Mobile Healthcare Infrastructure with Qos and Security

Afsheen Mughal, Mohammed Kanjee, and Hong Liu

University of Massashusetts Dartmouth
Department of Electrical And Computer Enginering
285 Old Westport Road, North Dartmouth, MA 02740, USA
{amughal,mkanjee,hliu}@UmassD.edu

Abstract. This paper proposes a security framework with quality of service (QoS) mechanisms embedded in a Next Generation Internet architecture to support healthcare infrastructure with mobile wireless sensors. The framework shields the complexity of internetworking with a policy management system to subscribe quality of service and level of security. The framework also hides the intricacy of mobile wireless-networked sensors with a middle ware component to deliver sensing data and retrieve patient monitoring information. Complying with the Internet Design Philosophy, the complexity is pushed to the end processing nodes for healthcare information comprehension and manipulation. Both security and service requirements for healthcare infrastructure are achieved with the established architecture of Next Generation Internet.

Keywords: Next Generation Internet (NGI) architectures; security framework; Quality of Service (QoS) mechanisms; Mobile Wireless Sensor Network (WSN); Healthcare Sensor Network (HSN).

1 Introduction

Healthcare infrastructure deploys both the Internet and wireless sensor networks (WSN) to achieve mobility in monitoring patient conditions. Sensors attached to patients are used to monitor and measure vital signs such as patient's heart rate or body temperature [1]. Having these body area wireless sensors allows the patients to be mobile and not be confined to one area. Critically ill patients have to be put under constant bedside monitoring for the healthcare practitioners to effectively react in a timely manner in case of emergency. If these patients were allowed to be mobile they would benefit from physical exercise as well as better patient recovery in a favorable environment away from the hospital, without sacrificing effective reaction time during emergency. These measurements are sent periodically to the medical staff. Because of the sensitive nature of the data, it is critical to provide mechanisms to protect patient's medical files. Security becomes an important design goal in such applications. Sensor nodes have constraints in computation, memory and power resources, therefore, it becomes challenging when designing a secure WSN application [2]. A trade-off must be made between the level of security provided and the resources consumed.

Recently, there have been several WSN applications proposed and designed specifically for the medical and healthcare industry. These include CodeBlue

Y. Cai et al. (Eds.): Mobilware 2010, LNICST 48, pp. 462–473, 2010.

developed for emergency medical care [3], AlarmNet to monitor continuously assisted-living and independent-living residents [4], and SNAP (Sensor Network Assessment of Patients) with some security mechanism in its architecture [5]. Unfortunately, security issues have not been systematically addressed in Healthcare Sensor Network (HSN) applications [6]. Besides serious consequences led by patient data adversaries, the complying requirement with HIPAA (Health Insurance Portability and Accountability Act) makes security the top priority in all healthcare settings. However, before a potential security mechanism can be integrated into a HSN, we must understand and develop the measurement to assess and evaluate the requirements and security goals for the application.

The remaining paper is organized as the follows. In Section 2, we discuss possible threats and attacks a healthcare sensor network may face. Next, we examine the requirements and characteristics of the healthcare environment, which distinguishes it from other mobile wireless sensor network applications. Section 4 describes our Next Generation Internet (NGI) architecture of security framework enabled with Quality of Service (QoS) mechanisms for HSN applications. We give our conclusion and future work in the last section.

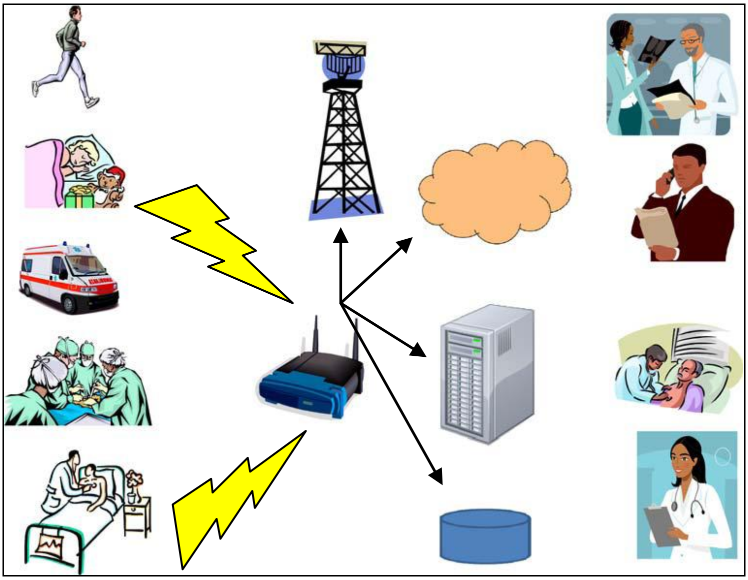

Fig. 1. Typical architecture of wireless sensor networks in healthcare applications [16]

