Research Paper Engineering

WSN Compatible IOT middleware for healthcare monitoring system

T. Jayasri Tata Consultancy Services, Chennai, TN, India

Hemalatha.M. Dept. of ECE, Narayana Engineering College, Nellore, AP, India

Kurunji Malar.R Dept. of ECE, Sri Manakula Vinayagar Engineering College, Puducherry, India

Aruna Singaravelu Learning and Development, BBG, Doha, Qatar

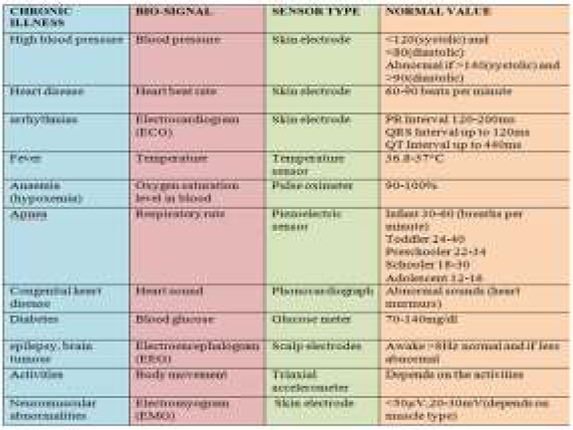
ABSTRACT

The influence of chronic illness results in 53% cessation of human life and also will cause 60 million people to lose their life by next 10 years in India according to report of World Health Organization (WHO). In addition to this, premature death due to chronic illness like heart stroke and diabetes has adverse effect on the economy resulting in drastic reduction of national income, so this problem needs to be encountered by improving quality of healthcare. Clearly, this work contributes to the improvement of healthcare by proposing an architecture making use of the internet of things for long term assessment of illness, supporting mobility and Hydra middleware to integrate heterogeneous clinical devices supporting interoperability. Most importantly, body area network (BAN) made of non-hydra or hydra clinical devices to measure medical parameters, and personal area network (PAN) made of hydra devices which act as gateways between non-hydra BAN devices and hydra network offer a smart environment for remote health monitoring of elderly patient having chronic illness. This paper discusses the feasible architecture for recapturing medical history, cost effective transmitting modes, medical data traffic, and security.

KEYWORDS : Health monitoring system, Internet of things, and Hydra middleware, WSN.

INTRODUCTION

Internet of things (iot) is the future internet that links virtual and physical world allowing things to things and things to human communication where the things being smart make the environment smarter. It creates a smart planet where all the objects which are IP enabled communicate with one another and also with human and achieves data transfer through wireless technologies (e.g.: Zigbee, WiMax, Wi-Fi, 6LoWPan) along with internet and these objects can be served, monitored, and controlled through internet having a unique IP address. Embedding these objects in the environment makes the environment smarter supporting mobility, interoperability, remote monitoring and control. This digital intelligence can be used in real time environment and widely used in home automation, health care, industries, transportation, intelligence building, environment monitoring, product management, process management, agriculture, security, education, government and public sector, and military applications. This work focuses mainly on remote health monitoring of elderly patients with chronic illness after acute care and ensures safety of the patients at home, on moving and also at different location apart from home. With the use of its technology and body area network it has become feasible to monitor the patients in different postures. Around 60% of mortality [1] is due to chronic illness. The chronic illness and its relevant signal values are shown in Table 1. Internet of things technically scaffolds integrating heterogeneous clinical devices using middleware, remote monitoring, data acquisition, analysis, sharing, communication between nodes through network, and a controlled pervasive environment. It comforts independent survival, enhance quality of healthcare, reduces cost and labour, minimize formal visiting in hospital, aids long-term assessment and diagnosis. This paper provides an architecture interconnecting servers of different regional hospitals through internet to exchange medical data (relevant to patients under their monitoring) in case, the patient while travelling to another region than enrolled one, for brief visit may get admitted in a hospital nearby due to health problem. That foreign hospital can retrieve data relevant to the patient using the unique patient ID by querying appropriate hospital server where the patient has previously enrolled. This work utilizes iot middleware for health monitoring to achieve interoperability between heterogeneous clinical devices and also to build a secure system. The following Table 1., describes the appropriate sensor used for bio signal acquisition to diagnose chronic illness.



