Data classification and scheduling for sensor virtualisation scheme in public healthcare system

Md. Motaharul Islam

Department of Computer Science and Engineering,
Islamic University of Technology,
Board Bazar, Gazipur-1704, Bangladesh
Email: motahar@iut-dhaka.edu

Mohammad Mehedi Hassan and Atif Alamri

College of Computer and Information Sciences,
King Saud University,
Riyadh 11543, Kingdom of Saudi Arabia
Email: mmhassan@ksu.edu.sa
Email: atif@ksu.edu.sa

Eui-Nam Huh*

Department of Computer Engineering,
Kyung Hee University,
1 Seochon-dong, Giheung-gu,
Yongin-si, Gyeonggi-do 446-701, South Korea
Fax: +82-31-204-3778,
Email: johnhuh@khu.ac.kr
*Corresponding author

Abstract: It is really surprising that most of the sensor nodes in wireless sensor network (WSN) remain idle for maximum period of its lifetime resulting underutilisation of resources. There are many ongoing researches to utilise WSN resources in an efficient way. Virtualisation of sensor network (VSN) is one of the novel approaches to utilise physical infrastructure of WSN. VSN can be simply defined as the virtual version of WSN over the physical sensor infrastructure. By allowing sensor nodes to coexist on a shared physical substrate, VSN may provide flexibility, cost effectiveness and manageability. This paper proposes quality of service (QoS) aware data classification and scheduling framework for VSN in the healthcare sector. We develop a tiny virtual machine called VSNware for healthcare application which facilitates QoS aware data classification and scheduling ensuring reliability, delay guarantee and speed. Simulation results also show that proposed scheme over performs conventional WSN approaches.

Keywords: VSN; virtualisation of sensor network; WSN; wireless sensor network; data classification; data scheduling; healthcare; overlay network; virtual network.

Reference to this paper should be made as follows: Islam, M.M., Hassan, M.M., Alamri, A. and Huh, E-N. (2016) ‘Data classification and scheduling for sensor virtualisation scheme in public healthcare system’, *Int. J. Sensor Networks*, Vol. 22, No. 4, pp.259–273.

Biographical notes: Md. Motaharul Islam received the BS in Computer Science and Information Technology from the Islamic University of Technology, Dhaka, Bangladesh in 2002. He obtained Masters of Business Administration in Management Information System in 2008. In 2013, he completed his PhD in Computer Engineering from the Innovative Cloud and Security (ICNS) Laboratory of Kyung Hee University, South Korea. He worked as a Faculty in the Institute of Scientific Instrumentation, University Grants Commission (UGC) of Bangladesh since 2006. Currently, he is an Assistant Professor in the Department of Computer Science and Engineering at Islamic University of Technology. His research areas are smart internet of things, network virtualisation, IP-WSN etc.

Mohammad Mehedi Hassan is an Assistant Professor of Information Systems Department in the College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia. He received his PhD in Computer Engineering from Kyung Hee University, South Korea in February 2011. His research interests include cloud collaboration, multimedia cloud, sensor-cloud, mobile cloud, thin-client, grid computing, IPTV, virtual network, sensor network and publish/subscribe system.

Atif Alamri is the Chairman of Information Systems Department in the College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia. He received his PhD in Computer Science from University of Ottawa, Canada in 2010. His research interests include multimedia -assisted health systems, ambient intelligence, rehabilitation, multimedia cloud, sensor–cloud, wireless sensor network, social network, privacy and security. He was the Guest Associate Editor of the *IEEE Transactions on Instrumentation and Measurement* in 2011, a Co-Chair of the first *IEEE International Workshop on Multimedia Services and Technologies for E-health*, a Technical Program Co-Chair of the *10th IEEE International Symposium on Haptic Audio Visual Environments and Games*, and serves as a Program Committee Member of many conferences in multimedia, virtual environments, and medical applications.

Eui-Nam Huh has earned BS from Busan National University in Korea, Master's degree in Computer Science from the University of Texas, USA in 1995 and PhD from the Ohio University, USA in 2002. He has been an Editor of *Journal of Korean Society for Internet Information and Korea Grid Standard Group Chair* since 2002. Now, he is serving as a Professor in the Department of Computer Engineering at Kyung Hee University, South Korea. His interesting research areas are cloud computing, ubiquitous computing, high performance network, sensor network, distributed real time system, grid, and network security. He is a Member of ACM and IEEE.

1 Introduction

Recent advances in electronics and communication systems have enabled the development of multifunctional smart sensor nodes that are small in size and communicate untethered over short distances. A sensor network consists of a large number of tiny sensor nodes that are densely deployed over a specific target area (Akkaya and Younis, 2005; Akyildiz et al., 2002; Islam and Huh, 2011a, 2011b). There is a robust deployment of WSN in healthcare sector for its miniaturisation. Today's smart sensor node can efficiently monitor different vital signs such as cardiac data, temperature, blood pressure, pulse rate and saturation of peripheral Oxygen (SPO_2) etc. of a patient. In case of healthcare scenario, applications demand different types of QoS requirement such as reliability, end to end delay, speed and timeliness. There are lots of ongoing efforts to enhance the QoS issues of WSN in the existing literatures (Felemban et al., 2006; Alam et al., 2009; Razzaque et al., 2008). In this age of recession providing QoS in WSN-based healthcare system with affordable cost is a big challenge for worldwide increasing elderly population which is the largest demographic group of the developed countries. For this very reason, researchers are searching cost effective way to support QoS in WSN for global healthcare sector.

Very recent, network virtualisation has created a resonance among the network research communities. The concept of sensor virtualisation has also attracted a great deal of attention from industry to academia (Islam et al., 2010, 2012). Virtualisation of sensor network (VSN) can be as defined as the separation of function for the traditional WSN service provider in two parts: sensor infrastructure provider (SInP) that manages the physical sensor infrastructure, and VSN service provider (VSNSP) that develops VSN by aggregating resources from multiple SInPs and offer services to the application level users (ALU).

WSN virtualisation renaissance has been started mainly from the realisation that maximum numbers of the sensor nodes remain idle for most of the time. Virtualisation is one of the best ways to utilise the physical sensor infrastructure. VSN can provide a platform upon which novel sensor network architectures can be built, experimented and evaluated. In addition, virtualisation in WSN is expected to provide a clean separation of services and infrastructure and facilitate new ways of doing business of sensor network resources among multiple service providers and application level users (Islam et al., 2012).

In this paper, we propose QoS aware data classification and scheduling framework for healthcare system in VSN environment. Sensor node senses data in parallel and forward it to nearby node or gateway node. Gateway node classifies data into urgent, suspicious, moderate and normal. Classified data are passed through the decoding module and queued up in VSN queues. Finally, scheduling module sends data to the specific path based on the delay, reliability and priority requirements of data packets. The main contributions of this paper are as follows:

- a business model for VSN has been proposed
- VSN-based public healthcare scenario has been depicted
- a tiny virtual machine called VSNware for healthcare has been developed
- data classification and scheduling mechanism for VSN have been suggested
- a detailed probabilistic model of delay and reliability for different data traffics has been proposed

- finally, simulation results of the proposed scheme are presented.

The remainder of the paper is organised as follows. Section 2 reviews the background related to virtual sensor network; overlay sensor network, VSN business model, related works and VSN-based public healthcare scenario. In Section 3, we discuss VSN architecture, detail model of sensor node and of sensor gateway router. Section 4 describes classification and scheduling of data packets. Sections 5 and 6 discusses a detailed mathematical model of delay and reliability for different class of data traffics. Section 7 shows the VSN network model. Section 8 presents evaluation and simulation results and finally Section 9 concludes the paper.

2 Backgrounds

VSN is a brand new research approach in the field of WSN. Before proceeding further, we need to clarify few basic concepts and the difference between VSN and conventional virtual sensor network. In brief, a traditional wireless sensor network consists of a large number of sensor nodes that are densely deployed either inside the phenomenon of interest or very close to it (Akyildiz et al., 2002). In this paper, VSN means virtualisation of WSN as defined in the introduction and in Section 2.3. The term VSN in this paper is synonymously used for the process of virtualisation of sensor network and for the network that support virtualisation.

2.1 Virtual sensor network

Virtual sensor network consists of collaborative wireless sensor network. It is formed by a subset of sensor nodes of a wireless sensor network, with the subset being dedicated to a certain task or an application at a given time (Kabadayi et al., 2006; Shin and Park, 2007). On the other hand, subset of nodes belonging to the virtual sensor network collaborates to carry out a given application at a specific time. It can be formed by providing logical connectivity among collaborative sensor nodes. Nodes can be grouped into different virtual networks based on the phenomenon they track or the task they perform. Its protocol should provide the functionality for network formation, usage, adaptation, and maintenance of subset of sensors collaborating on a specific task (Bandara et al., 2008).

