

Secure Authentication and Communication in Ubiquitous Healthcare Middleware

Mangal Sain*, Pardeep Kumar* and Hoon Jae Lee**

* Graduate School of Design & IT, Dongseo University, Busan, South Korea.617-716

** Division of Computer & Information Engineering, Dongseo University, South Korea

Mangalsain1@gmail.com, pardeepkumar@dit.dongseo.ac.kr, hjlee@dongseo.ac.kr

Abstract—Due to the complexity and inconsistency of various application modules, a middleware system should be designed and developed with such considerations that can provide a scalable infrastructure consist of synchronized service system, which built in a high availability environment to provide secure authentication and access control. A secure authentication and authorization are the primary requirements for secure communication in middleware, especially when it comes to ubiquitous healthcare, which deals with sensitive patient's data. In this regards, we have designed a user authentication scheme for sensor node and base station which provides secure communication between sensor node and application or base station. Several middleware are designed in J2EE, so their internal design of authentication and authorization services normally developed using JAAS. In this paper we try to find out the secure Authentication and Authorization Services framework for implementation of the Device Manager. Furthermore, we have analyzed several authentications -schemes for middleware, ubiquitous healthcare and proposed our secure authentication and communication solution by implementing a PingPong-128 algorithm to protect critical patient's data from unauthorized users.

Keywords— secure authentication, Ubiquitous middleware, PingPong 128, JAAS.

I. INTRODUCTION

A ubiquitous middleware for healthcare application consists of several applications that have different users such as patient, physician, nurses, administrator, researcher and students having different role and different responsibilities. In ubiquitous healthcare, authentication and access control should be provided according to privilege allocation in ubiquitous environment which can be varied in different environment such as hospital and home networks. For both case, security requirement will be different. In hospital it can be assumed that it's a trusted and safe network while any public place like home, Café, or remote area where more security credentials should be used. In this environment ubiquitous middleware can't rely on 'single method-fits all'. This authentication approach is not suitable for the diverse and dynamic nature of ubiquitous environment.

As computer technology is entering into modern phase there is great increase of ubiquitous application especially in the smart application and devices which have direct interaction with human. With this trend of technology devices

and services becoming more and more sophisticated and complex which waste lot of user time in configuration and reading manual of devices and services. Ubiquitous healthcare is an emerging field of technology that uses a large number of environmental and patient sensors and actuators to monitor and improve patients' physical and mental condition. There are several sensors which are designed and deployed on body and environment to gather information such as blood pressure, heart rate, temperature, breathing rate and volume, and almost any other information that can be used to diagnose health problems [1]. There are several sensors which are capable of doing desired activity with sampling, processing and communication with more than one vital signs such as heart rate, blood pressure, oxygen saturation and activity, or environmental parameters including location, temperature, humidity and light [2].

Figure 1 illustrates a ubiquitous healthcare network where several applications, sensor motes are deployed on field and body which collect the data and sent to base station which is connected with the main middleware interface. After receiving sensor data at base station, it can be distributed to various users' application with the help of middleware. In every ubiquitous application a middleware always play an important role. In this ubiquitous application, middleware provide a GUI to access all users, application and devices and sensors and analysis that sensor data on their particular application. To analyze that sensor data we build and modify LiveGraph [3] which is used to analyze any 2D data. After analysis of data, it can be stored on application server for further use. To design a completely secure ubiquitous healthcare system, security must be integrated into every module. If any module is left out from security then it could easily become a point of attack.

There can be several types of threats in ubiquitous healthcare specially related to communication and authentication. It's our primary as well as defensive measures to prevent or minimize their impact on the network [4]. In a secure communication we need two major assets which are cryptography and authentication. In order to implement them, we need mechanisms that allow key deployment, exchange and removal. To make more flexible and more user friendly we also proposed Ubiquitous middleware which play an important role to shields the underlying differences in sensor technology from the application layer.