CHRONIC ILLNESS	BIO-SIGNAL	SENSOR TYPE	NORMAL VALUE
High blood pressure	Blood pressure	Skin electrode	<120(systolic) and <80(diastolic) Abnormal if >140(systolic) and >90(diastolic)
Heart disease	Heart beat rate	Skin electrode	60-90 beats per minute
arrhythmias	Electrocardiogram (ECG)	Skin electrode	PR interval 120-200ms QRS Interval up to 120ms QT Interval up to 440ms
Fever	Temperature	Temperature sensor	36.8-37°C
Anaemia (hypoxemia)	Oxygen saturation level in blood	Pulse oximeter	90-100%
Apnea	Respiratory rate	Piezoelectric sensor	Infant 30-60 (breaths per minute) Toddler 24-40 Preschooler 22-34 Schooler 18-30 Adolescent 12-16
Congenital heart disease	Heart sound	Phonocardiograph	Abnormal sounds (heart murmurs)
Diabetes	Blood glucose	Glucose meter	70-140mg/dl
epilepsy, brain tumour	Electroencephalogram (EEG)	Scalp electrodes	Awake >8Hz normal and if less abnormal
Activities	Body movement	Triaxial accelerometer	Depends on the activities
Neuromuscular abnormalities	Electromyogram (EMG)	Skin electrode	<50µV-20-30mV(depends on muscle type)

Table1 Sensors for bio signal

LITERATURE SURVEY

A prototype model [2] consist of simple iot technology and RFID tag along with the web interface is deployed for monitoring and identify the patients and report to the physician in case of emergency. An ideal amalgamation [3] of transmission channels and data format to minimize the cost due to data overheads associated with health care and frequency of measuring the parameters related to a particular health hazards were discussed. Monere and movital hardware is used to integrate [4] heterogeneous clinical devices into iot environment where identification of patient and transmission of health parameter after data aggregation to increase lifetime is achieved with RFID and 6LowPan. Cooperative wireless nodes in the iot environment meant for rural health monitoring results [5] in increased energy saving with trade-off among energy utilization, efficiency, and delay. Internet of things made of the internet and things needs to use intelligent interface and integrate heterogeneous devices into the network. The above need is satisfied with the help of middleware which provides abstract from lower layers to upper layer facilitating transparent communication. The current iot middleware is analysed [6] and distinguished based on features of envisioning primary functional block. Middleware is software between the operating system and application layer, offer services to the application layer and sticks to Service oriented architecture (SOA) which brings about a horizontal view [7] by using traditional protocols and general interfaces. Pervasive system prototype [8] design for home automation and healthcare is developed using Hydra middleware and fundamental blocks accompanied by experiences learned during the design and development of hydra were discussed. Healthcare management system by means of hydra middleware is created to achieve a feasible cost-effective system which motivates the use of hydra middleware providing details about pre-configuration [9] of application and devices in hydra network. From a developer's perspective, the Problems and learned experiences [10] while modelling a pervasive healthcare environment with hydra giving excellent security, discovery components, and web services, were discussed. Architecture of the Internet of things built pervasive healthcare system was defined and the traffic parameters [11] while using Zigbee and WCDMA for heart disease and their impact on mobile networks were discussed. Hydra based building automation plan is used for analysing security risks and to overcome this, a meta-model integrated in hydra to provide trust and security. Security risks [12] for a hydra based building automation were analysed and to encounter this problem, a meta-model integrated into hydra was designed which provides security and trust for developers. Ambient Pervasive intelligent environment having high performance is achieved with self diagnosis and management using OWL [13] ontology based Hydra middleware. Semantic descriptions in HYDRA [14] project is defined with model based architecture.