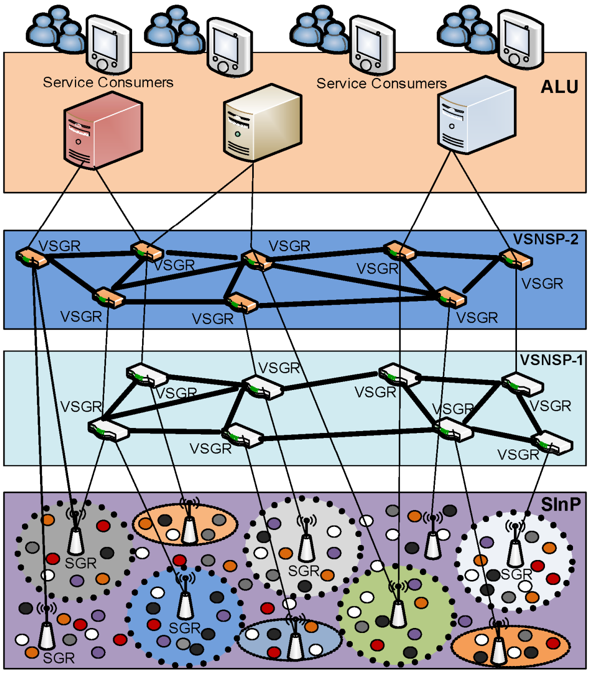
2.2 Overlay sensor network

An overlay sensor network is a type sensor network that creates a virtual topology on top of the physical topology of a WSN. Nodes in an overlay network are connected through virtual links which correspond to paths in the underlying network. Overlays are typically implemented in the application layer, though various implementations at lower layers of the network stack do exist (Waharte et al., 2004).

2.3 VSN and its business model

Unlike the conventional WSN, VSN environment has a collection of multiple heterogeneous sensor nodes that coexist in the same physical space. SInP in Figure 1 deploys different sensor nodes. In traditional WSN infrastructure provider and service provider are same entity. VSN differentiates between infrastructure provider and service provider thus provides a business model of true virtualisation.

Figure 1 Business model for VSN (see online version for colours)



SInP deploys sensor network resources. It offers resources through programmable interfaces of sensor gateway router (SGR) to different VSNSPs. Different interest group can deploy sensor node and can make individual infrastructure which can be used by VSNSP through different virtual sensor gateway router (VSGR) to run individual applications. VSNSP gets resources from multiple SInPs to deploy VSNs by sharing allocated virtualised network resources to offer end to end application user services. VSNSP can achieve resources from multiple SInPs. ALUs in VSN model are similar to those of the existing WSN, except that the existence of multiple VSNSPs from competing SInPs provides a wide range of choice. Any end user can connect to multiple VSNSPs from different SInP for using multiple applications.

2.4 Related works

Currently there are few approaches in the WSN (Felemban et al., 2006; Kabadayi et al., 2006; Shin and Park, 2007; Waharte et al., 2004; Leontiadis et al., 2012; Efstratiou et al., 2010; Hussain et al., 2009) that focus on the virtual and overlay sensor network rather than the purist view of VSN approach introduced in this paper. Table 1 summarises the area of a few of research projects that act as the background of the proposed research approach. It demonstrates the contemporary research direction in the field of virtualisation of sensor network in general.

Table 1 VSN research related projects

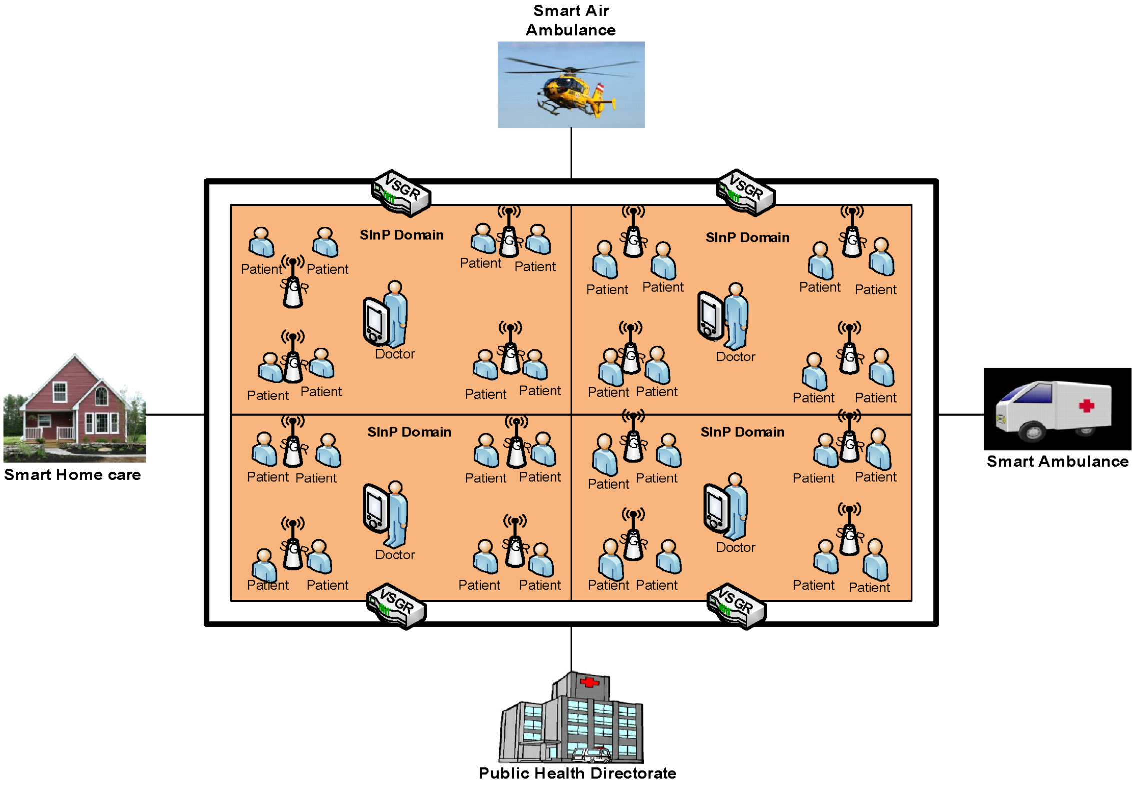
Projects	*Research area*	*URL*
FRESnel	To build a large scale federated sensor network framework with multiple applications sharing the same resources	http://www.cl.cam.ac.uk/research/srg/netos/fresnel/index.html
VSNs	Random routing, virtual coordinates, and VSN support functions	http://www.cnrl.colostate.edu /Project/VSNs/vsns.html
Sensor planet	Nokia-initiated cooperation, a global research framework, on mobile device-centric large-scale wireless sensor networks	http://www.sensorplanet.org/
ViSE	Virtualisation of sensor/actuator system, creating customised virtual sensor network test beds	http://groups.geni.net/geni/wiki/ViSE
DVM	To build a system that supports software reconfiguration in embedded sensor networks at multiple levels	http://nesl.ee.ucla.edu/project/ show/51
SensEye	Multi-tier multi-modal sensor networks	http://sensors.cs.umass.edu/projects/senseye/
SenQ	Complex virtual sensors and user-created streams can be dynamically discovered and shared	http://www.cs.virginia.edu/wsn/medical/projects/senq
WebDust	Multiple, heterogeneous, wireless sensor networks can be controlled as a single, unified, virtual sensor network	http://ru1.cti.gr/projects/webdust

Recently federated secure sensor network laboratory (FRESnel) aims to build a large scale sensor framework. The goal of this project is to offer an environment that can support multiple applications running on each sensor node (Leontiadis et al. 2012; Efstratiou et al., 2010). It provides an execution environment that hides the system details from the running applications. The system operates in a shared environment. The key characteristic of this approach is a virtualisation layer that is running on each sensor node. It provides abstract access to sensor resources which allows the management of resources through policies expressed by the infrastructure owner. A runtime environment on each node allows multiple applications to run inside the sensor node. It also provides policy-based application deployment that enables multiple applications to be deployed over the shared infrastructure. In MMSPEED (Felemban et al., 2006), a novel packet delivery mechanism for QoS provisioning in WSN has been proposed. It provides QoS differentiation in two quality domain such as timeliness and reliability. This approach is based on multiple logical speed layers over a physical sensor network which is based on conventional virtual sensor network. On the basis of the speed, it considers different virtual overlay. For virtual layering it employs virtual isolation among the speed layers. It is accomplished by classifying incoming packets according to their speed classes and placing them into the appropriate priority queue. SenShare (Leontiadis et al. 2012) is another platform that attempts to address the technical challenge of supporting multiple co-running applications in the sensor node. Here each application operates in an isolated environment consisting of an in-node hardware abstraction layer and a dedicated overlay sensor network. Instead of using virtual machine, SenShare use a hardware abstraction layer. It is a set of routine in software that emulates some platform specific details, giving programs direct access to the hardware. Mate (Levis and Culler, 2002) and Melete (Yu et al. 2006) systems are based on the virtual machine approach that provides reliable storage and enables execution of concurrent applications on a single sensor node. VSN approach proposed in this paper is based on Mate and Melete system. We name the modified version of proposed virtual machine as VSNware. VSNware provides an environment to support sensing different application's data for healthcare system such as cardiac data, blood pressure, blood sugar and temperature sensing. VSNware helps to provide the purist view of virtualisation concept. It is possible by dint of separation between SInP and VSNSP which is discussed in the previous sections. By applying the purist view of virtualisation in VSN, this scheme can be efficiently used in healthcare system which is the main contribution of this paper. To the best of our knowledge none of the research paper explores VSN approach for designing a ubiquitous healthcare system for QoS-based vital data classifications and scheduling scheme.

