Implementing Role Based Access in Healthcare Ad Hoc Networks

[1]A Santhosh Kumar [2]G Mohan Raj
[1]PG Scholar
santhoshadhi29@gmail.com
[2]Assistant Professor
mohanraj134@gmail.com
[1,2] Dept. of CSE
SONA COLLEGE OF TECHNOLOGY
SALEM, TAMILNADU.

Abstract **- As mobile ad hoc networks (MANETs) are becoming popular for a variety of applications, so are the issues surrounding corresponding implementations. In this paper, a healthcare application is developed for an environment where normal network connectivity may not be available hence networking of small scale healthcare units and corresponding devices becomes necessary. Different roles of such units are discussed to facilitate role based access control (RBAC) conformant access. The concepts of role-based access and databases are combined to specify separation of duty (on ad hoc networks) as required for database integrity. The framework to adapt policy based access control model in the MANET environment is discussed. Furthermore, XML implementation of such access control within a typical rural healthcare environment is investigated.**

Key Terms **- Healthcare Ad hoc Networks, Policy Based Access, Role Based Access, XML in Healthcare**

I. INTRODUCTION

A mobile ad hoc network provides a communication environment that is characterized by dynamic changes in the topology and in the availability of resources. Due to higher bandwidths available in the newer wireless local area network (WLAN) standards it is not far that database support would be routine to achieve workflow and communication management that includes setting up a dynamic infrastructure with changing sizes and authenticated access using certain access control policies. Nowadays healthcare providers such as doctors and nurses can directly communicate with one another via wireless infrared beaming in their PDAs. In particular, modern healthcare institutions can benefit from much more extensive use of mobile devices for pervasive and ubiquitous access to healthcare information systems to deliver healthcare services, such as general surgery and emergency services. However, along with the MANET computing possibilities comes a new raft of security as well as privacy vulnerabilities. Beyond the urgency of regulatory compliance, healthcare institutions are realizing that effective security management and privacy (especially content management) are essential for earning and maintaining public confidence as well as trust in their healthcare services. Typically, collaborations among the participants of an ad hoc network cannot be set up because they do not trust each other to use their respective services and resources. Therefore,

there is a need for explicit specification of policies for each activity. As an example, a large number of enterprises have recently started to explore Internet based workflow management systems to help improve their services and decision-making processes. In the same direction, there has been a number of access control models discussed in literature for various objectives. Among them, the RBAC model has gained attention as a generalized approach and provides several advantages Under the RBAC framework, users are granted membership into roles based on their responsibilities in the organization. Role-Based Access Control models are receiving increasing attention as a generalized approach to access control. Furthermore, RBAC has shown to be policy neutral and supports security policy objectives, and static and dynamic separation of duty constraints. The extensible Markup Language (XML) is generally regarded as having promise of becoming established as the general purpose framework for enabling transfer of data amongst heterogeneous environments. It is being implemented for secured data communications transfer once details of application requirements and constraints are taken into account. Therefore, it seems challenging to investigate possible implementation of XML access control and document security in a different network environment, for example a remote rural healthcare unit. As a summary, it can be said that the patient data and healthcare operations are both private in respective domains, and thus pose serious integrity, confidentiality, and accountability issues. In other terms, the technical challenges emerging from deployment of (rural and mobile) healthcare units are security of data transfer, organizational policy control and standardization of implementation within a short lived and smaller geography wireless ad hoc network. In this research work, the approach is customized to the environment, where privacy is mandatory to be implemented in a mobile, short lived wireless network with relatively fewer operating nodes. Moreover, emphasis is placed on the use of standards while implementing techniques. Presented to highlight existing approaches. In section 3, an approach is proposed that addresses the issues summarized in section 2. In fact, an access control model is developed for a healthcare environment. In section 4, a typical health care environment is discussed that enforces an access policy defined by a healthcare organization. A mobile rural healthcare application is investigated that consists of few operational units working on role based access model in an ad hoc network environment. Its XML implementation is discussed, and design parameters are investigated. The section 5 provides discussions on key findings and how it can further be improved. In section 6, conclusions are presented followed by references in section 7.