HEALTH MONITORING SYSTEM

Elderly people in a particular locality to be taken care can enroll themselves to regional hospital server nearby home with a unique ID. In hospital, application server maintains data relevant to patient ID like medical advices, type of health hazard, parameters to be measured, frequency of measurement, and medical history in its database. Depending on the health hazard, sensors are provided to measure medical parameters and device application deployed in a proxy device that can be controlled by physicians and used to receive data from sensors and transmit it to hospital server. Health monitoring system uses hydra middleware which gives interoperability and endwise security. There are different scenarios based on their location like at home, while moving out, and while moving into another region. When the patient is at home, resourceful devices like PC, Laptops can be used as gateway which holds complete middleware and it connects to hospital servers through internet. While moving out, this method supports mobility by making use of smart phones as a gateway which holds parts of the middleware and provides proxy to receive the medical data from body area network (BAN) and transmit to the server. Suppose if the patient while making a brief visit to another region get hospitalized there then medical data relevant to the patient are needed, so using the patients unique ID they can retrieve this data from the corresponding enrolled regional hospital's server. Wherever the patient moves the mobility supporting system using smart phone can continuously monitor the patient and sends medical data to corresponding enrolled regional hospital server.

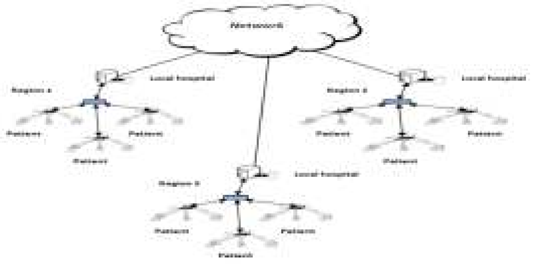


Figure 1 Architecture

Requirements of remote health monitoring system

- Privacy of patient
- Access control to prevent fraud
- Uninterrupted operation
- Less energy conservation
- Mobility support
- Dynamic network support
- Tracking patient by an authorized person
- Interoperability of clinical devices
- Device robustness
- Real-time data acquisition and analysis
- Reduced medical data traffic
- Transparent communication protocol
- Easy to use and develop

ARCHITECTURE AND TRANSMITTING MODES

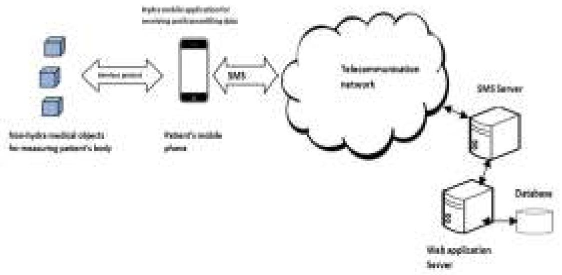

Hydra mobile application for receiving and transmitting data
Interface protocol
SMS
Telecommunication network
SMS Server
Database
Non-hydra medical objects for measuring patient's body
Patient's mobile phone
Web application Server

Figure 2 Transmission of data using SMS

While patient moves out, the medical data are measured and transmitted through SMS to enrolled server. Economic package [3] for SMS results in low cost when compared to other mode of transmission.

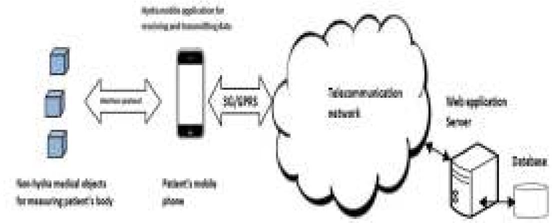

Hydra mobile application for receiving and transmitting data
Interface protocol
3G/GPRS
Telecommunication network
Web application Server
Database
Non-hydra medical objects for measuring patient's body
Patient's mobile phone

Figure 3 Transmission of data using GPRS

For transmitting large amount of data, GPRS technology can be used to transmit medical data to server.