2 Threats and Attacks on HSN

There are numerous different types of attacks or threats that a healthcare sensor network may face. These attacks can be classified according to the intended target: patient nodes or a healthcare system. A patient node attack is one in which the patient end is specifically targeted by malicious acts. In a healthcare system attack, the adversary aims to disrupt/destroy the link between the medical personnel and the patient nodes as well as the central system.

Attacks at the patient level include eavesdropping (snooping or traffic analysis), unauthorized modification, masquerading, and node compromising. Attacks at the system level include Denial-of-Service (DoS), system intrusion, and impostor.

A malicious sensor node intercepts and/or overhears packets which are being transmitted between a patient and a member of the medical staff. By overhearing packets not intended for it, an intruder can perform an analysis on the traffic patterns and potentially steal private and sensitive patient information. This leads to a violation of the patient's privacy. A malicious node can also gain information on the encryption scheme being used between the patient node and medical staff. This node can decrypt future communications between the patient node and medical staff. There can be a possible misuse of information by the malicious node.

Attacks can be classified into two abstract categories passive and active [16]. Passive attacks change the path of the information within the network in order to obtain specific information or to make routing inconsistent. Active attacks are more harmful in nature as they can be life threatening. They may try to corrupt vital patient information within the network, thereby preventing the monitoring entity to take the right action in a timely fashion. Some of the types of attacks that can be injected on a HSN are [16]

- Data Modification – The attack could modify or delete vital patient data and send the modified version back to the original receiver causing the patient to be misdiagnosed.
- Impersonation attack – The attack could eavesdrop and obtain the node identification information, which can be used to deceive other nodes.
- Eavesdropping – The attack could eavesdrop on information that is being sent on the open channel and use sensitive patient data for criminal acts.
- Replaying – The attack could reply stale information to the receiver and prevent real-time patient data from reaching the original receiver.

Security in HSN can be divided into two tiers [16]. The first tier consists of the System Security, which includes access to the physical systems – sensor nodes, gateways and centralized server. Accesses to these systems have to be controlled via measures of authentication and authorization and use of firewalls to prevent non-authorized users form assessing the system. System level security has to be applied at three levels – Administrative, Physical and Technical.

- Administrative Level Security is applied to check security breaches by the people who are responsible for system operation. Authentication measures along with access mechanism to prevent unauthorized users from accessing sensitive patient data.
- Physical Level Security is applied to prevent physical access to the devices attached to the patient and other equipment through which information is channeled or stored. These devices are open to attacks who would want to tamper with the devices in order to gain access to sensitive patient information. Physical Level Security is the hardest to implement in a distributed and scaled environment of HSN.

- Technical Level Security is implemented on hardware such as servers. In a network oriented design data is sent to central servers, server based security measures have to be implemented. Secure routing will have to be implemented to prevent attackers from causing routing inconsistencies resulting in erroneous destination. Due to sensitive nature of the data in the healthcare domain it is necessary to implement encryption schemes.

The second tier of security consists of Information Security, which prevents the tremendous amount of sensitive patient data traversing through the HSN to fall into the hands of attackers [16]. The data is at risk of sabotage, theft, exploitation and manipulation. The information security apparatus should be able to provide the following security services

- Data Encryption – Information traversing the HSN is encrypted so that it is not easy for eavesdroppers to gain access to data while it is in transit.
- Data Integrality – Sensitive patient information has to be authenticated against the sender, while also making sure that it stands the test of integrity. It provides against data modification attacks.
- Authentication – Various devices in the network have to be authenticated against some central system to make sure imposter devices are not induced into the HSN. False nodes masquerading as authentic devices can reroute sensitive information or induce false information into the HSN producing devastating effects for patients.
- Freshness Protection – Freshness provides protection against replay attacks.

