

# Mobile Middleware for Body Sensor Network: A Grid Approach

Rossi Kamal, Choong Seon Hong

Department of Computer Engineering, Kyung Hee University

rossi@networking.khu.ac.kr, cshong@khu.ac.kr

## Abstract

Wireless Existing mobile middleware for BSN (Body Sensor Network) has software agents both on sensor and gateway nodes. Software agents on BSN nodes depend entirely on that of gateway to connect to server. There must be a way by which sensor nodes themselves can communicate in BSN and connect to server. This paper solves the problem with a grid approach for mobile middleware on BSN. Sensor nodes (equipped with this middleware) with grid computing can operate entire BSN and perform QoS and security operations. .

## 1. Introduction

Wireless sensor networks have the potential to greatly improve the study of diseases that affect motor ability. Small, wearable sensors that measure limb movements, posture, and physiological conditions can yield high-resolution, quantitative data that can be used to better understand the disease and develop more effective treatments.[1]

Body sensor network has number of challenging issues associated with it. [1] depicts three challenges related to clinical requirements namely battery lifetime, operation tuning according to radio bandwidth and energy availability and confirmation of high-quality and clinically relevant data. Quality of services is another challenging issue.[2]discusses some of related issue namely prioritized data stream service, asymmetric QoS framework, radio agnostic QoS, adaptive bandwidth scheduling etc. Often heart activity reading is given more priority than body temperature reading. A glucose data stream might be assigned low priority on normal condition but might be given higher priority if there is nearest reading of hyper or hypoglycemia .Body sensor network often involve node and aggregator -built star topology and thus encourages asymmetric QoS features. Existing body sensor network consists of different radio networks like IEEE 802.15.4 or Bluetooth or CC1000. Interoperability among those is a challenging issue. Sensor nodes are affected by adverse fading of human body or interference from co-existing network or RF emitting

devices. Adaptive QoS scheduling is required for statistical bandwidth guarantees.

Wearable personal monitoring devices now-a-days can record and archive user activities for medical, safety reasons. A software architecture is needed to 'facilitate development of such wearable personal monitoring application, promoting their modularity and component reuse, to provide a simple modular architecture into which different classification algorithms, communication protocols and data filters can be integrated as components with well-defined interfaces'[3].Critical problems of distributed inter-process communication, signal processing and sensor data classification encourage the development of a generic software architecture. MIThrill 2003[4] created such an architecture to combine features and practices from a range of research systems and methodologies and they did it with an open, modular and flexible way.

Existing middleware for BSN use gateway that collects information from sensor node and sends to server. Often this middleware is placed in a mobile device and people have to carry it with him. But it is not mobility in real sense. We can think of a middleware consisting of only BSN nodes. The concept of grid computing comes at this point. We propose a grid approach based mobile middleware that will use distributed computing to overcome the limited resource of BSN nodes. We have proposed QoS and security approach for it based on mobile grid environment.

## 3. Challenges for mobile middleware for body sensor network

Body sensor nodes have to run sophisticated

---

This research was supported by the MKE, Korea, under the ITRC support program supervised by the NIPA (NIPA-2010-(C1090-1002-0003)).

Dr. CS Hong is the corresponding author.

programs and multiple applications may correspondent to a single node. Yet, relatively less attention is paid to QOS issues like delivery latency, sensory, accuracy, energy consumption, data throughput etc. Existing sensor middleware prefers best effort service, not considering application semantics. Programming tradeoff between QOS and resource-consumption is tedious and error-prone. However, some middleware adopts QOS features in different ways. MiLan[11] takes specification about the minimum QOS requirement and adopts network to it. But, it minimizes resource consumption at its possible level. In a monitoring system, while most of the time nodes will find nothing interesting. Making all nodes engaged to that work is just power consumption, so a sparse subset of nodes is engaged in the work. When a phenomenon occurs, then QOS of related nodes are increased. Thus proactive approach enables MiLan to provide higher QOS remembering power consumption. Autosec adopts resource allocation to provide QOS. It maintains a directory service which gives the current status of the network. Depending on current status, it gives resource allocation policy. Directory service maintenance, resource allocation policy is a challenging issue.