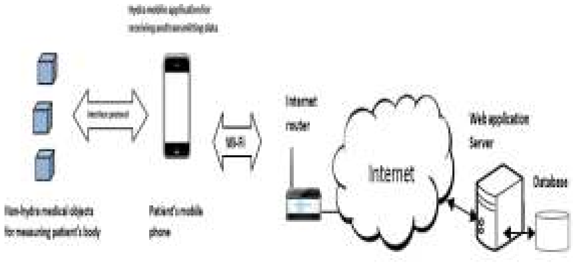

Hydra mobile application for receiving and transmitting data
Interface protocol
Wi-Fi
Internet router
Internet
Web application Server
Database
Non-hydra medical objects for measuring patient's body
Patient's mobile phone

Figure 4 Transmission of data through internet router

When the patient resides at home, medical data from hydra device can be sent to the server using WiFi via internet router.

WHY middleware: In the healthcare environment, there are a number of clinical devices from an increasing number of manufacturers each built with different technologies. It is essential to interconnect these heterogeneous devices to attain the full benefits of the application. So, for this purpose a software platform called middleware is needed to provide an abstract of these heterogeneous devices to application, supporting interoperability. The goal of middleware developer is to create a plug-and-play [6] adaptation layer.

HYDRA middleware: Hydra also called LinkSmart project developed middleware based on service oriented architecture (SOA) supporting embedded networking. Among existing iot middleware Hydra offers portability, context awareness, device administration, security, and interoperability as shown in figure 5. This work proposes an enhanced Hydra (eHydra) middleware for networked health monitoring system.

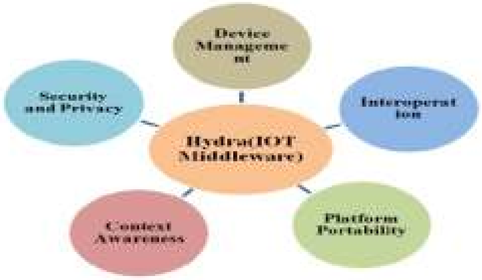


Figure 5 Hydra features

It provides a transparent communication layer, suits decentralized and centralized architecture, supports wired/wireless distributed resource constrained devices, and considers security through design. It achieves interoperability by integrating heterogeneous devices and helps to build an intelligent network. SOA being a software architecture design built with group of different software modules helps to support the above requirements. It hides internal details providing open interface and services for consumers.

TERMINOLOGIES

1. Devices

It is a complex physical device developed for a single purpose which is supposed to be connected to hydra network. These are clinical devices used to measure or aid in measuring medical parameters like blood pressure, glucose level, heartbeat rate, etc... In hydra, there are two types of devices one is non-hydra device and other is hydra device.

Non-hydra device which does not host middleware can be classified into a device that can be web-enabled and device that cannot, while the former can be connected directly or through proxy and the later can be connected only via a proxy which is a hydra device.

Here clinical devices like a glucose meter, temperature sensor, blood pressure monitor etc…. act as non-hydra device that can be web-enabled or not depends on manufacturers.

Hydra device which holds middleware and web-enabled, can be classified again into device that are able to control and act as proxy for connecting non-hydra devices to hydra network and device that cannot act as gateway but connected to hydra network directly. Suppose if the patient is at home resourceful devices like PC, Laptop can be used as gateway which provide proxy to connect non-hydra devices to the network but this cannot be used when the patient goes out with some wearable sensor, so simple devices like smart phones, PDAs that are web-enabled and capable of connecting sensors to hydra network can be used. Resourceful device can hold complete middleware but, devices like smart phones can hold only part of it, where the difference between these two mainly lies in their network managing capability. These hydra devices can be controlled via network using terminals by physician at the hospital.