2.5 VSN-based public healthcare scenario

VSN is envisioned to be heavily used in patient care environments especially in the cloud computing-based public healthcare system. The world is rapidly graying. The speed with which this age-structural change is taking place implies an urgent need for solutions that will relieve the mounting pressure over the healthcare systems as well as support a better quality of life and quality of care for the aged populations. With this thinking in mind, we depict a VSN-based patient care scenario which is shown in Figure 2. We consider here a multipurpose specialised hospital. In different floors of the hospital there are different types of patient care unit.

Figure 2 VSN based public healthcare scenario (see online version for colours)



Different floors are considered as individual SInP domain. SInP domain consists of a lot of smart sensor node and SGR. There are different VSGR that provide SVNSP support for multiple applications. Sensor nodes are deployed on the body of the patients as well as all over the surrounding environment. Doctors may always monitor the patients online. A patient can get special care both in the state of the art hospital and smart home care. In case of emergency, patient can also obtain medicare from smart ambulance, from smart air ambulance. For the emergency medical and infrastructural support, it is connected to the public health directorate. The patient care unit ensures real time care and observation of the patients from a central specialised doctor's forum. In case of emergency, patient can move from one place to another with its complete set-up so that seamless connectivity with the sophisticated medical equipment remains established and doctor can monitor the patient online from the central doctor's research group.

3 Architecture of VSN

3.1 System architecture

Here, we briefly describe the detail system architecture, software architecture of the sensor node and sensor gateway router (SGR). In the following sections, we will explain the architecture in details. The system architecture consists of three layers SInP, VSNSP and ALU. The software architecture describes the virtualisation of the individual sensor node and gateway router.

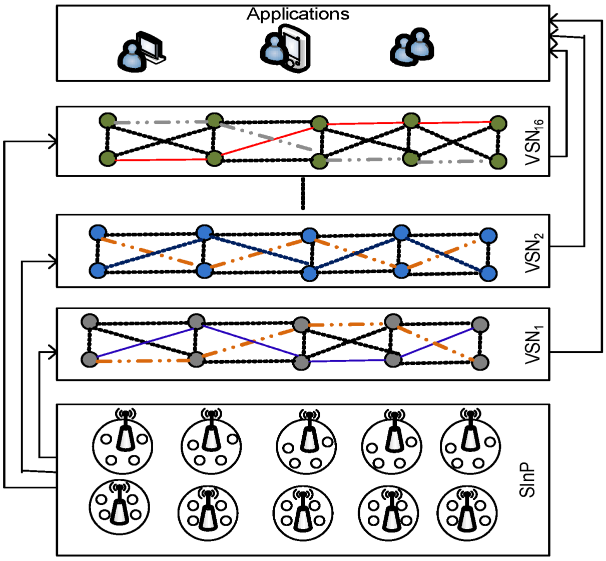
3.1.1 SInP

SInP consists of different smart sensor nodes. These nodes sense different vital signs of patient such as temperature, heart rate, blood pressure, blood sugar, etc in parallel. To sense patient body in the VSN environment we consider two types of sensor node, the fully functional device (FFD) and reduced functional device (RFD) sensor node. SInP deploy sensor nodes in the hospital in a distributed manner. Each group of sensor nodes are divided in different small area which is identified by the circle we name it as SGR domain. Each SGR domain may consist of one or more SGR which is an FFD sensor node. Each SGR support sensor virtualisation. In each domain there are many RFD sensor nodes which perform sensing vital sign. RFD is more resource constrained than SGR/FFD.

3.1.2 VSNSP

VSNSP consists of many virtual SGRs (VSGRs). It is the virtual representation of processing, storage and other resources of the SGRs. And the links between VSGR are the dynamically allocated channels between the SGRs. Since VSN scheme is based on IEEE 802.15.4 radio specification, it has 16 channels. Each channel is considered as individual path that is consist of multiple links between SGR. Each VSN provide specific application service to the users. In Figure 3, we depict up to maximum 16 VSNs provided by a specific VSNSP as the underlying SInPs can support.

Figure 3 VSN architecture (see online version for colours)



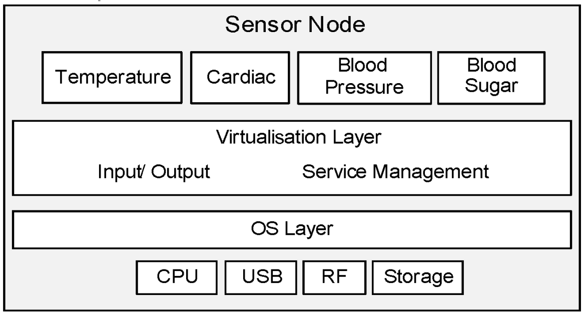
3.1.3 ALU

This layer consists of different application level users such as doctor, nurse, patient or any other specialised users. On the basis of the application requirements, ALU sends request to the VSNSP. VSNSP then maps the particular VSN according to the request of specific application. Individual applications may use multiple VSNSP resources. Users may be a machine in the case of a machine to machine (M2M) communication that can be individual computers and any other smart device.

3.2 Software architecture for sensor node and SGR

Figure 4 depicts the software architecture of smart sensor node. It senses vital signs from patients in a healthcare system. A single sensor node performs multiple sensing tasks by using physical infrastructure virtualisation as a service. Typical sensor node architecture consists of physical layer, operating system (OS) layer, virtualisation layer and multiple sensing service layers.

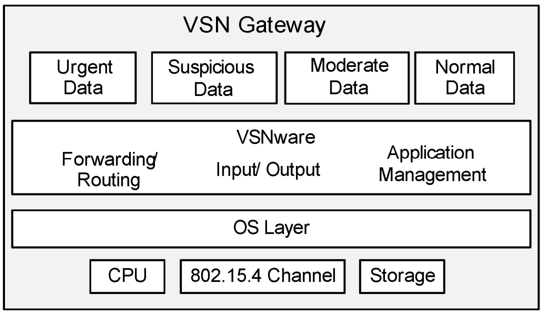
Figure 4 Architecture of sensor node



The lower layer consists of the physical sensor resources such as central processing unit (CPU), USB module, RF module and storage module. Layer 2 consists of a typical multitasking sensor network operating system. We use Embedded Linux in this case. Embedded Linux provides the environment to host virtualisation layer. Virtualisation layer supports concurrent service execution. Virtualisation layer includes input/output and application management module. Finally, application layer runs multiple services over virtualisation layer such as temperature, cardiac data, blood pressure, blood sugar, etc.

Figure 5 depicts detail architecture of SGR. SGR is one of the key components in overall VSN architecture for the healthcare system. SGR is a fully functional sensor node that supports multiple applications processing concurrently. It also consists of physical layer, sensor network operating system layer, VSNware layer and application layer. Lower layer consists of the physical sensor resources such as central processing unit (CPU), RF module and storage module. The sensor operating system layer consists of a typical multitasking sensor network operating system. In this model, we use Embedded Linux as it is used in individual sensor node. It provides the environment to run the VSNware. VSNware supports concurrent applications execution. VSNware consists of different module such as forwarding/routing in VSN, input/output and application management. Finally, the application layer provides the classified data such as urgent, suspicious, moderate and normal over different VSN based on the reliability and delay requirements.

Figure 5 Architecture of SGR



4 Classifications and scheduling of packets in VSN

Figure 6 depicts the packet classification and scheduling module of SGR for VSN environment. It consists of different components such as traffic classifier, scheduling, channel allocation and link estimator. In short the brief descriptions of the whole mechanisms are given below.

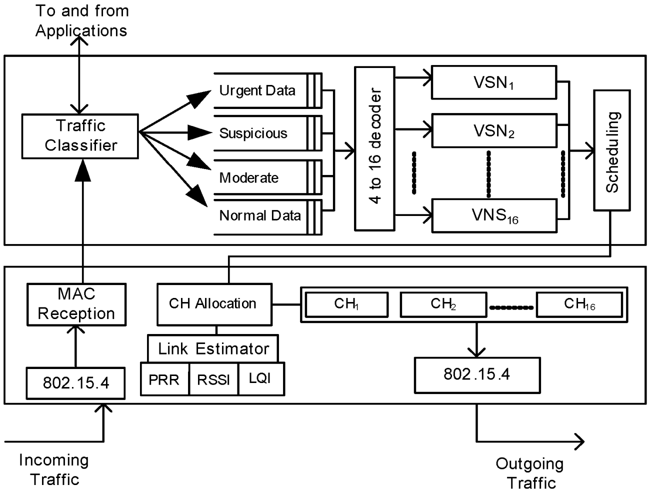
- Receive the data packet by IEEE 802.15.4 interface. Then, it sends data to MAC reception module.
- All the data from MAC reception passes through the traffic classifier module. On the basis of the information provided in the data packet such as reliability, delay deadline and priority information from

application layer, data are classified as urgent, suspicious, moderate and normal.