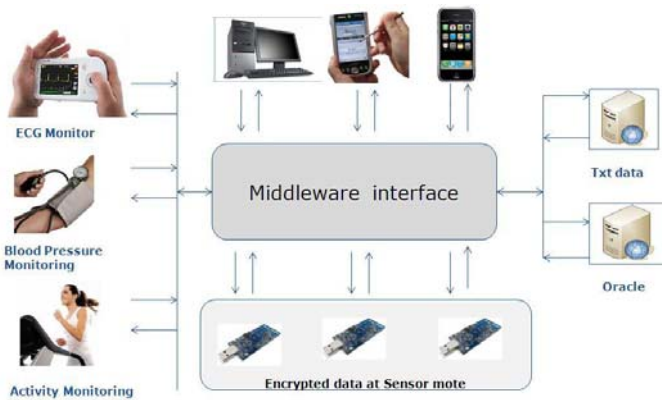


Figure 1. Ubiquitous healthcare system with middleware Interface

This middleware is designed to simplify/accelerate application development which also provide common middleware function but also other function such as portability, security reliability etc.

The rest of the paper is organized as follows: In section II we review the related work. Section III explains the preliminary requirements. Section IV explains design of proposed scheme. In section V explain the experimental setup and performance analysis. In section VI gives a brief conclusion and future remark or our work.

II. RELATED WORK

In this section, we present a related work that has been conducted during past years on the middleware in healthcare application using wireless sensor networks and others WSN applications. We have noticed that, only few of them addresses security.

Middleware systems such as CORBA [5], DCOM, and RMI, which offers high level of distributed network's programming modules with unlimited system resources. It is very unlike to integrate CORBA with wireless sensor networks because the sensor networks are very resource hungry devices. Thus, CORBA is not suitable for wireless sensor networks domain.

An efficient secure security scheme was proposed by Haque[6] for patient monitoring system using wireless sensor network which consist of three main components, patient, healthcare system and secure base station. To establish a secure communication between healthcare system and base station a pseudo-inverse matrix is use to derive the pair-wise shared key and a bilateral key handshaking method is used.

Recently, Waluyo et al's.[7] proposed a design and evolution of lightweight middleware for personal wireless body area network. The main components of proposed middleware architecture are data acquisition, on-the-fly, resource management and dynamic plug-and-play. This architecture is composed of three body area sensor network (BSN) accelerometers and one ECG sensor. The middleware is resided in the personal digital assistance (PDA). Furthermore, the proposed middleware is designed to be

actively notifying the application if there are any changes in the real-time environment.

M. Avvenuti et al's [8] proposed a non-intrusive patient monitoring of Alzheimer's disease subjects using WSNs. The proposed scheme is consists of followings; (a) monitoring the brain activity and the body movements and (b) a middleware, which handles quick and reliable communication of stored data to the hospital information system (HIS) server. (c) Gateway server, which connect the application to the HIS and provide security services, such as, authentication, authorization and non-intrusive patient identification.(d) Hospital information system (HIS), it server as the major repository for patient data in-hospital/home environment. His is contains the medical history of patients data. (e) Data mining and warning generator, which mainly developed for patient data training and testing/validation.

Gomez et al's [9] proposed design guidelines for integration of wireless sensor networks with enterprise systems. Author's discusses the necessity of an enterprise integration component (EIC) that addresses that business application requirement. SOA based architecture is proposed, which is imposed on top-down approach of context aware middleware and bottom-up approach of WSN middleware and offers a standardized, secure, and trusted way to access sensor data.

Levis and Culler [10] proposed a virtual machine for sensor networks, which is implemented on top of Tinyos [11]. Mate was building on stack-based architecture having three execution contexts- clock, send and receive. Furthermore, mate has a small, concise and simple programming module with very high energy consumption for long-time running program. Mate architecture preserve somewhat security features [12].