II. RELATED WORK

A lot of research work has, recently, been reported in the area of access control in role based operations of field units such as small businesses and defense units, etc. To our knowledge, healthcare privacy requirements in MANETs have not been addressed before. A number of research works were found in the area of medium access control (MAC) in wireless networks in the area of channel access. The respective authors do not address task based and secured access in the flow of data within an ad hoc environment. In another work, a methodology for reliability analysis in healthcare networks has been carried out to propose design of regional healthcare networks during its early stages, without any discussions on privacy and security issues

within an ad hoc environment. To state few implementation examples, role based access is investigated in military domain by developing a mobile secured role based access control (MS-Ro-BAC) device in a single unit system using satellite communication around the world. In, the authors have discussed a distributed approach for role based access management to enable secure resource sharing in heterogeneous scientific collaborative environment. Another implementation has been reported in, where authors have presented distributed role based access (dRBAC) to add contextual information to support spontaneous networking in coalition collaborative applications for users in different domains, where resources and services are located and owned by other entities. In all of these research works, the contribution is to support role based operations for long duration of time, within a large operational area and in some cases amongst different domains. However, healthcare operations, in rural area as an example, are of short duration (mostly mobile), consist of small groups of operators and deal with patient data that is considered private even to a healthcare organization. A lot of research work has been carried out in the area of XML, its specification development, and security features etc. In the area of security, XML key management specification (XKMS) is one of the XML's security specifications that define the protocol for distributing and registering public keys for verifying digital signatures and enciphering e-commerce applications. The authors in discuss XKMS-based key management system architecture and a service model using Java crypto technologies and XML security mechanisms. XML digital signature capability has also been discussed in, where authors describe a solution to add XML digital signature using a signature server implemented as a web service. In emerging applications, a similar work is found in where future directions for data and applications security that include secure semantic Web, XML security and applications such as peer-to-peer computing, and stream information management are addressed. The objective have been to embed XML within a document to address document (and document transfer) security. Since (rural and mobile) healthcare environment is wireless domain with data transfer within a small area, it seems appropriate to explore XML further and use its benefits (i.e., security and standardization) for an application environment using role based operations running in an ad hoc network.

III. PROPOSED APPROACH

In this section, only user access issues in ad hoc network and proposed framework for a typical healthcare environment are presented. Before proposing our approach, the database access concerns are summarized to highlight access constraints. The pertinent issues surface after an adhoc network of devices is formed.

A. Organizational Policy and Access Criteria

In general, data access in a wireless ad hoc network may require a service channel to boost cache recovery, application logging, role base access logging to facilitate retrieval of cache, and data management. The data management can further be elaborated to include access policy criteria such as:

a. User/Group/Role: Policy can be defined for groups and roles so user access is relevant to their organizational placement. This helps in assignment of data access to respective healthcare personnel.

b. Application and Application Content: Deep packet inspection enables identification of applications regardless of port. Applications using the same port can be distinguished from each other for accurate access control.

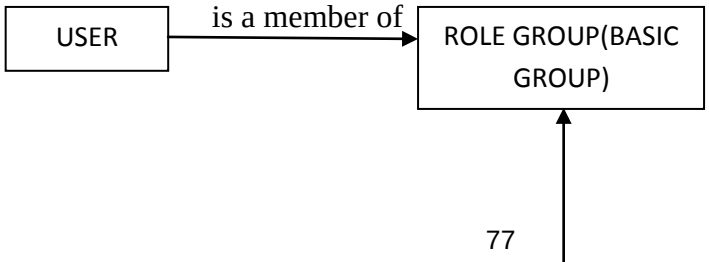
c. Standard ACL (Layer 2, 3, and 4): Traditional access control lists (ACL's), like those used in firewalls and routers, can be defined based on source MAC address, source and destination IP Address and protocol, and either type.

d. Periodic and Absolute Time: Policies can be defined as valid only during specified time and day ranges such as every weeknight between 11pm and 3am. Absolute times can be used to create policies that expire on a specific date and time such as December 25, 2008 at noon. This helps in assigning data access based on duty basis or time shift of healthcare personnel.

e. Location: **Access** policy can be defined based on the direction of traffic, which is a function of the source and destination locations. Inbound access policy may be different than outbound policy. This helps in denying access to patient and healthcare unit data while it is to be processed outside set limits of the policy domain (like cafeteria for example). This data management can be simplified if a formal (and standard) policy is followed that simplifies the job of IT manager as well. Below, the role based access and the respective standard model are discussed.