Real-time monitoring is also a part of QOS. Message and actions should be functional on time at right place. DSWare, publish subscribe middleware relies on standard real-time packet scheduling mechanisms like Earliest Deadline First. RAP uses real time query processing technique. It has velocity monitoring scheduling that uses spatial properties of network. A user issues a query with certain period, deadline and data refreshment requirements. As data is sent, its velocity determines how urgently it could be forwarded. A message with possibility of missing deadline has better priority than one that will be meeting deadlines.

Sensor nodes communicate confidential and sensitive data on patient's health. There must be measure to restrict unauthorized access to confidential data. The security is still in early age and too much work have to be done in this area [12]. [12] also depicts some problems on sensor security. Sensor nodes are generally developed with small nodes and spread over potential hostile area. It thus makes it open to the attacker. Limited energy of sensor nodes are attractive for attackers who force to exhaust their energy and die. Due to limited resource, availability, low computational power, most existing algorithms and security modes

are not suitable for sensor network[13]

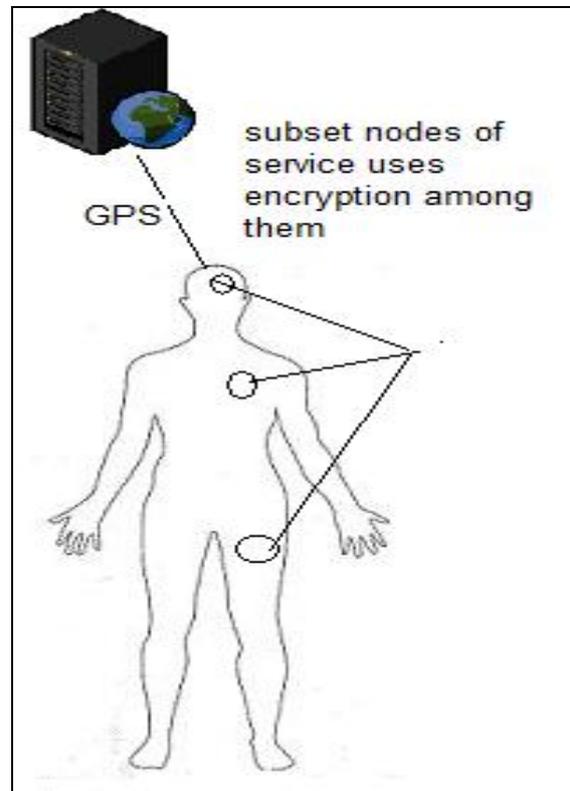


Figure 1: Encryption among nodes of a subset of specific service

#### 4. Grid Mobility Approach on middleware

To provide service of a guaranteed quality while maintaining user's profile and addressing characteristics of mobile devices and limited availability of resources [14], grid middleware is an efficient solution. It is extremely important to develop system that provides effective QOS management and allows mobile users to benefit from the service requested, regardless of users and user's movements. Grid provide innovative access to distributed data. Members on a grid are provided with wide scale computational data and resources toward same purpose. Grid makes of use of idle resources available on internet to perform distributed computational operations [14]

Grid, with rational use of resources of a distributed network may impact on load balancing, QOS management, secure access. Grid impacts on the mobile middleware in different ways. It provides effective management of distributed data to move to close to user or to manage overload or fault tolerant

situations. It manages services according to user device—as a result the same user gets access to services through different environments by the presence of different terminal equipments. It also provides service discovery using distributed strategies based on data replication.