Vairo et al's [13] sketch a secure middleware for wireless sensor networks, which is based on mote-class sensors. This paper describes SMEPP Light, a middleware for wireless sensor networks that have fundamental concepts of the secure middleware for embedded peer-to-peer (SMEPP) project [14]. The features of SMEPP Light includes mainly, group management, group level security policies, query injection mechanisms, data collection which is based on a subscribe/event approach and adaptable energy efficiency mechanisms.

To define a secure middleware several papers has addressed this issue in different way. TinyLIME [15] is a middleware developed for wireless sensor networks, where sensor data is collected by a central monitoring station, and enables instead multiple mobile monitoring stations to access the sensors in their proximity and share the collected data through wireless links. This intrinsically context-aware setting is demanded by applications where the sensors are sparse and possibly isolated, and where on-site, location-dependent data collection is required.

III. DESIGN REQUIREMENT

A secure authentication and communication is basic key to any healthcare system. In this paper our objective is to build a

secure ubiquitous healthcare system. To achieve this object, our system need two basic key as we stated earlier a proper authentication and secure communication between different devices and application. After analyse several healthcare design and application we conclude the following basic requirements for this ubiquitous system.

1) *Energy constraint:*

In ubiquitous healthcare each patient need a regular and long term monitoring where each and every sensor must be configure to give accurate information. There may be several reason due to that sensor mode can be turn off so we can't rely on the assumption that a sensor node can be always on so we should find some replacement for that time or some warning while a sensor node is sleeping mode or turned off. Secondly a sensor node can't be recharge for whole life so we need to charge and it should programmed with the power consumption so after a particular time it can inform it will be not available for regular reading or communication. Due to sensibility of data we cannot assume on prediction which can harmful for continuous monitoring. Now as several application devices are getting smaller the energy constraints is becoming more and more important which also effect to security constraints.

2) *Privacy:*

A healthcare system is extremely sensitive, especially when it comes to data privacy it's a core requirement for any healthcare system. We have to make sure that personal healthcare data can't be accessed by any outsider or any unauthorized person. From healthcare providers' point of view, a data breach would have very serious legal and financial consequences. From users' point of view, they may be hesitant to use the system if they are not convinced that their data will be kept confidential.

3) *Authentication:*

Data authentication is one of the key requirements in any healthcare application and device, since healthcare providers rely on the data to diagnose and treat their patients as well as react to emergencies. Patients' lives can be endangered if their data or commands from healthcare providers are intentionally changed or forged. Note that verification of data authenticity has to be carried out as soon as data is received to ensure timely reaction to emergencies. We try to concentrate to secure patient data which secure as it is transferred to base stations. The problem of data security does not stop at that point; there are still issues such as ensuring that only authorized personnel can view the data, and preventing accidental disclosure of the data.

4) *Security:*

Security is the most important phase of any system. When it comes to ubiquitous healthcare security becomes more important to every phase.

- a) The service can reliably identify the user or system
- b) Information security from unauthorized users
- c) Application can log security relevant events

Figure1 illustrate the block diagram of proposed middleware interface for ubiquitous system that consist of various sensor nodes, healthcare application, application server and database, which is connected with middleware interface. Each application is connected with each other with the help of middleware which play a core role to provide authentication and secure communication between different application and devices. This middleware provide an interactive graphical user interface (GUI) to different users such as patient, physicians, nurses and researchers. The sensor nodes transmit an encrypted data to the base station/gateway. The gateway then decrypts the encrypted data, processes the information and make available to the application layer for further analysis. After process that data at application layer, the information will be transferred to database.

As shown in figure 1, a client can access different applications through middleware interface. All applications are enabled with web application, which is a part of middleware. After accessing the application, users can feed the data and retrieve all the previous record which they are authenticated. After login each user will be given the authorization according to their specified rules which are stored in database. Rule based service locator allocate the roles according with the information provided by users. Each client is using Web based GUI application through they can access send their request to server and use a common architecture to communicate. The JVM and Server side web components are used in servlets and java server page (JSP).