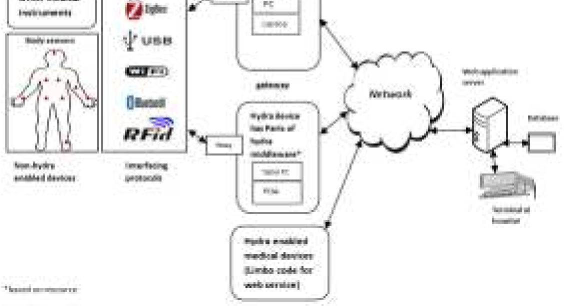

gateway
Application device has full Hydra middleware*
PC
Laptop
Proxy
Other medical instruments
Body sensors
ZigBee
USB
WiFi
Bluetooth
RFid
Non-hydra enabled devices
Interfacing protocols
gateway
Hydra device has Parts of hydra middleware*
Tablet PC
PDAs
Proxy
Network
Web application server
Database
Terminal at hospital
Hydra enabled medical devices (Limbo code for web service)
*based on resource

Figure 6 Hydra as gateway between non-hydra devices and network

2. Gateway

A hydra device with IP ability supporting web services provides Universal Plug and Play protocol (UPnP) for discovery process and capable of compiling discovery manager. It handles proxies to control other devices. PC, Laptop, smart phones, PDAs etc….can be used as gateway to which non-hydra devices are connected.

3. Bridge

It is software present in hydra device (gateway) converting non-IP into IP communication.

4. Proxy

It is a software component resides in hydra device (gateway) knows about the data configuration and technology used to interact with non-hydra device. The proxy must be aware of the technology because different clinical device may use different communication protocols like Bluetooth, Zigbee etc.… Thus it helps in achieving interoperability by providing transparent communication. Proxy runs on UPnP and gives service for automatic discovery of devices.

5. Hydra ID

It is a unique ID for hydra device and service for context-based identification. Network manager produces this ID and matches physical and local ID.

6. Session

It cares the state and provides understandable communication between entities in hydra network.

7. Persistent ID

Application code developers can make use of this ID for referring hydra device.

8. Ontology

It has knowledge about the concepts and logical relations of system in OWL language.

9. Hydra network

Hydra devices located in different local networks can communicate via applications to help of IP and web service over peer to peer architecture.

10. Hydra device

Hydra device holds middleware with web services as interface to the web and UPnP for the discovery process

MANAGERS IN HYDRA MIDDLEWARE

1. Network manager

It is implemented in an ample resource device like a PC, laptop, smart phone etc…. which provides proxy for low resource device like glucose meter. It routes web service calls and set up a mobile IP to support mobility and take care of end nodes that may vanish ads reappear

2. Event manager

Hydra provides publish/subscribe mechanism where an application is informed about the event published by the device when the application ispreviously subscribed to that event. Suppose if an intelligent temperature sensing device publishes an abnormal value, then application subscribed to this event sends alert messages to physicians and care takers. It also supports prioritization among events generated at the same time such as an event which generates an emergency alert gets high priority over normal periodic events.

3. Quality of service manager

A selection algorithm used to choose the best services from group of services sharing similar functionality but with differences in characteristics like throughput, energy utilization etc.…Suppose if accuracy is of main concern then making use of service with high throughput.

4. Context manager

It is closely connected to application than to middleware and supports self-management. It stores semantic data along with raw data supporting context awareness.

TO CONVERT A DEVICE INTO HYDRA DEVICE

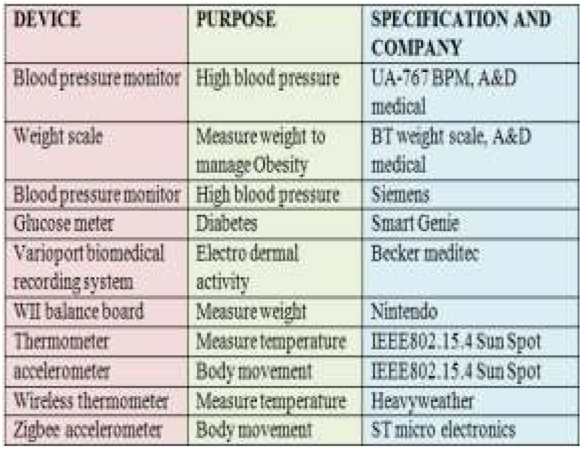
A device in which hydra can be deployed is said to be hydra compliant and they should provide an interface (eg: Zigbee, Bluetooth) externally to interact and control. To enable hydra their functions are to be made accessible and controlled by another hydra device in the network. The procedure involves