3 Requirements and Security Goals in HSN

The main issue of the existing security solutions for HSN is that not all security goals or application requirements are satisfied. Although many security solutions have been proposed for WSN [7-9], they are not designed for healthcare in mind. Furthermore, among the HSN applications, not all have addressed security in their original design [3, 4]. As a result, a gap exists between the security requirements of HSN and the state-of-the-art WSN security solutions for medical applications.

Because HSN has different characteristics compared to other WSN applications, existing WSN security technologies are not suitable to or overkill HSN. The table below lists the key differences between a healthcare application and a general wireless sensor network.

Unlike a general WSN, a HSN application deploys two levels of different security goals: the node (patient) level and the system level. At the patient level, confidentiality ensures that patient's medical files are protected from eavesdropping or traffic analysis. Integrity prohibits altering medical reports, at the nodes as well as during transmission from patients to medical staff, by any external or unauthorized source. Patient data freshness keeps the information recent. Patient data availability ensures patient data obtainable to doctors and other medical personnel at all times. Authentication verifies the legitimacy of an entity while authorization grants the access to that confirmed entity to access the patient data.

A healthcare sensor network is a network of sensors deployed on human bodies to monitor patients' health. These sensors collect personal medical data, therefore, security and privacy are important requirements in healthcare sensor networks. At the same time the network should be able to transmit the data in a robust manner in order for it to be readily available in case of a medical emergency. Any delay or latency can prove to be fatal for the patient if the medical staff is not able to respond in time.

Despite the increased range of potential health care applications – ranging from pre-hospital, in-hospital, ambulatory and home monitoring, to long term database collection for analysis – the security gap that exists between wireless sensor networks and the requirements of the medical applications and community has yet to be resolved. Wireless sensor networks are limited in terms of power and computation, and are deployed in areas where they can be easily accessed causing security vulnerabilities. Dynamic ad hoc topology, multicast transmission, location awareness, critical data acquisition, and co-ordination of diverse sensors of health care applications further exacerbate the security challenges [1].

Table 1. Contrast HSN vs. WSN

Characteristics	**Healthcare**	**Wireless Sensor Network**
Energy Efficient	Batteries replaced by medical staff	Energy source not usually replenish
Privacy	Protect from unauthorized users	
Real-Time Response	Time-critical	Delay tolerable
Accurate Patient Results	For better treatment/diagnose	Application-dependent
ID-Centric Addressing	Patient identity as important as data	Data-Centric addressing scheme
In-network Processing	Limited redundancy	Communication cost reduction
Robustness	Limited redundancy	Node failure tolerable
Scalability	Vary patient density	Nodes enter/leave network
Mobility	Both patients and doctors are mobile	Application-dependent

Table 2. Compare Node vs. System

Security Goals	**Patient Level**	**System Level**
Confidentiality	YES	
Integrity	YES	
Freshness	YES	
Availability	YES	YES
Authentication	YES	YES
Authorization	YES	YES

Sensor nodes in the healthcare environment are semi-permanently deployed, since the topology of such networks changes over time, due to new sensors being introduced into the environment and in the case of mobile patients, the patients themselves moving in and out of the network. Since each sensor node is acquiring critical medical data the nodes should be able to coordinate with each other with to acquire the data, perform computation and selection to transmit the required information. The purpose of deployment of sensor nodes in the healthcare environment is to allow patients to be mobile and not be confined to one location; some type of location awareness implementation is required. This implementation becomes even more critical if security is involved, as the security key shared between a group of sensors and the cluster node would change if the group of sensors transgresses into an area covered by another cluster node.

At the network level, availability guarantees that the system remains operational 24/7. Authentication is used to establish legitimate communication between sensor nodes and the system. Authorization is used to make sure that authorized medical personal are accessing patient data. Once authentication and authorization are in place, confidentiality and integrity would be implied at the system level. Therefore, confidentiality, integrity, and freshness (guaranteed by patient nodes) have no need to be addressed specifically at the system level. Table 2 summarizes our findings.

4 Our Approach: NGI Architecture

A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or closely around it. The positions of sensor nodes need not be engineered or predetermined, which allows random deployment in an inaccessible terrain or disaster relief operations. On the other hand, such a feature requires self-organizing capabilities in sensor network protocols and algorithms. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensors fit with an onboard processor, instead of sending raw data to a cluster head responsible for data fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit processed data.