- The classified data are passed through the 4–16 decoder module. On the basis of the availability of the VSN queues data are queued up.
- Scheduling module sends data to the specific path based on priority and other requirements of the data packet and VSN queue.
- Channel allocation is based on link estimator information and scheduling requirements.
- Link estimator module depends on PRR, RSSI and LQI for link quality measurements.
- Finally data packets are transmitted to the next VSN gateway.

In the following sections, we describe the individual components in details.

Figure 6 Protocol architecture of SGR



4.1 *Traffic classifier*

Traffic classifier receives different types of data packet from MAC reception module. Specific VSN may carry particular types of data packet or combination of different types of data based on application requirement. Data packets consist of different vital signs of the patient such as cardiac data, glucose level, blood pressure, pulse rate and temperature. Packets received from smart sensor nodes include data type, deadline, and delay and reliability requirement. On the basis of these information's in the packet data are classified as urgent, suspicious, moderate and normal. Traffic classification is context-dependent.

Urgent data: It includes emergency traffic or other data that is specified by the applications. These types of traffic assume ~100% reliability and hard delay guarantee. It is usually event triggered traffic and is generated whenever a life threatening situation appears. For instance when the heart rate and blood pressure of a patient exceed the danger limit, an emergency action is needed which thereby requires urgent transmission with the highest reliability and lowest delay.

Suspicious data: This type of data requires strict reliability requirement (>90%) but can tolerate delay up to certain limit, such as medical image of X-ray and ultrasonography. On the other hand, a few of data need to meet strict delay deadline but can tolerate some packet loss such as telemedicine video transmission.

Moderate data: In this case, both delay and reliability guarantee are required. But it requires soft rather than hard QoS. In this case, reliability requirement is assumed to be more than 80%. Different types of medical applications such as regular pulse rate, SPO_2 etc. generate data continuously that must be delivered with moderate reliability and delay requirements.

Normal data: This type of traffic does not require any strict delay or reliability constraints. It is the regular data for the patients such as temperature, glucose level etc. For normal data, <70% reliability is maintained during transmission.

The classified data are transmitted over different VSN according to their delay, reliability and priority requirements. Data over different VSN are forwarded to different users and applications through the dynamically allocated channels.

4.2 *VSNs*

In technical point of view, all the VSNs are the logical combination of the CPU resources, storage and link of the SInP. It is formed dynamically based on the requirement of the application level request provided by different user. However a typical VSNSP consist of 16 VSNs due the dedicated and available channels in the physical layer. These 16 channels of the particular VSNSP can be allocated based on the priority, reliability and end to end delay requirements of the traffics. Particular application may use more than one VSN for ensuring guaranteed service. In a specific VSN there are multiple communication paths by which the data may be transmitted.

4.3 *Scheduling*

It performs data scheduling based on information provided by different components such as traffic classifier, VSNs priority and channel allocation module. The goal of this module is to ensure application specific reliability and end to end delay. Different applications have different reliability and end to end delay requirements.

4.4 *Link estimator*

Link estimation is based on three parameters such as packet reception rate (PRR), received signal strength indicator (RSSI) and link quality indicator (LQI). On the basis of these parameters link estimator provide quality information of the particular link. Detail mathematical derivations of these parameters are given below.

We estimate the current path state by link quality information. This uses link quality indicator (LQI) and received signal strength indicator (RSSI) (Shuaib and Aghvami, 2009; Hussain and Rahman, 2009). The RSSI is a function of the distance between two nodes and can be computed as follows:

$$RSSI(d) = RSSI(d_0) - 10n \log\left(\frac{d}{d_0}\right) \tag{1}$$

In equation (1), *RSSI*(*d*) is the received signal strength in dB at a distance *d* from the source node. *RSSI*(*d*$_0$) is the received signal strength at a distance d_0 from the source and n is the attenuation exponent.

IEEE 802.15.4 specification ensures that each incoming frame must contain a link quality indicator (LQI) value. LQI indicates the quality of the link at the time of frame reception. According to the standard, the LQI value must be an integer that is uniformly distributed between 0 and 255, with 255 indicating the highest signal quality. LQI is measured as follows:

$$LQI = 255 + 3 \times P_{\mathrm{r}x_{dBm}} \tag{2}$$

Here, $P_{\mathrm{r}x_{dBm}}$ is the power of a received frame expressed in decibel-milliwatts. If the computed value is in fraction, then rounding operation is performed to get integer. We define R_{ab} to represent the link quality and receive signal strength between two nodes. *RSSI* of node *a* to node *b* is represented by $RSSI_{ab}$ and *RSSI* of node *b* to node *a* is represented by $RSSI_{ba}$. In this case, we consider symmetric transmission. The *LQI* value of node *a* and *b* are represented as LQI_a and LQI_b. Thus the R_{ab} can be calculated as follows:

$$R_{ab} = RSSI_{ab} \times RSSI_{ba} \times LQI_a \times LQI_b \tag{3}$$

For calculating the packet reception rate (PRR), each node estimates the link loss rate for every outgoing link using the weighted average loss interval method discussed in Alam et al. (2009). It uses interval between loss events to estimate the loss rate of a link. We denote the interval between *m*th and (*m* + 1)th loss for the outgoing link of the *i*th path as $l_{i,1}(m)$. Then, for recent $1 \le m \le n$ losses, the average loss interval, $l_{i,1}$, is

$$l_{i,1}(i,n) = \frac{\sum_{m=1}^{n} l_{i,1}(m) w_m}{\sum_{m=1}^{n} w_m} \tag{4a}$$

$$l_{i,1}(0,n-1) = \frac{\sum_{m=0}^{n-1} l_{i,1}(m) w_m}{\sum_{m=1}^{n} w_m} \tag{4b}$$

$$l_{i,1} = \max(l_{i,1(i,n)}, l_{i(0,n-1)}) \tag{4c}$$

$l_{i,1}(0)$ is the interval since the most recent loss and w_m is the weight given to each loss interval. We compute the average PRR of the first hop of the *i*th path, $P_{i,1}$, using average loss rate, $p_{i,1}^c = 1/l_{i,1}$, as

$$p_{i,1} = 1 - p_{i,1}^c \tag{4d}$$

Communication nature of VSN enables to measure the success rate of a path by passive information exchange. When a node forwards a packet in a path, it includes the success rate of the path in the packet. The success rate of the *i*th path of a node, $P_i(h_i)$, is given by

$$P_i(h_i) = \prod_{J=1}^{h_i} p_{i,j} = p_{i,1} \prod_{J=2}^{h_i} p_{i,j} \tag{5}$$

$p_{i,j}$ is the success rate of the *j*th hop and $p_{i,1}$ is the success rate of the first hop of the node. Whereas, $\prod_{J=2}^{h_i} p_{i,j}$ is the success rate of the path from the downstream node and the node overhears this from the forwarded packets of the downstream node.

4.5 Channel allocation

Channel allocation is a dynamic process by which the system allocates a particular channel to the specific VSN. There are 16 channels in the 802.15.4 PHY layer specification starting at 2.4 GHz. On the basis of the link status from the link estimator, this module allocate channel. Channel quality is computed by the following:

$$R_{\text{Channel}} = \frac{\sum_{i=1}^{n} R_{ab}^{i}}{n} \tag{6}$$

where, R_{ab} is the quality of the link and *n* is the number of links on the channel.

With the help of channel quality computation, channel allocator selects the channel as follows:

Step 1: Periodically measure the channel quality with R_{Channel} and PRR values.

Step 2: Define the scheduling probability *P*(*a*) which is the probability for assigning traffic to a channel I, representing the normalised value of R_{Channel} relative to other channel values as,

$$P_i(a) = \frac{R_{\text{Channel}}}{\sum_k^i R_{\text{Channel}}} \tag{7}$$

We measure probability ranges for channels using the scheduling probability $P_i(a)$. Thus, for each channel *i*, the probability range is defined as follows:

$$\left(\sum_{k}^{i-1} p_i(a),\ \sum_{k}^{i} p_i(a)\right);\ i = 1, 2....N,$$

$$\text{where } p(a) = 0 \text{ and } \sum_{k=0}^{i} p_i(a) = 1 \tag{8}$$

Step 3: We use probability ranges to follow the data to the channel in each interval of time. Priority is assigned to the channel referring to its R_{Channel}. A channel with a high R_{Channel} has higher priority. This is dynamic and changes with time.

The channel allocation module selects a particular channel according to the generated random number between 0 and 1. The value of the random number falls into range defined in equation (8). Thus, the channel with index *i* related to the selected range is chosen to send the data packet. The probability range is used as priority. Lower priority channels have lower chance than higher priority channels to follow data.