- If a device capable of hosting middleware then, Hydra middleware parts installed based on available resource on the device
- With JAVA, Limbo tools used to create web service code for the device provided information about the device and its data
- Consequently generate proxy for the device knowing its interface

PROPERTY OF HYDRA DEVICE

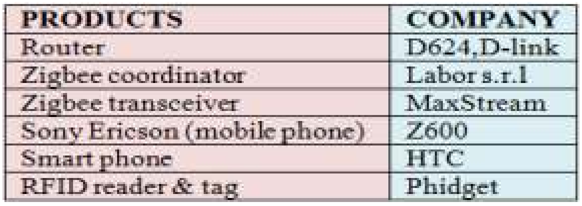
- Discovered
- Offers Web service (directly/proxy) to access its functions
- Provides energy service to get information about energy profile and policy of the device
- Provides generic service to question device property
- Support UPnP for discovery process

Available Hydra devices are shown in Table 2 and 3



DEVICE	PURPOSE	SPECIFICATION AND COMPANY
Blood pressure monitor	High blood pressure	UA-767 BPM, A&D medical
Weight scale	Measure weight to manage Obesity	BT weight scale, A&D medical
Blood pressure monitor	High blood pressure	Siemens
Glucose meter	Diabetes	Smart Genie
Varioport biomedical recording system	Electro dermal activity	Becker meditec
WII balance board	Measure weight	Nintendo
Thermometer	Measure temperature	IEEE802.15.4 Sun Spot
accelerometer	Body movement	IEEE802.15.4 Sun Spot
Wireless thermometer	Measure temperature	Heavyweather
Zigbee accelerometer	Body movement	ST micro electronics

Table 2 Available Hydra enabled medical devices



PRODUCTS	COMPANY
Router	D624,D-link
Zigbee coordinator	Labor s.r.l
Zigbee transceiver	MaxStream
Sony Ericson (mobile phone)	Z600
Smart phone	HTC
RFID reader & tag	Phidget

Table 3 Available Hydra enabled networking and gateway devices

DEVICE DISCOVERY

After creating a hydra device it must be made available at the IP layer. The procedure involves three processes such as device detection, UPnP broadcast, resolve semantically. Initially specify information about the device interface (WDSL by Limbo) and meta-data about the device (in OWL) where meta-data is nothing but device type, manufacturer, model, specification and description. Then with this information, web service code is created using Limbo in order to give semantic device information, web service and UPnP service. Next enroll this service in network manager [8] of proxy device which act as a gateway for the device to be discovered. Discovery process produces UPnP proxy for protocol of the device under discovery so that they are available at the IP layer and the proxy calls the application server to register itself with the application after device discovery. The device is accessible as the hydra device as shown in figure 7.

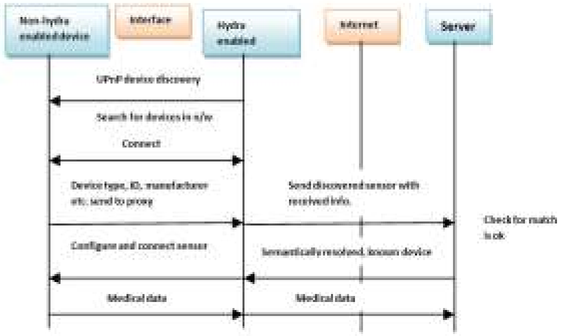

Non-hydra enabled device
Interface
Hydra enabled
Internet
Server
UPnP device discovery
Search for devices in n/w
Connect
Device type, ID, manufacturer etc. send to proxy
Send discovered sensor with received info.
Check for match is ok
Configure and connect sensor
Semantically resolved, known device
Medical data
Medical data