In healthcare applications, sensor nodes are deployed to monitor patients and assist disabled. Our research is focused on designing a wireless sensor network that collects, transmits, and processes sensitive patient information for medical personals to monitor patients in real time. Since security is of significant challenge in transmitting data wirelessly and timely, we propose a security architecture enabled Quality of Service (QoS) to support mobile healthcare infrastructure. Our approach is unique in that we place security in the center of the architectural design. The goals of our research are to

- Develop an architectural design that positions security as a core component,
- Implement a security structure that provides low latency encryption and decryption, and
- Design security algorithms that are not resource intensive, permitting its deployment on sensor nodes.

We present our work in five subsections. Subsection 4.1 describes our two-tier architecture that places security in its core design and makes security implementation feasible under resource scarce computing environment. Our assumptions of sensor nodes are given in the second subsection. The next two subsections discuss the two tiers: the low-tier structure is a middle ware to shield the diversity of sensing nodes in security implementation, and the high-tier structure deploys policy management for the Next Generation Internet (NGI) to adapt changes in security requirements. The assessment of our architecture towards its design goals is shown in Subsection 4.5.

4.1 Two Tier Architecture

Our two-tier networking architecture untangles long haul medical communications on the Internet from short-range transmissions within individual wireless clusters of patient sensor nodes. The low-tier structure deals with diverse patients' data: being assistant living, clinic heart monitoring, or a sudden epidemic like swine flu. The high-tier structure provides medical staff communication, real-time observation, or health data processing. Naturally, the patient-oriented low tier contains wireless sensor networks while the doctor-oriented high tier deploys the Internet. Figure 2 depicts our two-tier architecture. The two tiers interact as if each wireless cluster of patient sensor nodes is a periphery of a medical system plugged through an end node of the Internet.

The two tiers possess drastically divergent features that lead to different approaches. For security, the low tier fulfils the security goals at the patient level, listed in Table 2,

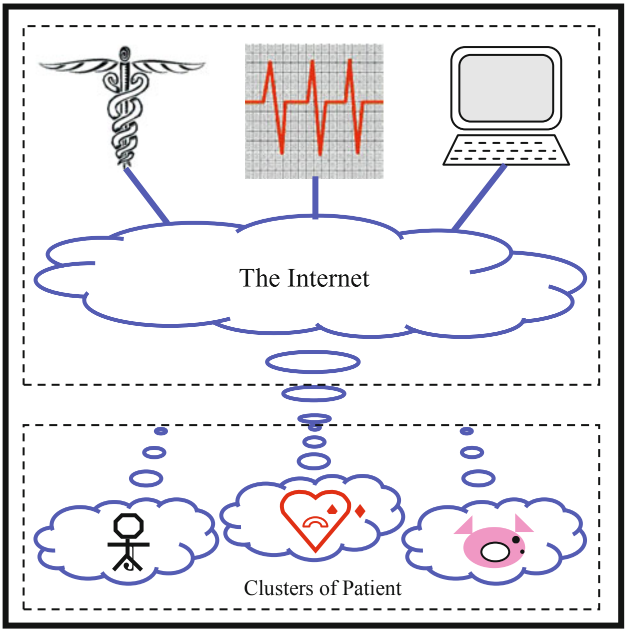

Fig. 2. Two Tier Architecture

while the high tier covers those at the system level. However, a secured infrastructure would diminish its purpose if it provides poor Quality of Service (QoS) such as data loss and long delay. For QoS requirements, the high tier, using the Internet, has the traditional QoS issues that can be dealt with mechanisms proposed for the Next Generation Internet (NGI), to be discussed in Subsection 4.4. The low tier, composed of wireless sensor networks (WSN), faces new QoS challenges due to unreliable communication service of wireless links and limited computation resource of sensor nodes. Pay attention to the unique characteristics of healthcare sensor network (HSN) summarized in Table 1; Subsection 4.3 presents our solution.

The two tiers possess drastically divergent features that lead to different approaches. For security, the low tier fulfils the security goals at the patient level, listed in Table 2, while the high tier covers those at the system level. However, a secured infrastructure would diminish its purpose if it provides poor Quality of Service (QoS) such as data loss and long delay. For QoS requirements, the high tier, using the Internet, has the traditional QoS issues that can be dealt with mechanisms proposed for the Next Generation Internet (NGI), to be discussed in Subsection 4.4. The low tier, composed of wireless sensor networks (WSN), faces new QoS challenges due to unreliable communication service of wireless links and limited computation resource of sensor nodes. Pay attention to the unique characteristics of healthcare sensor network (HSN) summarized in Table 1; Subsection 4.3 presents our solution.