In a wireless infrastructure, co-operative and resource sharing techniques become an essence. Grid computing in this case becomes major strategy for ad-hoc network. Wireless grid introduces grid computing concept to resource limited devices so that they can carry on parallel operations by sharing idle devices. Its peer-to-peer paradigm discovers resources and services of devices..Its component based programming binds software modules of of shared nodes. In this way, mobile grid has become a challenging issue in mobile middleware for ad-hoc environments like body sensor network.

## 5. Proposed Grid Approach

### 5.1. Architecture

Security module of this mobile middleware consists of three main components namely Authentication and authorization, permission, message integrity and confidentiality. Authentication features allow whether requesting node is valid or not. It also includes whether the service requested by the requesting node is valid or not. Permission detects the access permission on body nodes or service. There will be subset of nodes for particular service (blood-pressure, temperature calculation etc ). Nodes of same service will have access permission to the only nodes of that subset or that specific service [Fig-1]. It also includes permission variances like http, socket, file or runtime access-rights. Special instance of permission module will control over the longevity of cluster node. This will control how long the cluster node will hold the clustering property and who will become the next cluster for immediate service. Integrity and confidentiality feature enable that message is not altered or ready during transmission. Security module has the option to add protocol, encryption, and signature depending on the service or the body organ. QOS module has two major components—proactive and reactive. Proactive module ensures high QOS ensuring low-power consumption. A subset of all nodes related to a specific service will monitor the status. At occurrence of any critical session, all other nodes will be triggered to ensure high QOS standard

[Fig-2]. Reactive module with real-time query processing will use spatial property of the network.

Here the body sensor node sends a query with certain period, deadline and freshness requirements. When a message is sent from a node, its velocity is used to determine the current QOS condition of the network.

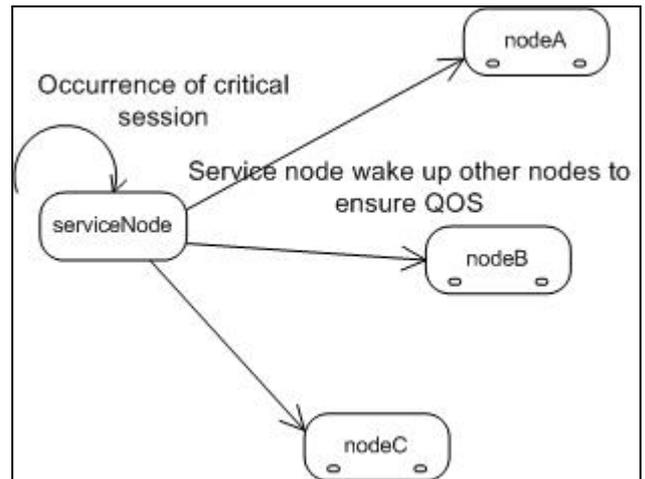


Fig 2: Proactive QoS mechanism in proposed middleware

### 5.2. Prototype

This middleware is built on OSGI specification [15], a industry standard software development paradigm. There are three major modules—service, impl and slick. Service module contains definition of services namely core, security or QOS. Core service contains data or control management, protocol management etc. Security service contains three parts for authentication, protection and integrity. Proactive and reactive features are placed within QoS. Impl directory contains implementation of sections and their subsections of service module. For example, ReacMan implements reactive QoS mechanism described in the paper. slick is last module that creates testing environment in the middleware. Implementation of any protocol or service is tested by creating two instances within slick module of the middleware.

Let us go inside the design of this mobile middleware [Fig 3]. DataMan exchange packets within the sensor network. ContMan controls connection between nodes and connection to GPS. It also has the property of

change node properties on the fly by getting or resetting sample rate, controlling critical awake state. ProtMan controls the variances of communication protocols( 802.15.4 or Bluetooth), Auth-Manager, PermManager and IntegrManager are involved in ensuring security mechanisms authorization, protection and integrity. ReacMan deals the dynamic QoS management while ProacMan engages some nodes of a subset nodes of a specific service. These nodes trigger other idle nodes at any critical situation. To add a new service servA ( for example, new monitoring system of existing organ, new organ monitoring system ), we will add servA module in subsections of service, impl and slick. servA in service module will define solution, servA in impl will implements the complement system. .Two instances of servA will be functional inside slick to check its validity. To add a new protocol (security or QoS), we have to adopt the same procedure.

