of temporary group. Even if we can ensure the securities by using module operation, it can also give some calculation burden to the sensor node.

Furthermore, Feige-Fiat-Shamir authentication inherently has a lot of length of keys. The longer it has, the more burden on the sensor node will be. Therefore, to decrease calculation burden on the sensor node, it's advisable that we use both faster encryption algorism and conduct lesser operations.

## 3. LPMA(Low Power Mutual Authentication) Protocol

The security requirements for Ubiquitous computing in this study are classified to the location of sensor, limited capacity by low power communications by broadcasting, Among them, and this study suggests LP*AM* protocol to consider the limited capacity by low power.

### *1)Outline*

This study suggests *LPMA* protocol. It also tries to use the advantages of ultra light, and low power encryption, and at the same time tries to minimize the number of operations to decrease the burden on the sensor node.

We divide *LPMA* protocol into *RM* and *AM* so as to use registration and access process. The following are a few requirements to conduct protocol in this study

*First, we assume AM (Authentication Manager) between subsystems communications considers the limited sensor network environments.*

*Second, once authenticated, there would be no further authentication process until its completion of communications. (When it tries to communicate with another sensor node based on a different RM, it requires a new authentication process.)*

*Third, the parameter of the sensor node has ID, PW, and TS in the process of registration and has ID, PW, TS, and PK in the process of authentication process. At this time, each parameter is allocated as many as 16bytes memory.*

Based on the requirements above, System count for registration and authentication of *LPMA* protocol is defined in Table 1.

**Table 1. Notation**

| *Notation* | *Meaning* |
|---|---|
| *Entity* | *Sensor Node* |
| $ID_A$ | *Identification of Node A* |
| $PW_A$ | *Password of Node A* |
| $Sig_A$ | *Signature of Node A* |
| $IDK_A$ | *Hash of ID* |
| $PK_A$ | *Private key of Node A* |
| *TS* | *Timestamp* |
| $SK_A$ | *Session key of AM and each Node* |
| $PIN_{Adiv}$ | *Device number of Node A* |

### *2) Registration Process*

All sensor nodes in Ubiquitous Computing request for information registration through *RM* in the network. One can register the user and device information together in the process of registration and make a private key by using this information.

The following are the process of private key issuance.

(1) Node A requests *RM* for the registration by sending its information through Function.

$Node\ A \rightarrow RM : f(ID_A \| PW_A \| PIN_{Adiv} \| TS \| Sig_A)$

( Function operates all the information given by XOR )

(2) It is accepted as the initial registration when *ID* and *PIN* are not searched by *RM* through *InfoDB*, and make *IDK* and a private key.

$RM : IDK = h(ID \| PIN)$

$PK = h(IDK \| PW)$

(To avoid the duplicate, it is advisable to go through searching process.)

(3) If a node has a private key, *RM* saves $ID_A$, $IDK_A$, $PIN_{Adiv}$, $PK_A$, $Sig_A$ in *InfoDB*.

(It saves all the information of the node, so that one can compare the identity between the node

information and information in Info DB by comparing the signature and all other information.)

(4) *RM* forwards the private key $PK_A$, the user $ID_A$, device information $PIN_{Addr}$ hashed to Node A.

Different from previous researches, because *LPMA* protocol which is suggested operates key in *RM* and forwards to the sensor node, it can avoid the unnecessary power consumption by calculation overload.

*LPMA* protocol can finish its registration through XOR operation, while the sensor node in the process of service registration [9] conducts two operations which is causing calculation burden by modular arithmetic.

### *3) Authentication process*

To decrease in calculation burden of the sensor node, the session key is issued through authentication process in *AM*. The following are the process of authentication.

(1) Node A and Node B forward a request message to *AM* for communications through a private key encryption. (Message is sent with a private key to encrypte $IDK_A$, *TS* replay attack $ID_B$)
*AM* checks *Mas* given by Node A to see if the information in *Mas* is available at the current level through *InfoDB*. (*AM* take $ID_B$, $PK_B$ from *InfoDB* use it to verify and authenticate forwarded message from Node B in next step.)

(2) *AM* requests for *Mas* Message from Node B (Node A transmits the message which is asking for the communications)

(3) Node B sends *Mas* message to *AM*.
*Node B→AM : Res* $ID_B$, *Mas*
*Mas* $E\{IDK_B,TS,ID_A\}PK_B$
*AM* checks if *Mas* from Node B is the same as the results of [1] through *Info DB*. After checking, Node A and Node B will verify authentication through *AM*. Then, *AM* makes the session key for the message.

(4) *AM* forwards each session key to Node A and Node B with a private encryption. For communications between Node A and Node B, *AM* issues a safe session key through mutual authentication. Only one operation is needed for mutual Authentication between the sensor nodes.

## 4. LPMA Protocol Evaluation and Analysis

*LPMA* protocol suggested in this study is designed to decrease in power over-consumption during the operation of each sensor node. At the same time, it also offers mutual authentication, authentication of the user and device, MITM Attack, integrity, and confidentiality.

*LPMA* Protocol suggested in this study secures the higher level of securities like other low power protocols and also solves the problem of the power over-consumption caused by lots of operations. Table 2 and Table 3 describes the number of message transmission in the process of registration and authentication, XOR operation of the message, the number of repetition of modular arithmetic in node, and the number of operation in encryption of node. Also to compare *LPMA* protocol, Protocol and operation has been evaluated by Feige-Fiat-Shamir authentication suggested in [8].