4.2 Sensor Node

As shown in Figure 3 below [2], a sensor node consists of four units: a sensing unit, a processing unit, a transceiver unit, and a power unit. A sensor node might also equip some application-driven components such as a location finding system, a mobilizer, and a power generator. Its sensing unit contains sensors and analogue-to-digital converters (ADC). It performs sensing data and delivers the data to the processing unit for analyses. The processing unit has a processor and a small storage. The transceiver unit transmits the processed data and receives control signals for nodal

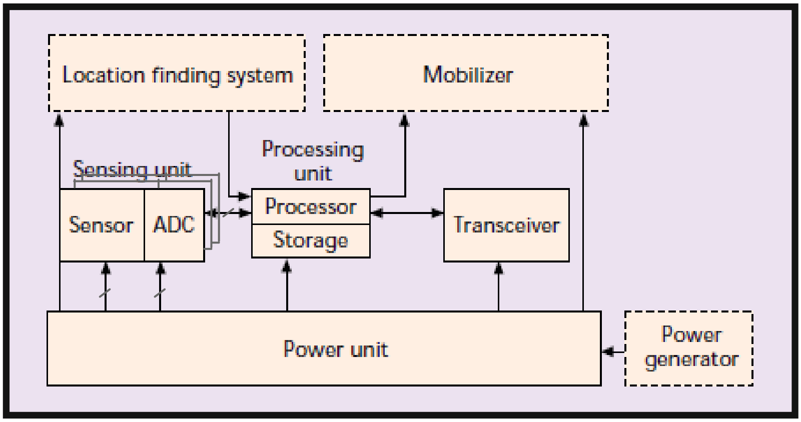

Fig. 3. Components of a Sensor Node

reconfiguration or for data relay. The power unit supplies electricity. For mobile patients, a location finding system keeps track of him for emergency response. Most medical sensor nodes, wearable, do not need a mobilizer to propel the node. A power generator is included if the node does not use batteries or a wall plug.

Process/storage limitation and real-time requirement are the driving forces behind the design of a security protocol tailored for HSN.

4.3 Low-Tier Structure: Middle Ware

The low tier is a sky topology of wireless sensor networks (WSN), each of which is a star topology. A star stems at a Base Station and rays in several Cluster Heads, as shown in Figure 4. Although the figure provides one cluster head for each patient, a cluster head can accommodate several patients geographically nearby without increasing computational complexity because only simple addressing not routing is involved to locate a patient under a cluster. A *Patient Node* deploys sensors to gather various medical data such as temperature, blood pressure, and EKG. It then processes/encrypts data and sends them to its cluster head located in the near vicinity. A *Cluster Head* in our HSN does not deploy any sensors, and its function is to fuse and relay data. A *Base Station* acts as the interface between the low tier and the high tier.

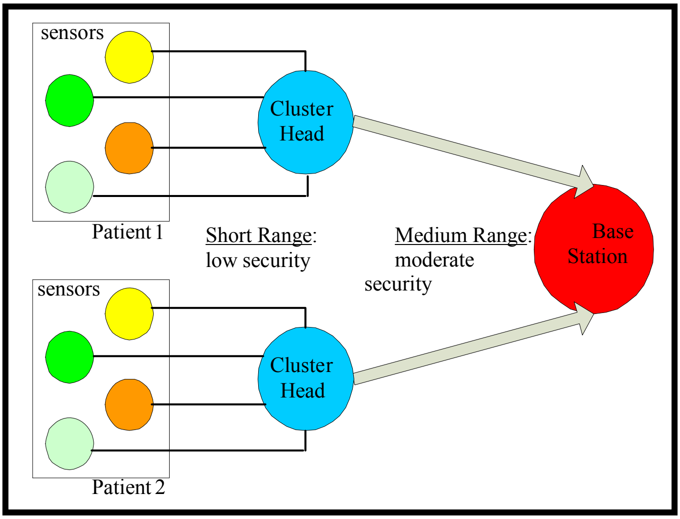

Fig. 4. A Star in Low Tier

The distances from the sensors of a patient node to its cluster head are short, body length in our prototype. The short range of communication minimizes interception of data by foreign entities; therefore, a low degree of security is sufficient enough for ad hoc settings as individual patients come and go. Even with the resource limitation on these nodes, it is feasible to develop low-latency or real-time security protocols for patient's sensor nodes and its cluster head with small overhead on encryption.