B. Access control based on roles

The research on policy based design in networks is the idea that groups are defined around objects and that objects can be hierarchically combined. Object can be any resource subject to access control like file, printer, terminal, database record, people, location, or a meeting etc., where as role is a job function within the context of an organization with some authority and responsibility conferred on the user. An operation, upon invocation, executes some function for the user. The permission is an approval to perform an operation on one or more objects. To develop access control on the objects, a draft role engineering model proposed by National Institute of Standards and Technology (NIST) in January 2006 may be adopted. This standard describes implementation requirements for RBAC systems. The model is shown in Figure 1. Once a session is established, a subset of roles are activated, which contains functional roles that contain permissions that a user has available once the session is established. In establishing a connect session, there is an implicit assumption that the user is in fact an authenticated user to invoke certain permissions, such as opening a session. Functional role activation cannot occur until the session is established. To accomplish basic connect function, the user would possess, in addition to authentication information, some set of basic (static) roles that would be prerequisites to a user's being authorized to "connect" to the task. Thus, role groups can allow a user to "connect" to a resource but do not necessarily grant finergrain authorizations on protected information objects. The role groups define what specific work profiles users are allowed to perform, while functional roles define what authorizations are needed by an entity to access protected information technology or application resources. Some healthcare basic role examples include: Doctor, Pharmacist, Registered Nurse, and Office Assistant. These are basic roles suitable for session-connect privilege that do not necessarily specify what the user can do once connected. The Figure 1 highlights relationships between role groups, work profiles, and functional roles consistent with RBAC standard.



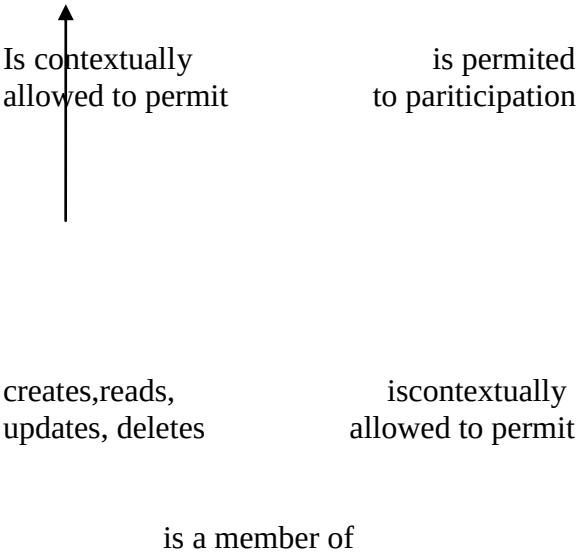


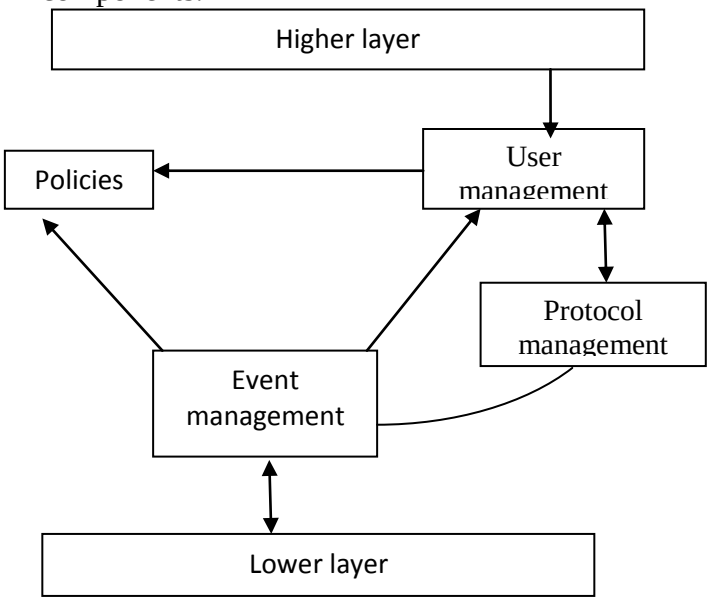
Fig1: NIST Role Engineering Model proposed in January, 2006

Initially, work profile is decided by an organization and stored along with organization data and content in a database. Based on the work profile, different roles are set and then assigned to users (based on his role) once connect session has been established. Based on functional role of users, access is granted to a data object stored in a database. This model is intended for (a) software engineers and development managers who design products incorporating access control features; and (b) managers and procurement officials who seek to acquire computer security products with features that provide access control capabilities in accordance with commonly known and understood terminology and functional specifications.