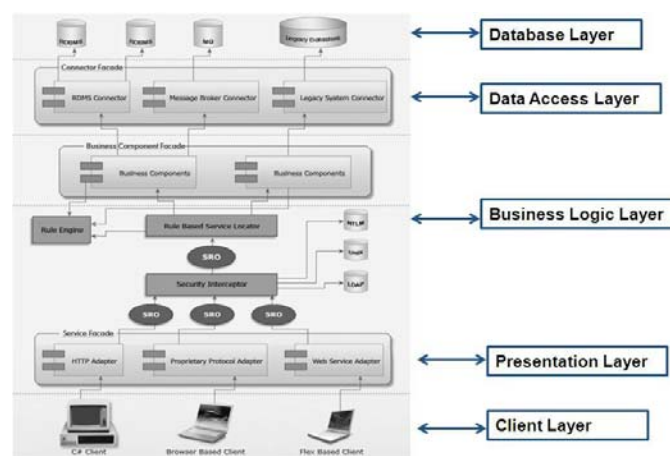


Figure 2. J2EE core architecture for middleware

As figure 2 shows an application client runs on a client machine and provides a way for users to handle tasks that require a richer user interface than can be provided by a markup language. Application clients directly access enterprise beans running on the business tier. However, if an application requirement permits it, an application client can open an HTTP connection to establish communication with a servlet running in the web tier. Application interface which is provided by middleware is developed in J2EE technology, which is based on model-view-controller [16]. Model-view

controller architecture provides a software design pattern at different application levels, namely, the presentation logic (view), business logic (control), and data objects. It also plays an important role to achieve high reusability of code between different modules. This application interface which is for different user interaction is design in J2EE, Swing with eclipse IDE. In figure 2 illustrates the J2EE architecture, which is most suitable to design any web-based application.

IV. SYSTEM DESIGN

To get the maximum benefit of any ubiquitous healthcare system, it's necessary to build such middleware that can support different ubiquitous application and devices. Furthermore that middleware also process data management and information processing. There are several attributes which are essential for ubiquitous applications such as: usability, distributability, extensibility, performance, portability, and security.

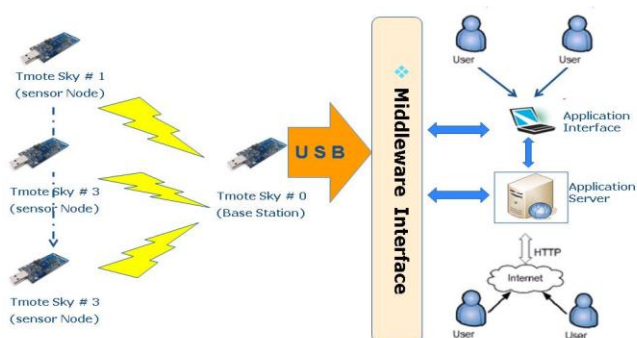


Figure 3. A sample line graph using colors which contrast well both on screen and on a black-and-white hardcopy

Figure 3 illustrate the internal architecture of or proposed scheme which is secure communication from different sensor node to various application. We also build a middleware to provide an interface and GUI to communicate between different application and database. Each application is connected with each other with the help of middleware which play an important role in this project. This middleware provide an interactive graphical user interface (GUI) to different users such as patient, physicians, nurses and researchers. The sensor nodes transmit an encrypted data to the base station/gateway. The gateway then decrypts the encrypted data, processes the information and make available to the application layer for further analysis. After process that data at application layer, the information will be transferred to database.

V. EXPERIMENTAL SETUP AND PERFORMANCE ANALYSIS

To build a secure application it need to fulfill several requirements such as confidentiality, authentication, integrity etc. In every application security is the main concern which we also took into our prior consideration. To prevent unauthorized access from unauthorized users we have used

PingPong algorithm during data communication. By applying symmetric PingPong-128[17 and 18] stream cipher, we achieve data confidentiality, data authentication and data integrity. The security configuration is discussed below. We have to implement in each phase, either it is registration, authentication or verification.