5 QoS model in delay domain

Different types of traffic require certain delay guarantee. In this section, we introduce QoS differentiation model for the urgent, suspicious, moderate and normal data in the delay domain. λ_α, λ_β, λ_χ, λ_δ are the arrival rates and μ_α, μ_β, μ_χ, μ_δ service rates of urgent, suspicious, moderate and normal data, respectively. λ is the total arrival rate that indicates the number of the incoming packets per second at the SGR and $\lambda = \lambda_\alpha + \lambda_\beta + \lambda_\chi + \lambda_\delta$. $\mu = \mu_\alpha + \mu_\beta + \mu_\chi + \mu_\delta$ denotes the number of packets depart per second. Packet arrival rate to each SGR is a Poisson process. For a given SGR, end to end path delay is composed of transmission delay and queuing delay. Transmission delay is avoided due to its negligence. We consider *M*/*M*/1 queue model with non-pre-emptive priority. We consider individual priorities, p_α, p_β, p_χ and p_δ for different class of traffics. The traffic intensity at the SGR is computed as,

$$p = \frac{\lambda}{\mu} = p_\alpha + p_\beta + p_\chi + p_\delta \tag{9}$$

Probability that an urgent packet finds other packets in service is equal to the ratio of the time spent by SGR on the suspicious, moderate and normal packet. This is calculated as, $\lambda_\beta / \mu = p_\beta$, $\lambda_\chi / \mu = p_\chi$, and $\lambda_\delta / \mu = p_\delta$.

Little's law (Little and Graves, 2008) gives us a good approximation regarding queue behaviour and a basis for predicting performance of the individual queues.

$$E(n) = \lambda E(t) \tag{10}$$

Here, *E*(*n*) is the average number of packet in the queue, λ is the packet arrival rate, and *E*(*t*) is average delay time per packet in the system.

Urgent packet processing: Urgent packets have the highest priority. For its processing, there are dedicated VSNs. It ensures almost negligible delay which includes the short queuing delay.

Suspicious packet processing: For delay guaranteed suspicious packets, processing is done in the same method like urgent packet. The packets which are not delay guaranteed, they face longer queuing delay. Mean delay of such packet depends on *E*(*n*) and the packets in service. This can be formulated as follows:

$$E(t_\beta) = \frac{E(n_\beta)}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(p_\chi + p_\delta) \tag{11}$$

$$E(t_\beta) = \frac{1 + (p_\chi + p_\delta)}{(1 - p_\beta)\mu} \tag{12}$$

$$E(t_\beta) = \frac{1}{\mu} + \frac{(p_\beta / \mu)}{1 - p_\beta} \tag{13}$$

Moderate packet processing: This type of packet has to wait for suspicious packet in service and the moderate packets in the ready queue. The delay can be calculated as follows:

$$E(t_\chi) = \frac{E(n_\beta)}{\mu} + \frac{E(n_\chi)}{\mu} + \frac{1}{\mu} + \frac{1}{\mu} p_\delta \tag{14}$$

Since $p = p_\alpha + p_\beta + p_\chi + p_\delta$, equation (14) can be represented as following.

$$E(t_\chi) = \frac{E(n_\beta)}{\mu} + \frac{E(n_\chi)}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(p - p_\alpha - p_\beta - p_\chi) \tag{15}$$

Normal packet processing: Normal packet has to wait for the suspicious and moderate packet in the service and also for the normal packet in the queue. The delay can be calculated as follows:

$$E(t_\delta) = \frac{E(n_\beta)}{\mu} + \frac{E(n_\chi)}{\mu} + \frac{E(n_\delta)}{\mu} + \frac{1}{\mu} + \frac{1}{\mu} p_\delta \tag{16}$$

$$\begin{aligned} E(t_\delta) = {} & \frac{E(n_\beta)}{\mu} + \frac{E(n_\chi)}{\mu} + \frac{E(n_\delta)}{\mu} \\ & + \frac{1}{\mu} + \frac{1}{\mu}(p - p_\alpha - p_\beta - p_\chi - p_\delta) \end{aligned} \tag{17}$$

$$E(t_\delta) = \frac{E(n_\beta)}{\mu} + \frac{E(n_\chi)}{\mu} + \frac{E(n_\delta)}{\mu} + \frac{1}{\mu} \tag{18}$$

The average delay of the arrived packet depends on the packets, which are already buffered in the queue, plus the packets in service.

6 QoS model in reliability domain

Reliability is a unit less quantity which can be defined as the ratio of the number of unique packets received by the gateway node to the number of unique packets sent by the source node. In this paper, we consider both link layer reliability and network layer reliability. In wireless network, MAC layer retransmission is used to improve the reliability. But retransmission increases the delay at each hop. Moreover MAC layer retransmission does not efficiently increase the reliability in the densely deployed WSN due to its increased medium contention. Here, we consider VSN-based approach to achieve required reliability. For urgent traffic, the VSN approach provides around 100% reliability by using dedicated paths over multiple VSNs. For suspicious data with reliability requirement more than 90% are transmitted over multiple paths of multiple VSNs. For moderate data with reliability requirement more than 80% are transmitted over multiple paths of specific VSN. And finally normal traffic with reliability <70% are transmitted over available paths. This reliability differentiated traffics are transmitted with the help of scheduling module of network layer and channel allocation module of link layer.

Let us assume the number of unique data traffic sent by the source node is X_s and the number of unique data traffic received by gateway router is X_r. Thus, the reliability is $R = X_r / X_s$. Reliability calculation follows the multiplication law of probability.

$$p(k) = \prod_{i=1}^{k} (1 - p_i^d) \tag{19}$$

Now we will address the probabilistic model of reliability (Felemban et al., 2006; Alam et al., 2009; Razzaque et al., 2008) for different cases such as multiple paths over multiple VSN, multiple paths over single VSN and single path over single VSN.

- *Multipath over multi-VSN*: In multipath over multi-VSN packet forwarding, if there are m paths in n VSNs, then the probability that at least one copy of a packet is successfully received by the SGR is,

$$p(m,n) = 1 - \left[\prod_{i=1}^{16} [1 - p_i(k_i)]\right]\left[\prod_{j=1}^{m} [1 - p_j(k_j)]\right] \tag{20}$$

$$p(m,n) = 1 - \left[\prod_{i=1}^{16}\left[1 - \prod_{i=1}^{k}\left(1 - p_i^d\right)\right]\right] \times \left[\prod_{j=1}^{m}\left[1 - \prod_{j=1}^{m}\left(1 - p_j^d\right)\right]\right] \tag{21}$$

where $p(m, n)$ is the probability of success for multipath and multi-VSN packet forwarding with m paths and n VSNs. $p_i(k_i)$ and $p_j(k_j)$ are the probability of success for the ith VSN and jth path, respectively. And p_i^d and p_j^d are the probability that a packet is dropped by ith VSN and jth path, respectively.

If X_s packets are sent and X_r packets are received by the gateway node with probability $p(m, n)$, thus the number of total packets received by the SGR has binomial distribution and probability mass function (*pmf*) is given by

$$p[X_r = t] = \binom{X_s}{t}[p(m,n)]^t [1 - p(m,n)]^{X_s - t} \tag{22}$$

The required reliability R_{req}, is achieved when the number of unique packet is received by the SGR is X_r. This implies $X_r = R_{\text{req}} X_s$. To fulfil the requirement X_r should be $\geq R_{\text{req}}$. So the probability that the required reliability is met in multi-path over multi-VSN packet forwarding, p_{mPath}^{mVSN}, is

$$p_{mPath}^{mVSN} = \sum_{t=X_r}^{X_s} \binom{X_s}{t}[p(m,n)]^t [1 - p(m,n)]^{X_s - t} \tag{23}$$

- *Multipath over single-VSN*: In multipath over single-VSN packet forwarding, if there are m paths over a VSN, then the probability that at least one copy of a packet is successfully received by the SGR is.

$$p(m) = 1 - \left[\prod_{j=1}^{m} [1 - p_j(k_j)]\right] \tag{24}$$

$$p(m) = 1 - \left[\prod_{j=1}^{m} [1 - p_j(k_j)]\right] \tag{25}$$

where $p(m)$ is the probability of success for multi-path over a specific VSN packet forwarding with m paths. $p_i(k_i)$ and $p_j(k_j)$ are the probability of success for the ith VSN and jth path, respectively. And p_i^d and p_j^d are the probability that a packet is dropped by ith VSN and jth path, $p_i(k_i)$ respectively. Since X_s packets are sent and X_r packets are received by the gateway node with probability $p(m)$, thus the number of total packets received by the SGR has binomial distribution and *pmf* is given by,

$$\mathrm{p}[X_r = t] = \binom{X_s}{t}[p(m)]^t [1 - p(m)]^{X_s - t} \tag{26}$$

The required reliability R_{req}, is achieved when the number of unique packet is received by the SGR is X_r. This implies $X_r = R_{req} X_s$. To fulfil the requirement X_r should be $\geq R_{\text{req}}$. So the probability that the required reliability is met in multi-path over single-VSN packet forwarding, p_{mPath}^{sVSN}, is

$$p_{mPath}^{sVSN} = \sum_{t=X_r}^{X_s} \binom{X_s}{t}[p(m)]^t [1 - p(m)]^{X_s - t} \tag{27}$$