C. Access Model

The formation of a typical healthcare ad hoc network requires that authentication and database services are to be present to initiate formation of an ad hoc network. In case of typical ad hoc healthcare units, we assume that servers remain relatively stationary, and transmission and reception of communication remains largely confined within a specified area. Roles essentially partition database information into access contexts. Methods associated with a database object, also partition the object interface to provide windowed access to object information. By specifying that all database information is held in database objects and authorizing methods to roles, we achieve object interface distribution across roles. By authorizing different users to the different roles, we can enforce both the order of execution on the objects and separation of duty constraints on method execution. Because of space limitations in mobile devices, data is proposed to be at database server and then caching of events, registries and other services can be allowed on individual devices. Based on these guidelines and those in section 3.2, the role based access control framework in an ad hoc network is proposed of four components as shown in Figure 2. The framework runs on every user's device. In that, the event service collects and aggregates events and subsequently forwards them to the policy enforcement, e.g. the triggering of the execution of obligation policies. System events are forwarded to the protocol management, so that appropriate protocols can be performed. Events regarding the discovery of new communities are forwarded to the membership component of user management – other component being profile management. The profile management component maintains the user's credentials, such as key certificates and stores, and attributes certificates. Users can manage their credentials and device settings through user management interface. In addition, this component also maintains the user's preferences on which

communities the device should automatically join. The membership management component exposes the user management interface to the application level, so that applications can initiate the establishment of a new community, search for communities, as well as joining particular communities. Through this interface, the user can register the services that it is providing to other participants. The membership management component is also responsible for checking the authenticity of the doctrines and enforcing them by extracting and distributing the policy instances to various enforcement components.



IV. POLICY IMPLEMENTATION

In order to combine RBAC and XML to simplify operations within one process, the XML implementation of RBAC for healthcare unit operations in a typical ad hoc healthcare environment is explored in this section. It should, however, be noted here that for such an implementation, the user authentication and database services may be merged in one device, where all transaction processing takes place.

A. Access Security for a Healthcare Application

The database application chosen in this implementation is a healthcare centre, and termed as Basic Rural Healthcare Model (BRHCM). The selection of this model is arbitrary and is chosen as an implementation example, though a similar development can be devised for any ad hoc networking of healthcare unit devices. The data resides in out-patient records, in-hospital records, and family-visit records, and the transactions are executed on daily basis. The application is used by Basic Health Unit Manager, Doctors, Mother and Child Care Unit In charge to perform various transactions. It is also used by Nurses, Health Visitors, Operation Theatre (OT) in charge, and Office Assistant to post data. The Accounting Manager, Accountant and Internal Auditor post, generate and verify accounting data. The process of developing RBAC-based access control for this application is stated below.

(i) *Role definition and functions identification*

Based on various categories of participants that will use this ad hoc network application, the participating roles and functions required for each role can be defined as follows:

- Office Assistant: Input data in family folders regarding nutrition, and vaccination provided to respective family.
- Mother-Child Unit (MCU) in charge: Create and delete family folders in addition to tasks defined for office assistant.
- Health Visitor: Input/modify vaccination information of children under age 10; input and modify mother nutrition chart.
- Nurse: Input/modify in-patient record.

- Operation Theatre (OT) in charge: Input/modify OT record.
- Doctor: Create/modify/delete in-patient record; enter prescription; create/modify/delete OT record.
- Accountant: Input all health unit transactions and generate General Ledger Reports.
- Accounting Manager: In addition to accountant functions, the ability to modify Ledger Posting Rules.
- Internal Auditor: Verify all transactions and Ledger Posting Rules.
- Basic Health Unit In charge: Ability to perform any of the functions of other roles in times of emergency and to view all transactions, account statuses and validation flags.

(ii) Role Graph

Based on the intended functionality and privilege assignments required for each role, a structural relationship emerges among roles, as shown in Figure 3. It is clear from the figure that roles higher in hierarchy accumulate more privileges than the ones lower in hierarchy. The privileges set for any two roles which are not part of the same chain are disjoint.