A) Experimental Setup

Figure 4 illustrate the real time setup of our communication architecture which consist of ECG and tri-axial accelerometer where sensors mote transmit the encrypted data to the base station wireless and after implementing decryption that data can be will be transferred to middleware where it will be processed with the help of LiveGraph which will explain later. We can see mote directly transfer the data to base station. We encrypt the data on mote A and after it will be transferred to base station where, after authentication it will be decrypted and after processing that data it will be stored into server for further processing.

For the experimental setup a sensor board is integrated to a wireless sensor node which consists of an ECG and a tri-axial accelerometer sensor. In the sensor board, ECG signals from the electrodes are amplified with a gain of 300 (24.8 dB) and filtered with the cut-off frequencies of 0.05 Hz and 123 Hz. An ECG electrode has two electrodes which are integrated within the sensor belt. In addition, the sensor board also has a three-axis accelerometer sensor (MMA 7260Q, Freescale) to measure acceleration signals.

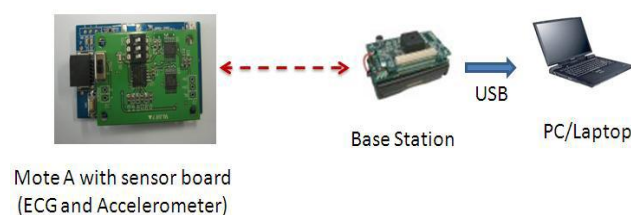


Figure 4. Real-Time Testbed Setup

B) Security analysis

PingPong family is based on summation generator stream cipher with addition of mutual clocked control structure. The algorithm is designed with both security and efficiency in mind to satisfy the need for lightweight algorithms. PingPong is highly secure algorithm, dedicated to hardware environment and easy to implement in software. PingPong-128 is a bit based stream cipher. This stream cipher is constructed on two mutually clocking LFSRs and a single memory bit. PingPong-128 accept key as 128-bits and 128-bits initialization vector to feed the internal states. It generates an output block of 128 pseudo-random bits from a combination of the internal states for every iteration PingPong-128 has 257-bits of internal state. For the detailed specification, refer to [17].

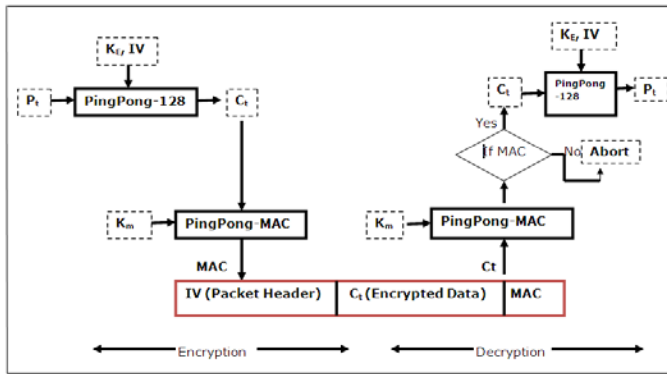


Figure 5. Authenticated encryption work flow in PingPong-MAC

As shown in fig 4, authenticated encryption work-flow, sender feed P_t (plaintext) into PingPong-128 cipher with key and IV, and obtained C_t (encrypted data) as output. This C_t again feed into PingPong-MAC with key K_m and obtained MAC as output. Now encrypted data is having IV (packet header) and MAC. For the authentication, when another node received this encrypted packet, then node first confirms whether this data is sending by its corresponding node or not. This PingPong-MAC is Encrypt-then- MAC stream cipher mode. In Decryption process, the C_t (encrypted data) is fed into PingPong-MAC with K_m , and then MAC is checked. If MAC is matched then this C_t is again feed into PingPong-128 with Key and IV and obtained P_t (plaintext). After implementing this algorithm finally we can give some final conclusion below.

a.) Confidentiality:

In sensor networks, data should not be leaked to neighboring node because sensor deals with very sensitive data. In order to provide the security, the data should be encrypted with secret key. Secret key is intended to recipient only; hence confidentiality is achieved by applying of PingPong-128 stream cipher.

b.) Entity Authentication:

Authentication allows to receiver, to verify that the data is really sent by authenticated sender or not. In node-to-node communication entity authentication can be achieved through symmetric mechanism: a message authentication code (PingPong-MAC) is computed on secret shared key for all communicated data.

c.) Data Integrity:

Data integrity is a service, which addresses the illegal alteration of data. To conformation of data integrity, one must have the ability to identify data manipulation by illegal parties. must be indented.

C) Experimental Result

For simulation purpose we implemented PingPong-128 stream cipher in wireless sensor networks and results are shown in Table 1. Our scheme is taking 598 bytes RAM and 16,474 bytes of program space for encryption. By doing so,

we achieved a secure pair wise communication between neighboring sensor nodes.

TABLE 1. EXPERIMENTAL RESULT

Description	ROM (Bytes)	RAM (Bytes)	Execution Time ms
Without security scheme	15,354	470	-
PingPong-128 (Encryption only)	16,474	598	14.43
(Encryption only)	16,474	598	14.43

In the beginning of our architecture we said we also build a tool to analyze data such as ECG, accelerometer, Spo2 etc. As we aware with the fact that MATLAB is the best tool to analyze any kind of data, so when we try to build such application, which can analyze any kind of live data. MATLAB is already a full fledge application so it's not feasible to use MATLAB with existing or new application. With our LiveGraph module we can fulfill this requirement and figure 5 will the result of ECG wave form which is exactly the same if we will plot that data on MATLAB. So we try to build a module which can give the same performance and result in live atmosphere.

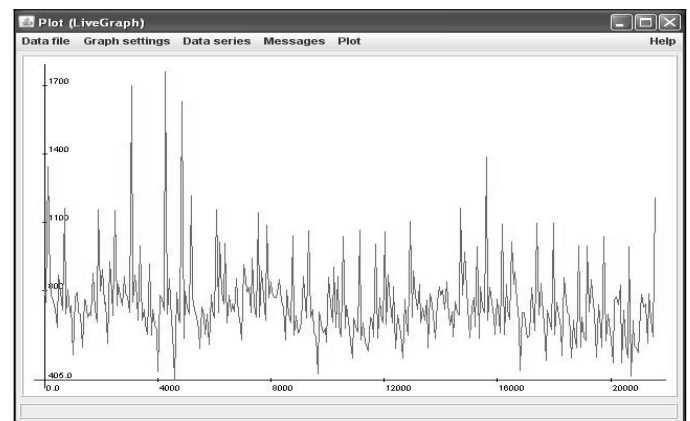


Figure 6. ECG data analysis with LiveGraph

In figure 5 we can see ECG data is analyze and displaying in LiveGraph with Plot module. LiveGraph can fulfill some basic requirement and it's much easier to add several algorithms in LiveGraph instead of MATLAB for live application.

VI.CONCLUSIONS

A ubiquitous healthcare system is wide and continued growing field which is exposed to numerous security threats that can affect the application on any level. In this paper, we proposed a secure authentication and communication in healthcare system which certainly enhance the quality communication between different sensors and also improve

the quality of service with several modules. There is one middleware interface also developed with this system to communication with different application module and sensor which will play an intermediate role in secure communication by receiving sensor data as well as control the sensor devices attached to patient or spread in environment. After implementing Ping Pong-128 stream cipher algorithm in communication, we can assure the security threat will not be a problem anymore. With this prototype a secure middleware is presented and implemented in this paper with several other measurements such as performance, portability, scalability and security.

To future work, we plan to analyze the trade-offs of security and performance. In addition we are planning to analysis some decision making algorithm and technique to enhance the feature of any ubiquitous healthcare. With the help LiveGraph which can enhance and add new features such as healthcare decision making in ECG and applying some feature extraction on Accelerometer sensor which will increase the reliability of this system.