**Table 2. Sensor Node Operation in Registration Process**

| Operation | Operation in Sensor Node | |
|---|---|---|
| | [6]Protocol | Our Protocol |
| Massage | *** | ** |
| X OR | - | * |
| Modular | ** | - |

**Table 3. Sensor Node Operation in Authentication Process**

| Operation | Operation in Sensor Node | |
|---|---|---|
| | [6]Protocol | Our Protocol |
| Massage | **** | **** |
| X OR | - | * |
| Modular | *** | - |

* : Execution count  - : Non Count

Three times of modular arithmetic in [6] protocol despite of consideration of low power supply has been resulted in calculation overload. It can be too much burden to the sensor node which has a low power. Furthermore, Feige-Fiat-Shamir has the weak points in terms of key size, which might also lead to the calculation overload to the sensor node. *LPMA* protocol in the paper, decreases the number of the operation between the nodes to solve the low power problems. Also it is very safe protocol in terms of the stability. Only one operation of encryption in the process of registration and authentication can lead to the safe communications with mutual authentication. This protocol decreases the calculation overload which has the low power or limited calculation capacity. The stability of *LPMA* protocol can be evaluated with classifications of the following sections; mutual authentications, session key installation, user and device authentication, MITM attack, the replay attack and its efficiency, confidentiality and integrity.

**– Mutual Authentication**
Mutual Authentication in *AM* can be conducted Mac message which is sent by each sensor node. $E\{IDK_A,TS,ID_B\}PK_A$ sent from Node A gurantee it's freshness as sendiry with time stamp in each sensor node.

**– Session key installation**
$PK=h(IDK||PW)$ is mode with *IDK* in *RM* and session key is made with $PK=h(IDK||PW)$ each sensor node is made with ok in each sensor node.

**– User and device authentication**
Can be made by the identification of *PIN*, *ID*, *Sig* each authentication and issued private key.

*Node A→RM :f($ID_A$||$PW_A$||$PIN_{Adv}$||$TS$||$Sig_A$)*

- **MITM(Man-In-The-Middle) Attack**
  A attacker who is located in between sensor node and *AM* snatches their information and then attacks the session key installation between the sensor node and the attacker, the attacker and *AM*. In this case, the attacker can't even get the private key from the sensor node message. Session key can not be made because it is a outcome of hash of private key in Node A and B.

- **Efficiency**
  The efficiency of the sensor node had been increased by reducing the number of calculation in the sensor node. Only one operation in the node is needed to *AM*. The rest of calculating operation is conducted in *AM* so that the calculation overload in the node has extremely been decreased.

- **The Confidentiality and Integrity**
  The confidentiality and Integrity of the data while sending user's private information can be made by the encryption and the time stamp.

## 5. Conclusions

In this paper, we propose *LPMA* protocol considering the low power problem in Ubiquitous computing. To build the higher level of stability, *LPMA* protocol which features mutual authentications, session key installation, user and device authentication, MITM attack, and its efficiency, confidentiality and integrity are suggested and this study also considers the low power problems of the sensor node where there is low power by calculation overload. Only XOR operation in *RM* and one encryption process in *AM* can lead to issue the safe session key with mutual authentication.

*LPMA* protocol can increase the number of operation in the sensor node, and also maintain the higher security level. *RM* and *AM* are divided and designed to decrease the number of operation while considering the low power in the sensor node. Also *TS* is verified in *AM* and it proves the message freshness and replay attack. In the future, considering the amount time and power for authentication by simulation in *LPMA* protocol are needed.

## References


[1] Dayoung Kim, Yunmi Do, and Nosung Pak, "Sensor Network Technology", *Korea Information Processing Society*, pp85-95, 2003.

[2] Chunsik Pak, "Consideration for Ubiquitous Network and Security", *Journal of the Korea institute of information security and cryptology*, pp12-20, 2004.

[3] DukDong Lee, "Ubiquitous Network and Sensor Ttechnology", *Telecommunications Review*, 13-1, 91-104, 2003.

[4] H. Chan, A. Perrig, D. Song, "Random Key Predistribution Schemes for Sensor Networks", *to appear in Proc. of the IEEE Security and Privacy Symposium 2003*, May 2003.

[5] Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu , "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes", *WSNA'03*, September 19, 2003.

[6] Kaan Y¨uksel, Jens-Peter Kaps, and Berk Sunar, "Universal Hash Functions for Emerging Ultra-Low-Power Networks ", *CNDS 2004*.

[7] Gunnar Gaubatz, Jens-Peter Kaps, Berk Sunar, "Public Key Cryptography in Sensor Networks-Revisited", *ESAS* 2004

[8] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J.D. Tygar, "SPINS: Security Protocols for Sensor Networks", *Mobile Computing and Networking 2001 Rome* , Italy Copyright 2001 .

[9] Laurent Bussard, Yves Roudier "Authentication in Ubiquitous Computing", *Workshop on Security in Ubiquitous Computing UBICOMP 2002*, Göteborg Sweden, 29 Sept 2002.

[10] L.Echenauer, V.D.Gligor, "A Key-Management scheme for Distributed Sensor Networks", *In proceedings of the 9th computer communication security*, Nov 2002.

[11] Jalal Al-Muhtadh "A Flexible Privacy-Preserving Authentication Framework for Ubiquitous computing environments", IEEE ICDCSW Proceeding of the 22nd, 2002.

[12] Ross Anderson, "A New Family of Authentication Protocols", *Operating Systems Review*, 32(4), 1998.

[13] Dong-wook Cho,Yeon-yi Choi, Hee-do Kim, Dong-ho Won " Design of Height Division Protocol that Offer suitable Quotation between in Mobile Communication Enviroment" *Journal of the korea institute of information security and cryptology*, 10-3, 2000.

[14] Dae-hee Seo, Im-yeong Lee "Study of Safe Sensor Network Management", *the Korea Information Science Society*, KISS 2004 Spring, 2004 .