(iii) Formulation of Constraints

a. The maximum number of users that can be assigned to Basic Health Unit In charge and Internal auditor is ONE.

b. The following pair of roles can not be assigned to the same user ("Static separation of Duty (SSD) or
Membership Mutual Exclusivity (MME)")

1. MCU In charge and Accounting Manager
2. MCU In charge and Internal Auditor
3. Doctor and Accounting Manager
4. Doctor and Internal Auditor
5. Accounting Manager and Internal Auditor
6. Nurse and Health visitor
7. Nurse and Office Assistant
8. OT Support staff and Office Assistant
9. OT Support staff and Health Visitor
10. Nurse and Internal Auditor
11. Nurse and Accounting Manager
12. Office Assistant and Accounting Manager
13. Office Assistant and Internal Auditor
14. Health visitor and Accounting Manager
15. Health visitor and Internal Auditor

c. The following pair of roles can not be activated or enabled at the same user session ("Dynamic separation of Duty (DSD) or Activation Mutual Exclusivity"):

1. Health Visitor and Accounting Manager
2. Office Assistant and Accounting Manager
3. Nurse and Accounting Manager
4. Operation Theatre and Accounting Manager

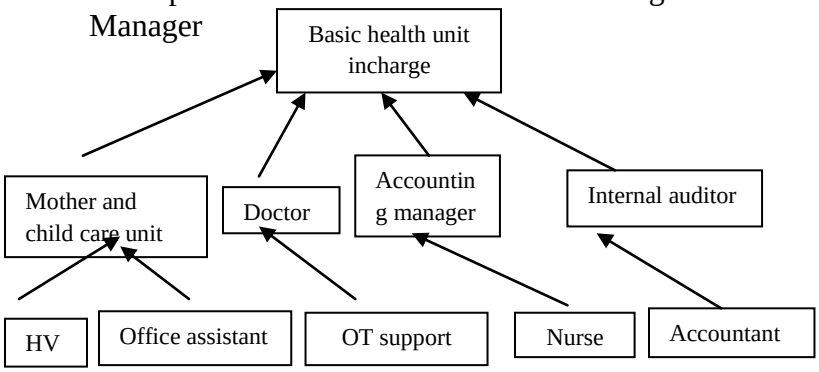


Figure 3: Role Structural Relationships

B. Representation of RBAC-based Access Control Data in an XML Document The next task is to define a Document Type Definition (DTD) that will represent the schema for the chosen RBAC Model for this application, and then to capture the actual data in a conforming XML document. A DTD provides the logical organization of the tags themselves that are used in an XML document. Several issues to be considered to define a DTD include the following:

a. Expressiveness: to capture the semantics of various RBAC model constructs.

b. Flexibility: Generic DTD to describe most common RBAC models.

c. Document Readability: That the conforming XML document is readable so that the logic of the RBAC implementation

program that parses this document is not unduly complicated. Since 'Expressiveness" and "Document Readability" have conflicting requirements, hence we have developed DTD for representing the RBAC model schema. The grid view of this DTD is shown in Figure 4. A fragment of the XML document that conforms to the DTD in Figure 4 (that contains RBAC-based access control data related to this application) is shown in Figure 5. Since a conceptual RBAC model is used for this application to create XML document, many commercial XML processors can be used to validate for conformance to the schema RBAC.dtd. These commercial processors parse an XML document and create a data structure whose contents are then accessed by application programs written in language like C++ or Java.

C. Implementation of RBAC Model for BRHCU using the

data in XML Model A Java program (say RBAC_XML_to_DB.java) to read data in XML document is written to parse the XML document and generate the internal Document Object Model (DOM) tree representation of XML document. This step is followed by navigating through this DOM tree to extract data related to roles, their relationships and constraints by navigating to the appropriate nodes. Using the semantics of extracted data, corresponding SQL queries are generated to either (a) create role or (b) specify a structural relationship or (c) a constraint involving previously created roles. These SQL queries are passed as parameters to appropriate Java Database Connectivity (JDBC) methods to implement them on the database (resource) server. The steps are repeated for all relevant nodes in the DOM tree.