- *Single path over single-VSN*: In a single path over single-VSN packet forwarding, to get the required reliability level, it needs to retransmit packets since the failure probability is high. The probability denoted as $p_j(r)$ indicates that j hop successfully forwards a packet within r retransmission attempts. In such scenario, if there is a path in a VSN, the probability that at least one copy of a packet is successfully received by the SGR is

$$p_j(r) = 1 - (p_j)^r \tag{28}$$

The probability that a data packet is successfully received by the SGR in a single path over specific VSN with hop count s, is

$$p(s) = \prod_{j=1}^{S} [p_j(r)] = \prod_{j=1}^{S} \left[1 - (p_j)^r\right] \tag{29}$$

Here, $p(s)$ is the probability of success for single path over single-VSN packet forwarding. The required reliability R_{req}, is achieved when the number of unique packet is received by the SGR is X_r. This implies $X_r = R_{\text{req}} X_s$. To fulfil the requirement X_r should be greater than or equal to R_{req}. So the probability that the required reliability is met in single-path over single-VSN packet forwarding, p_{sPath}^{sVSN}, is

$$p_{sPath}^{sVSN} = \sum_{t=X_r}^{X_s} \binom{X_s}{t}[p(s)]^t [1 - p(s)]^{X_s - t} \tag{30}$$

7 Network model of VSN

We consider densely deployed large scale and heterogeneous wireless sensor network in which N sensor nodes and M sensor gateway router are uniformly distributed. The nodes and SGRs may find out their geographical locations. In fact, networking in such WSN is very dynamic and differs from traditional wired network. Node in WSN is very tiny which consists of small processing and storage unit. Since VSN is based on existing SInP, it inherits most of the properties of WSN. Link in VSN is different channels used in WSN. We use IEEE 802.15.4 that has 16 channels. We describe the network model of WSN by using graph theory that follows procedure discussed in Chowdhury et al. (2009, 2012). We also discuss the VSN node and VSN link embedding. Virtual node embedding in VSN is like the conventional network embedding. But link embedding is quite different from the conventional approach. In this case, link embedding is done by dynamically using different channels that consist of multiple links.

7.1 SInP

We model the S network as a weighted undirected graph and denote it by $G^{SInP} = \left(N^{SInP}, L^{SInP}\right)$, where N^{SInP} is the set of physical sensor nodes and L^{SInP} is associated links. SInP sensor nodes are divided into two functionalities based on their processing capability and storage space i.e., common widely deployed sensor nodes and sensor gateway router. Each sensor gateway router in the SInP is associated with the CPU capacity weight value $C(N^{SInP})$ and its GPS location loc(N^{SInP}) on a globally understood coordinate system. Each substrate link $l^{SInP}\left(i, j\right) \in L^{SInP}$ between two substrate gateway router nodes i and j is associated with the bandwidth capacity weight value $b(l^{SInP})$ denoting the total amount of bandwidth. We denote the set of all substrate paths by P^s and the set of substrate paths from the source node s to the destination node d by $P^s(s,d)$. Figure 1 shows the substrate SInP network, where the sensing node is indicated by small circles of different colour and sensor gateway routers are indicated by node with wireless antenna.

7.2 VSN request by ALU

As we discuss the graph-based description of SInP, we also model VSN request as weighted undirected graphs and denote a VN requests in terms of service request as the $G^{vsn}\left(N^{vsn}, L^{vsn}\right)$. We mention the requirement on virtual nodes and links of the substrate physical sensor network. Each VN request has an associated nonnegative value D^v expressing how far a virtual node $n^{vsn} \in N^{vsn}$ can be embedded from its preferred location loc(n^{vsn}). D^v is expressed naturally as link delay or round-trip time from the loc(n^{vsn}).

7.3 SInP network resources measurement

To measure the different types of resource usage of the SInP, we use the notion of utility. The substrate SInP node utility $U_n^{SInP}\left(n^{SInP}\right)$ is defined as the total amount processing power allocated to different virtual sensor nodes hosted on the substrate SInP node $n^{SInP} \in N^{SInP}$.

$$U_{n^{SInP}}(n^{SInP}) = \sum c(n^{vsn}) \tag{31}$$

The substrate SInP link utility $U_l^{SInP}\left(l^{SInP}\right)$ is defined as the total amount link usage by different virtual sensor nodes hosted on the substrate SInP node $n^{SInP} \in N^{SInP}$. It is actually the dedicated channel utilisation to specific virtual sensor node.

$$U_{l^{SInP}} = \sum b(l^{vsn}) \tag{32}$$

The substrate SInP storage or memory utility $U_m^{SInP}\left(m^{SInP}\right)$ is defined as the total amount storage usage by different virtual sensor nodes hosted on the substrate SInP node $n^{SInP} \in N^{SInP}$. It is actually the memory utilisation of different virtual sensor node.

$$U_{m^{SInP}} = \sum s(m^{vsn}) \tag{33}$$

Total utility of processing power, link and storage can calculated by summing up equations (31)–(33). Here α, β and γ are the weighted value to express the node, link and storage capacity by single utility.

$$U_{T^{SInP}} = \alpha\sum c(n^{vsn}) + \beta\sum b(l^{vsn}) + \gamma\sum s(m^{vsn}) \tag{34}$$

7.4 Residual resources measurement

Residual resources management is performed by measuring the available remaining after utilisation. In this section we have given the mathematical formulation of the remaining resources of SInP sensor node, corresponding link and storage only. The residual capacity of the SInP sensor nodes are defined as the total processing capacity of the sensor nodes which is explained by equation (35).

$$R_{n^{SInP}}(n^{SInP}) = \sum_{n \in N} c(n^{SInP}) - U_{n^{SInP}}(n^{SInP}) \tag{35}$$

In wireless sensor network, communication is performed by wireless links. By link, here we mean wireless between different SGR nodes. We allocate different channel of a particular wireless link to a particular applications in virtualisation of sensor network. Equation (36) represents the residual channels capacity in the underlying SInP.

$$R_{l^{SInP}}(l^{SInP}) = \sum_{l \in L} b(l^{SInP}) - U_{l^{SInP}}(l^{SInP}) \tag{36}$$

There are two types of storage in the underlying SInP node such as flash memory and SDRAM. In this mathematical model, we only consider the SDRAM which is only physical memory shared by different applications in the

VSN applications. Equation (37) shows the total remaining residual storage for further applications.

$$R_{s_{SInP}}\left({}_{s_{SInP}}\right)=\sum_{m\in M} s(m^{vsn})-U_{m_{SInP}}(m^{SInP}) \qquad (37)$$

7.5 *VSN node and link embedding*

In this work, VSN node and link embedding is very much restricted to SGR and wireless link between different SGR. Different VSNSP node share same or different SGR of the SInP. The typical sharing depends on the storage limit of the SGR. For wireless link embedding, we consider the efficient channel utilisation. Individual VSNSP provides particular services. For example, VSN-1 may provide urgent data services and use channel-1; VSN-2 may provide suspicious data services and use channel-2 of the specific VSNSP. In this way same SInP can be used by different VSNSP. We are interested to explore VSN embedding mechanism as one of our future research works.

8 Evaluations

In this section, we discuss the simulation environment and evaluation results. We have implemented and evaluated the VSNware on the Imote2 sensor node. The Imote2 sensor node has Marvel PXA27x ARM processor with 400 MHz clock speed, 32 MB Flash and 32 MB SDRAM. We have selected Imote2 as the sensor node for its advanced features such as memory size and CPU speed. In this evaluation, sensor node runs Embedded Linux as its operating system. The detail system specifications are given in Table 2. VSNware environment restricts access to all physical devices on the node, thus ensuring that applications are only allowed to access the hardware through the VSNware. VSNware is available in all SGR nodes. VSNware support concurrent application execution and dynamic application deployment. The VSNware supports applications implemented in high level language, thereby enabling different applications of healthcare scenario to be executed and run in the VSN environment. For evaluations, we compare the proposed VSN approach with MMSPEED (Felemban et al., 2006) and traditional WSN approach. Traditional WSN approach in this evaluation process is used to emulate the exact scenario which is provided by the proposed VSN approach.