Porting middleware to this new change will be also challenging. Interoperability is a concern, but we need to remember about the limited resource of BSN nodes.

We have a plan to implement proposed middleware on a test-bed. To implement mobility in real sense, we may play with distributed shared object implementation on our middleware. SOAP is one of them and implementing SOAP on nesC over TinyOS will be very challenging.

**References**

[1] Konrad Lorincz, Bor-rong Chen, Geoffrey Werner Challen, Atanu Roy Chowdhury, Shyamal Patel, Paolo Bonato, and Matt Welsh ,Mercury: A Wearable Sensor Network Platform for High-Fidelity Motion Analysis,In Proceedings of ACM SenSys2009

[2] Gang Zhou, Jian Lu, Chieh-Yih Wan, Mark D. Yarvis, and John A. Stankovic ,BodyQoS: Adaptive and Radio-Agnostic QoS for Body Sensor Network,In Proceedings of IEEE INFOCOM 2008

[3] Raghu K. Ganti,Praveen Jayachandran,Tarek F. Abdelzaher,John A. Stankovic ,SATIRE: A Software Architecture for Smart AtTIRE, In Proceedings of MobiSys'06

[4] Rich DeVaul, Michael Sung, Jonathan Gips, Alex Sandy Pentland ,MITHril 2003: Applications and Architecture,In Proceedings of the Seventh IEEE International Symposium on Wearable Computers (ISWC03)

[5] Agustinus BorgyWaluyo,Isaac Pek,Xiang Chen,Wee-SoonYeoh,,Design and evaluation of lightweight middleware for personal wireless body area network,Personal and Ubiquitous Computing,Springer-Verlag,2009.

[6] NSA: National Security Agency Skipjack and KEA algorithm-specifications, <http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf>. Referenced 2 April 2008

[7] OracleJava ME:the Most Ubiquitous Application Platform for Mobile Devices, <http://java.sun.com/javame/index.jsp>

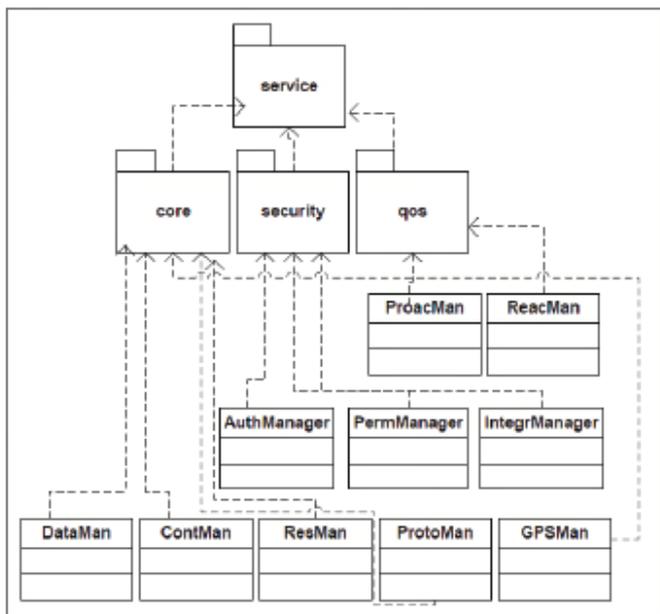


Fig 3: Class Diagram of Proposed Mobile Middleware

**6. Conclusion**

BSN nodes are coming with high capacity of computing complex, sensitive information. Addition of newer products to existing system, giving software support, reuse previous resource-these will be challenging issues in days to come. Advancement of QoS and security protocols of BSN is still in process.