Alternatively, these three steps may also be accomplished using a model as shown in Figure 4. The model is based on programming Microsoft SQL Server 2000 with XML. In Figure 4, the receiving application passes the XML document to a stored procedure in the database that inserts order data into the appropriate tables. It should, however, be noted here that when a stored procedure is written for inserting data from an XML document into the database, care should be exercised so that the parameter to be used to pass the XML data to the procedure is large enough to handle the maximum size of documents that are expected to be received in a healthcare environment. Further, the XML document needs to be parsed and mapped to in-memory tree structure that represents the nodes in the document. The stored procedure then returns a handle to a node tree that can be used to retrieve data from the elements and attributes in the document. The next step is to get XML data into a relational format so that it can be inserted into a table. This process is known as *shredding* the document. Finally, stored procedure contains *cleaning up* operation to reclaim the memory used by the node tree. In case of multiple database servers, which is more likely the scenario for healthcare databases, the access control restrictions across (say) two servers have to be identical. Since access control data is not an application

data, and is in fact stored in system tables, one way to implement RBAC model with identical data on two database servers is to extract relevant RBAC data from first server, express it in database server neutral format (like generating XML document) to conform to RBAC.dtd, parse that data to generate necessary SQL commands to implement RBAC policy on other server. The validating generation of the XML document may be processed, as before, using commercial processors.

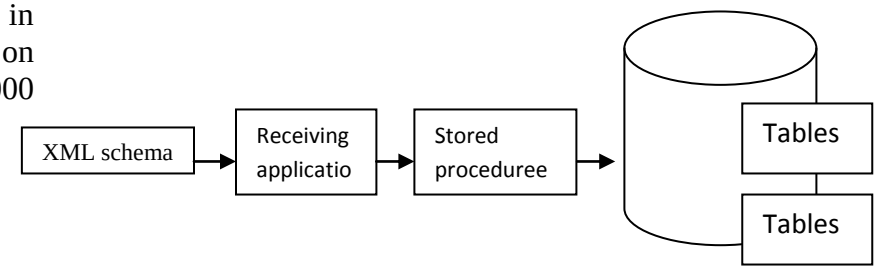


Fig 6: Receiving and inserting XML document in a database

VI. CONCLUSIONS

The main objective in this work was to guarantee the aspects of integrity, confidentiality, and accountability, a prime requirement for a healthcare application. The proposed setup helps integrating RBAC model with modern database server tools. We conclude that for any type of application where number of mobile devices is relatively small, the issues of role based access integrated with modern tools can easily be addressed to improve data and access security in an ad hoc network environment like healthcare. The setup drastically improves the efficiency of an IT manager, and enhances the security level of data and its transfer within an ad hoc network.

REFERENCES

[1]. Y. Hu et al. Ariadne "A Secure On-demand Routing Protocol for Ad hoc Networks", *Proceedings of the* 8th *ACM International Conference on Mobile Computing and Networking*, September 2002.

[2]. Y. Zhang and W. Lee "An Integrated Environment for Testing Mobile Ad-Hoc Networks", *ACM Symposium on Mobile Ad hoc Networking and Computing*, June 2002.

[3]. F. Stajano. "The Resurrecting Duckling –What Next?" *Proceedings of 8th International Workshop on Security Protocols*, 2000.

[4]. Dan C. Marinescu, *Internet-Based Workflow Management: Toward a Semantic Web*, ISBN: 0-471-43962-2, Wiley Publishers, April 2002.

[5]. J. Doshi, W. Aref, A. Ghafoor, and E. Spafford, "Security Models for Web-Based Applications", *Communications of the ACM*, Vol. 44, No. 2, pp. 38-44, February 2001.

[6]. Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R. "Proposed NIST standard for role-based access control", *ACM Transactions on Information and System Security*, 4 (2001) pp. 224-274.

[7]. Bertino, E., Bonatti, P.A., Ferrari, E. "TRBAC: A temporal role-based access control model", *ACM Transactions on Information and System Security* 4 (2001) pp. 191-223.

[8]. Qin, X. Berry, R., Qin, "Exploiting Multi-user Diversity for Medium Access Control in Wireless Networks", *Proceedings of INFOCOM*, Vol. 2, pp. 1084 – 1094, April 2002.

[9]. Cypher, D., Chevrollier, N., Montavont, N., Golmie, N., "Prevailing over Wires in Healthcare Environments: Benefits and Challenges", *IEEE Communications Magazine*, pp. 56-
63, April, 2006.

[10].Spyrou, S., Bamidias, P., Maglaveras, N., Pangalos, G., Pappas, G., "A Methodology for Reliability Analysis in Health Networks", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 12, No. 3, pp. 377-386, May, 2008.