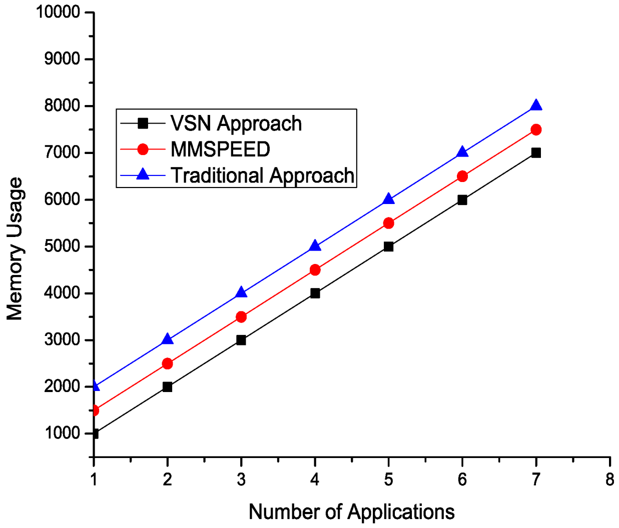
In the following simulation results, utilisation of VSNware is the technical point of VSN-based system evaluation. Here, we focus on different issues such as memory utilisation, CPU utilisation and execution times of individual applications. Utilisation of memory and CPU in an efficient way is the main concern of VSN approach. Execution time and CPU utilisation is related to each other. We have compared the memory and CPU utilisation of our proposed VSN scheme to the MMSPEED and traditional approaches.

In Figure 7, we plot memory usage of the traditional approach, MMSPEED and VSN approach. The sensor virtualisation version includes the overhead of the applications due to additional usage of memory of a single sensor node. However, the overhead is linear and increases slowly based on the deployment of the number of applications. In comparison to MMSPEED and traditional approaches, the proposed VSN approach provides better performances. The performance evaluation shows that the proposed VSN approach reduces 53% and 56% average memory utilisation than the MMSPEED and traditional approach, respectively.

Table 2 System specifications

Type	*Specifications*
Sensor node	Imote2
CPU	Marvel PXA27x ARM
CPU speed	400 MHz
Operating System	Embedded Linux
OS version	2.6.29
VM	VSNware
Flash size	32 MB
SDRAM size	32 MB
Interface	USB
Bandwidth	250Kbps
Radio	IEEE 802.15.4

Figure 7 Comparative memory usage in VSN approach (see online version for colours)



In Figure 8, we plot execution time of different applications in different number of virtualised sensor nodes. The figure shows execution time of 3, 5 and 7 vital signs sensing applications based on virtualisation of sensor network methodology. Execution time increases linearly based on the number of application in a sensor node.

In Figure 9, we plot the CPU utilisation vs. the number of applications in the traditional approach, MMSPEED approach and in the virtualisation of sensor network scenario. CPU utilisation increases linearly in all the cases. In this scenario, the VSN approach uses CPU resources efficiently since it executes different application on the same sensor node. The performance evaluation result shows that the proposed VSN approach reduces 56% and 60% average CPU utilisation than the MMSPEED and traditional approach, respectively.

Figure 8 Execution time vs. number of nodes (see online version for colours)

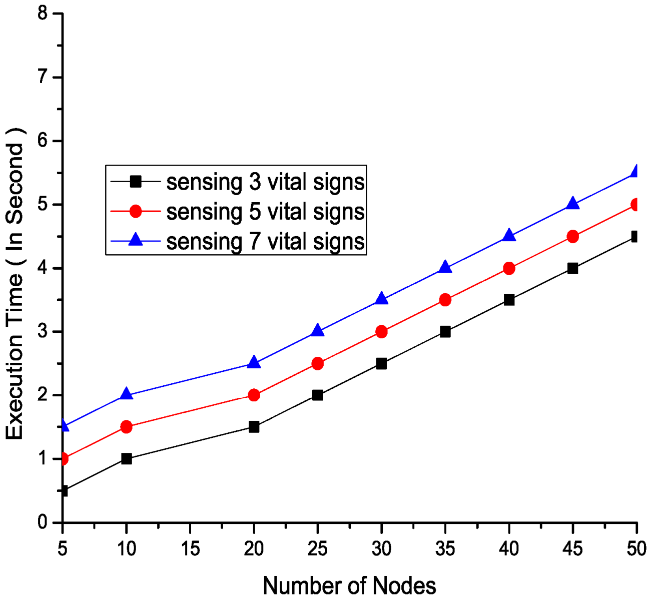
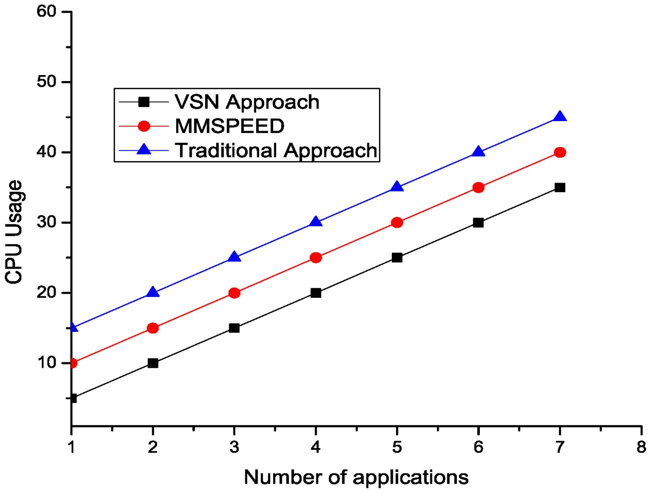


Figure 9 Comparative CPU usage in VSN approach (see online version for colours)



In Figure 10, we depict the memory usage of different typical applications such as medical image, cardiac, blood sugar, blood pressure and temperature. Medical image applications use more memory than other applications. Since the total memory in Imote2 sensor node is 32 MB, it can provide the environment for the execution and running of the typical applications. The figure also demonstrates the memory usage of different applications in MMSPEED scheme, traditional WSN and proposed VSN approach.

In Figure 11, we have presented the end to end delay of different data flows. It shows the average delay for the four classes of data packet that increases with the increasing of sensor nodes. It clearly shows that the average end to end delay of urgent packet is significantly lower than the suspicious, moderate and normal data packets.

Figure 10 Comparative memory usage by applications (see online version for colours)

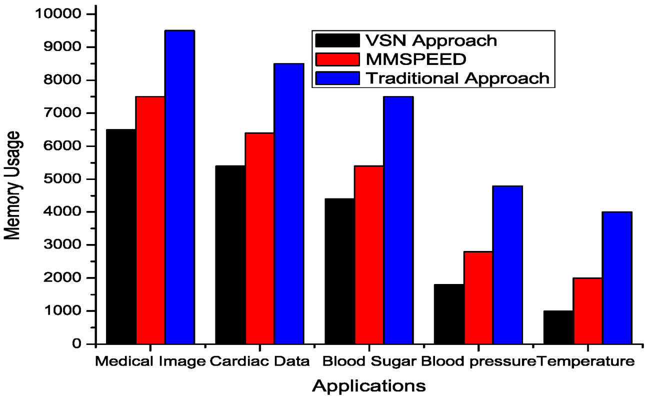
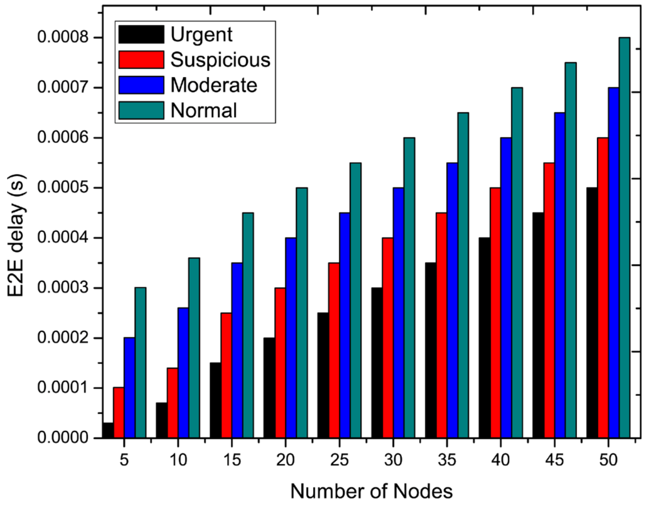


Figure 11 End to end delay vs. number of nodes (see online version for colours)



In Figure 12, we have presented the end to end delay of different data flows with respect to the data rate. The data rate varies according to the priorities assign to different data flows. Since the highest priority is assigned to urgent class, it experiences lowest delay with respect to other classes of data packet. Suspicious and moderate data are also facing minimum delay due to priority and VSN approach used in this scheme.

Figure 13 shows reliability of different data packets with respect to the number of nodes. Since we focused on designing our scheme to ensure 100% reliability, but practically on an average it is ensuring around 98% reliability. But in case of necessity dedicated channels can be allocated to ensure 100% reliability. Reliability level of the suspicious and moderate data is also significantly higher than the normal data. In Figure 14, we demonstrate the packet dropping probability vs. arrival rate. Packet dropping depends on the packet arrival rate at the queues. Figure 14 shows that the urgent data have lowest loss, followed by the suspicious, moderate and normal traffic.

Packet dropping probability increases with the increase of arrival rates. This happens due to the limited queue size and buffering technology.