Communications between cluster heads and their base station is medium range, vulnerable to security breaches. Fortunately, cluster heads and a base station have abundant resources, capable of running a moderate degree security protocol without causing much latency [10, 11].

A star topology easily houses a *Middle Ware*, a warehouse of software/ firmware/hardware to process data for security and QoS while hide the intricacy of various wireless networking and sensing technologies. To counterattack *Traffic Analysis*, study of traffic patterns without knowing their contents, the transmissions both of short range (from patient's sensors to its cluster head) and of medium range (from cluster heads to the base station) are kept in regular intervals. All data in transmission at the low tier are encrypted, and no decryption is involved until the base station. This simplicity works as a double-edged knife that ensures the desired level of security in Table 2 and promises QoS with ignoble loss, low delay, and no jitter in Table 1. Depending on its configuration dictated by the policy (to be discusses in the next subsection), a base station filters traffic before forwards it to the high tier. It uses partial decryption (full decryption at medical systems of the high tier) and prunes noise/insignificant traffic to reduce aggregated traffic towards the high tier.

4.4 Low-Tier Structure: Middle Ware

The high tier incorporates policy management into the differentiated service (DiffServ) model for the Internet. *DiffServ* is the most prominent QoS model for NGI, evolving from the original Internet with a best-effort service model, by handling classes of traffic in different ways. Instead of trying the best to deliver all packages equally poor, a DiffServ-capable router offers subscribed QoS to aggregated traffic by their service class [12]. DiffServ routers are classified into edge routers and core routers. An *Edge Router*, at the "edge" of the Internet, connects to end systems, base stations of the low tier or medical systems of the high tier in HSN. A *Core Router*, within the Internet, finds a path to forward a packet with the QoS by that packet's class. Figure 5 depicts policy management in DiffServ. A Policy Enforcement Point (PEP), added to each edge router, executes configured policies. A Policy Decision Point (PDP) performs complex policy interpretations for PEPs [13]. The Policy Information Base (PIB) stores policies, which is created and maintained by a Policy Management Tool (PMT) whose performance is feedback by a QoS monitoring at each edge router.

Policy management in DiffServ has been successfully applied to offer QoS by major Internet Service Providers (ISP) [14] and to combat Denial-of-Service attacks [15]. Applied to support mobile healthcare infrastructure, we need to address the QoS requirements in Table 1 and the three security goals at system level in Table 2. Real-time response [14] and system availability [15] at the high tier are readily done. New policies need to be developed for authentication and authorization.

4.5 Assessment

We have conducted qualitative evaluations of our architecture's suitability to healthcare. As discussed in Subsections 4.3 and 4.4, both the two tiers satisfy the QoS requirements in Table 1; the low tier achieves the security goals in Table 2 at the patient level while the high tier at the system level. The details of our assessment with a prototype will be presented in a sequel paper.

We need to design a quantitative matrix for assessing performance vs. efficiency with respect to its real-time response, data accuracy, privacy protection, system vulnerability, scalability, and mobility. We also need to devise a comparative study of our architecture with other architectures applicable to healthcare.