ACKNOWLEDGMENT

This research was supported by the 2010 NRF (National Research Foundation) Project, South Korea.

REFERENCES

- [1] Lo B, Thiemjarus S, King R, Yang G-Z (2005) Body sensor network—a wireless sensor platform for pervasive healthcare monitoring. In: Proceedings of the 3rd international conference on pervasive computing, pp 77–80
- [2] Estrin D et al (1999) Next century challenges: scalable coordination in sensor networks. In: Proceedings 5th annual ACM/IEEE International conference mobile computing and networking (MobiCom), pp 263–270.
- [3] LiveGraph is a framework for real-time data visualization, analysis and logging <http://www.live-graph.org/index.html>.
- [4] Wang, Yong , G. Attebury, and B. Ramamurthy. " A survey of security issues in wireless sensor networks ." Communications Surveys And Tutorials, IEEE 8 , no. 2 (2006): 2-23 .
- [5] OMG, "The Common Object Request Broker: Architecture and Specification", Rev.2.2, 1998.
- [6] F. Hu, M. Jiang, M. Wagner and D.C. Dong, "Privacy-Perserving Telecardiology Sensor Networks: Towards a low-cost portable wireless hardware/software codesign, " IEEE Trans. on Inf. Tech. in Biomedicine, vol. 6, no. 6, pp 619-627.
- [7] Agustinus Borgy Waluyo, Isaac Pek , Xiang Chen and Wee-Soon Yeoh "Design and evaluation of lightweight middleware for personal wireless body area network" Personal and Ubiquitous Computing Volume 13 , Issue 7 (October 2009) Pages: 509 - 525 .
- [8] Avvenuti, M.; Baker, C.; Light, J.; Tulpan, D.; Vecchio, A.; "Non-intrusive Patient Monitoring of Alzheimer's Disease Subjects Using Wireless Sensor Networks" World Congress on Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS '09.
- [9] Laurent Gomez, Annett Laube, Alessandro Sorniotti, "Design Guidelines for Integration of Wireless Sensor Networks with Enterprise Systems" In MOBILWARE '08: Proceedings of the 1st international conference on MOBILE Wireless MiddleWARE, Operating Systems, and Applications (2007), pp. 1-7.
- [10] Philip Levis , David Culler, "Mate: A Tiny Virtual Machine for Sensor Networks" 10th international conference on Architectural support for programming languages and operating systems, 2002.
- [11] <http://www.tinyos.net>
- [12] Mohammad M. Molla, Sheikh Iqbal Ahamed, "A Survey of Middleware for Sensor Network and Challenges"Proceedings of the 2006 International Conference Workshops on Parallel Processing, 2006
- [13] Claudio Vairo ,Michele Albano, Stefano Chessa "A secure middleware for wireless sensor networks" International Conference on Mobile and Ubiquitous Systems:Computing, Networking, and Services 2008.
- [14] Javier Barbarán, Carlos Bonilla, Jose Ángel Diances, Manuel Díaz, Ana Reyna "Simulating SMEPP Middleware" International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshop, Marseille, France 2008
- [15] C. Giani et. Al. "Data collection in Sensor Networks: the TinyLime Middleware", J. of Pervasive and Mobile Computing, 4(1), pp. 449–469.
- [16] Edward Curry, Paul Grace,(2008) "Flexible Self-Management Using the Model-View- Controller Pattern," IEEE Software, vol. 25, no. may-June 2008 3, pp. 84-90,
- [17] Hoon Jae Lee, Kevin Chen, PingPong-128, A New Stream Cipher for ubiquitous Application. ICCIT, 2007. South Korea
- [18] Pardeep Kumar, Sang-il Cho, Dea-Seok Lee, Young-Dong Lee and HoonJae Lee "TriSec: A Secure Data Framework for Wireless Sensor Networks Using Authenticated Encryption "International Journal of KIMICS 2010