Figure 12 Delay vs. data rate (see online version for colours)

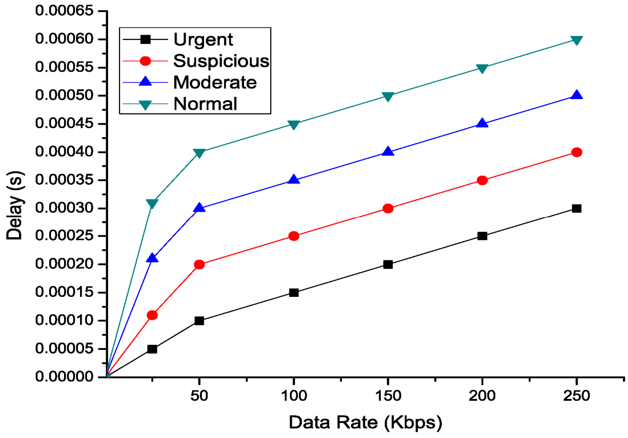


Figure 13 Reliability vs. number of nodes (see online version for colours)

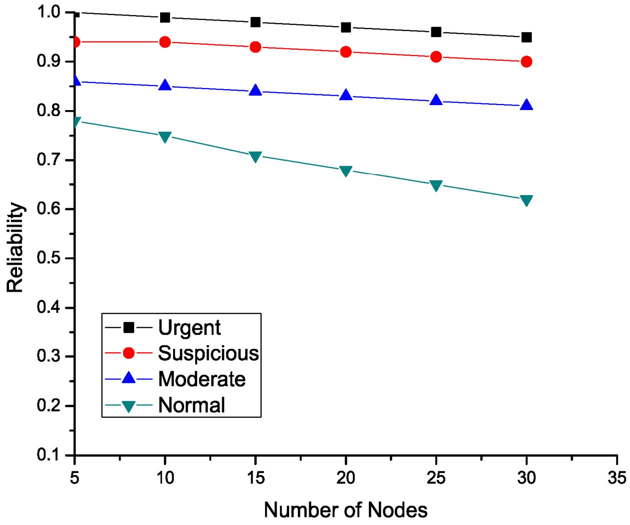
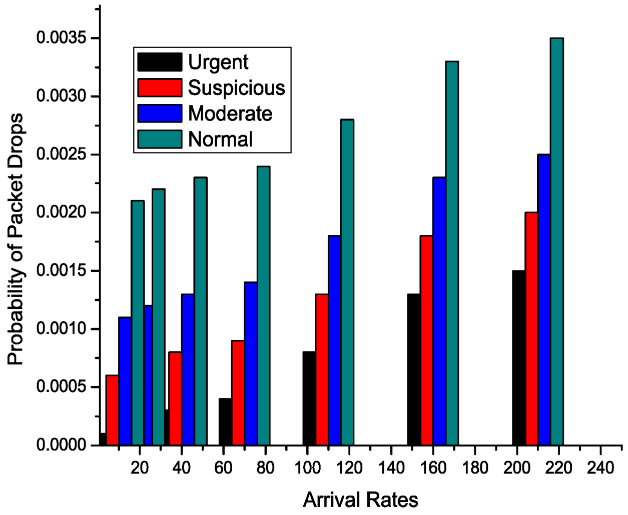


Figure 14 Packet dropping probability vs. arrival rate (see online version for colours)



9 Conclusions

In this paper, we propose a novel approach of VSN-based packet delivery mechanism in healthcare system to provide service differentiation and probabilistic QoS assurance in the delay and reliability domains. It explores QoS-based data classification and scheduling scheme for public healthcare applications in VSN environment. For the delay domain, we use multiple layers based on VSN so that different data packets can dynamically choose the appropriate layer according to the delay requirement of individual data traffic. For the reliability domain, we use multiple virtualisation layers as well as different paths within the corresponding VSN. The performance evaluations show that the VSN scheme provides low end to end delay and high reliability for the urgent data. It also significantly increases the performance for the other data classifications. Our future interest is to emphasise on the large scale and federated sensor network platform with multiple applications sharing the same physical resources that will facilitate the rapid deployment of the sensor cloud based ubiquitous healthcare system.

Acknowledgements

The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for its funding of this research through the Research Group Project No. RGP-281.

References

Akkaya, K. and Younis, M. (2005) ‘A survey on routing protocols for wireless sensor networks’ *Ad Hoc Networks*, Vol. 3, No. 3, pp.325–349.

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) ‘A survey on sensor networks’, *IEEE Communications Magazine*, Vol. 40, pp.102–114.

Alam, M.M., Razzaque, M.A., Rashid, M. and Hong, C.S. (2009) ‘Energy-aware QoS provisioning for wireless sensor network: analysis and protocol’, *Journal of Communications and Networks*, Vol. 11, No. 4, pp.390–405.

Bandara, H.M.N., Jayasumana, A.P. and Illangasekare, T.H. (2008) ‘Cluster tree based self organization of virtual sensor networks’, *IEEE GLOBECOM Workshops*, New Orleans, LA, USA, pp.1–6.

Chowdhury, N.M.M.K., Rahman, M.R. and Boutaba, R. (2009) ‘Virtual network embedding with coordinated node and link mapping’, *IEEE INFOCOM*, pp.783–791.

Chowdhury, N.M.M.K., Rahman, M.R. and Boutaba, R. (2012) ‘ViNEYard: virtual network embedding algorithms with coordinated node and link mapping’, *IEEE Trans. on Networking*, Vol. 20, No. 1, pp.206–219.

Efstratiou, C., Leontiadis I., Mascolo, C. and Crowcroft, J. (2010) ‘Demo abstract: a shared sensor network infrastructure’, *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems (Sensys’10)*, Zurich, Switzerland.

Felemban, E., Lee, C-G. and Ekici, E. (2006) 'MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks', *IEEE Trans. Mobile Comput.*, Vol. 5, No. 6, pp.738–754.

Hussain, S. and Rahman, M.S. (2009) 'Using received signal strength indicator to detect node re-placement and replication attacks in wireless sensor networks', *SPIE Proceedings on Data Mining, Intrusion Detection*, Information Assurance, and Data Networks Security.

Hussain, S., Azim, A. and Park, J.H. (2009) 'Energy efficient virtual MIMO communication for wireless sensor networks', *Telecommunication Systems*, Vol. 42, pp.139–149.

Islam, M.M. and Huh, E.N. (2011b) 'Sensor proxy mobile IPv6 (SPMIPv6) – A novel scheme for mobility supported IP-WSNs', *Sensors*, Vol. 11, No. 2, pp.1865–1887.

Islam, M.M. and Huh, E-N. (2011a) 'A novel addressing scheme for PMIPv6 based global IP-WSNs', *Sensors*, Vol. 11, No. 9, pp.8430–8455.

Islam, M.M., Hassan, M.M. and Huh, E-N. (2010) 'Virtualization in wireless sensor network: challenges and opportunities', *Proceedings of the 13th International Conference on Computer and Information Technology (ICCIT)*, 23–25 December, Dhaka, Bangladesh.

Islam, M.M., Hassan, M.M., Lee, G-W. and Huh, E-N. (2012) 'A survey on virtualization of wireless sensor networks', *Sensors*, Vol. 12, No. 2, pp.2175–2207.

Kabadayi, S., Pridgen, A. and Julien, C. (2006) 'Virtual sensors: abstracting data from physical sensors', *Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Buffalo-Niagara Falls, NY, USA, pp.26–29.

Leontiadis, I., Efstratiou, C., Mascolo, C. and Crowcroft, J. (2012) 'Senshare: transforming sensor networks into multi-application sensing infrastructures', *9th European Conference on Wireless Sensor Networks*, 15–17 February, University of Trento, Italy.

Levis, P. and Culler, D. (2002) 'Mate: a tiny virtual machine for sensor networks', *ASPLOS-X: Proceedings of the 10th International Conference on Architectural Support for Programming Languages and Operating Systems*, New York, USA, pp.85–95.

Little, J.D.C. and Graves, S.C. (2008) 'Little's law', in building intuition: insights from basic operations management models and principles, *Springer Science and Business Media*, pp.81–100.

Razzaque, M.A., Alam, M.M., Rashid, M. and Hong, C.S. (2008) 'Multi-constrained QoS geographic routing for heterogeneous traffic in sensor network', *IEICE Trans. Commun.*, Vol. E91-B, No. 8, pp.2589–2601.

Shin, J.H. and Park, D. (2007) 'A virtual infrastructure for large-scale wireless sensor networks', *J. Comput. Communication*, Vol. 30, pp.2853–2866.

Shuaib, A.H. and Aghvami, A.H. (2009) 'A routing scheme for the IEEE-802.15.4-Enabled wireless sensor networks', *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 9, pp.5135–5151.

Waharte, S., Xiao, J. and Boutaba, R. (2004) 'Overlay wireless sensor networks for application-adaptive scheduling in WLAN', *Proceedings of the 7th IEEE International Conference on High Speed Networks and Multimedia Communications (HSNMC)*, LNCS 3079, pp.676–684.

Yu, Y., Rittle, L.J., Bhandari, V. and LeBrun, J.N. (2006) 'Supporting concurrent applications in wireless sensor networks', *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, November, 01–03 November, Boulder, CO, USA.