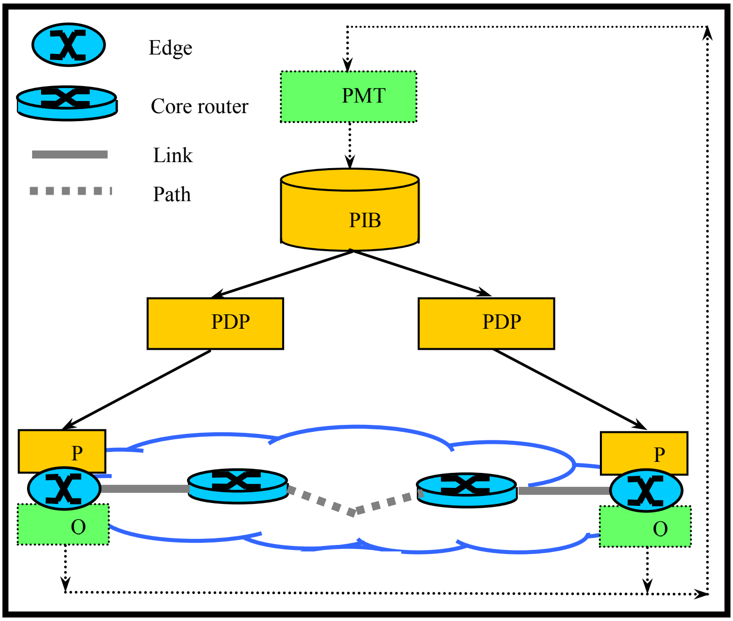

Fig. 5. Policy Management in High-Tier

5 Conclusion

This work is the first attempt to provide security in mobile healthcare infrastructure at architectural level. The unique two-tier architecture offers end-to-end total security from patients to doctors across long haul internetworking and covering wireless communication islands. The secure framework with QoS mechanisms oversees complicated processes of security and quality assurance with ease, where existing piecewise protocols/algorithms fit seamlessly and new ones would be justified to fill in security holes. The low tier also acts as a middle ware to hide the diversity of wireless medical sensing techniques, and the high tier utilizes NGI's DiffServ model enhanced with policy management to outlive the unpredictable security challenges.

Another contribution is the unique approach we use to solve security problems. Instead of focusing on surfaced problems, we analyze the characteristics of the application and identify its security goals. We let the application lead to a natural architecture for security and design testing procedures before a purposeful implementation. The method is applicable to other field of WSN applications.

The architecture lays a grant future work. Besides its self-correction, we need to choose and design specific security techniques for its components. We also need to assess the work systematically.

References

[1] Tan, C.C., Wang, H., Zhong, S., Li, Q.: Body sensor network security: an identity-based cryptography approach. In: Proceedings of the 1st ACM Conference on Wireless Network Security, Alexandria, VA, USA, March 31-April 02, 2008, pp. 148–153 (2008)

[2] Karl, H., Willig, A.: Protocols and architecture for wireless sensor networks. Wiley, Boston (2007)

[3] Malan, D., Fulford-Jones, T., Welsh, M., Moulton, S.: Codeblue: An ad hoc sensor network infrastructure for emergency medical care. In: International Workshop on Wearable and Implantable Body Sensor Networks (2004)

[4] Wood, A., Virone, G., Doan, T., Cao, Q., Selavo, L., Wu, Y., Fang, L., He, Z., Lin, S., Stankovic, J.: ALARM-NET: Wireless sensor networks for assisted-living and health monitoring, Technical Report CS-2006–01, University of Virginia (2006)

[5] Malasri, K., Wang, L.: Addressing security in medical sensor networks. In: Proceedings of the 1st ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments, San Juan, Puerto Rico, June 11-13 (2007)

[6] Wang, Y., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials 8(2), 2–23 (2006)

[7] Malan, D.J., Welsh, M., Smith, M.D.: Implementing public-key infrastructure for sensor networks. ACM Transactions on Sensor Networks 4(4), 22–45 (2008)

[8] Karlof, C., Sastry, N., Wagner, D.: TinySec: A link layer security architecture for wireless sensor networks. In: Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems, Baltimore, Maryland, USA (2004)

[9] Liu, A., Ning, P.: TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In: Proceedings of the 7th International Conference on Information Processing in Sensor Networks, April 22-24, pp. 245–256 (2008)

[10] Kurian, J., Sarac, K.: A security framework for service overlay networks: access control. In: BroadNets 2008, Internet Track 3: Overlays and Traffic Estimation London, UK, September 8-11 (2008)

[11] Wang, Y., Ramamurthy, B., Xue, Y., Zou, X.: A key management framework for wireless sensor networks utilizing a unique session key. In: BroadNets 2008, Wireless Track 6: MAC and Key Management London, UK, September 8-11 (2008)

[12] Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: An architecture for differentiated services. RFC2475 (December 1998)

[13] Rajan, R., Verma, D., kamat, S., Felstaine, E., Herzog, S.: A policy framework for integrated and differentiated services in the Internet. IEEE Network, 36–41 (September 1999)

[14] Liu, H., Dempsey, H.H.: Multi-facet Internet resource management system. In: Proceedings of IFIP/IEEE International Symposium on Integrated Network Management (IM), Boston, MA, USA, May 24-28 (1999)

[15] Yu, Q., (Liu, H., advisor): Denial-of-Service Countermeasure with Immunization and Regulation: Ph.D. Dissertation University of Massachusetts Dartmouth, Dartmouth (2005)

[16] Ameen, M., Jingwei, L., Kyungsup, K.: Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. Journal of Medical Systems (March 2010)