Figure 7 Device discovery process

MOBILITY AND UBIQUITOUS

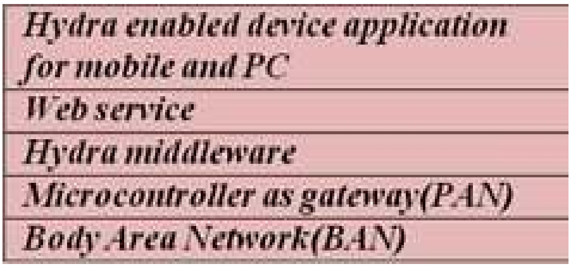
Hydra devices have their own IP address which changes while supporting mobility. In order to address them particularly in hydra network supporting mobility, each device is referred using Hydra ID which helps to identify the device uniquely though the patient moves to different location which leads to change in IP address. Hydra middleware abstracts heterogeneous devices by offering web service irrespective of communication protocol. All devices in Hydra network holds part of middleware and works cooperatively without need of centralized system to build ubiquitous environment.

TRANSPARENT AND COMPATIBILITY WITH WSN

Hydra middleware is highly compatible with existing wireless sensor network because it uses IP accomplished gateway device to provide proxy for resource restricted wireless sensor nodes having heterogeneous communication protocols. Hydra thus provides legal and transparent communication platform by interacting with each nodes in the wireless sensor network.

IMPLEMENTATION CASE STUDY

Body area network periodically monitors and gives out measured medical parameters. These parameters are received transparently through microcontroller based hydra gateway and analysed locally in order to determine whether there exist any emergency condition. Event manager in middleware provides publish subscribe mechanism which publishes the events based on subscribed parameters given by BAN.



Hydra enabled device application for mobile and PC
Web service
Hydra middleware
Microcontroller as gateway(PAN)
Body Area Network(BAN)

Figure 8 Hierarchical Implementation of Hydra middleware using microcontroller

Web service as proxy and client applications built for user interface. J2ME technology can be utilized to create mobile application which in turn gains access to web service deployed at middleware. It is both adaptable and scalable by connecting heterogeneous devices.

SECURITY

In hydra project, security is considered as an important feature from the starting point and presents a meta-model concept to realize security. Confidentiality, truthfulness, authorization, availability, privacy and non-repudiation are the key elements to be considered in security aspects. Remote health care monitoring system must provide secure peer to peer communication [6] , secure routing information, authenticate entering of new peers, secure network access permission , secure exchange of data, and protect the device and user ID. A procedure offered by hydra to protect the message end wise at application layer results in confidentiality and non-repudiation.

The requirement of contextual information about application and device results in high linkage of various contexts which leads to disclosure of personal information. Hydra encounters this problem by reducing gathering of information but still supporting context-awareness.

Hydra developers implement two concepts they are [12] Virtualization and meta-data for security. Hydra provides Virtualization which is a logical representation of device, application, traffic, user and identity. It maps one logical representation of multiple entities (one to many mapping). For example, virtual ID helps to identify the user only in a particular context and the same user can't be identified in other contexts with this virtual ID thus it provides privacy. Middleware resolves the entry of new device semantically using meta-data about the device and its protocol.

Hydra spreads it security till boundary which contains only hydra enabled device, beyond that the proxy allows non-hydra authorized device to exchange information with hydra network and to provide security at this point it can utilize the security attributes supported by device protocol.

Security attributes by device protocol

Rfid, Bluetooth, WiFi, Zigbee, serial, and USB are the communication protocols supported by middleware to integrate heterogeneous devices as shown in figure 9.

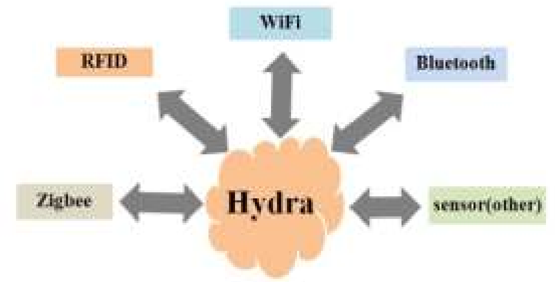


Figure 9 Hydra supporting communication protocols

Each of which have their own optimized security algorithms in their domain to attain maximum protection against security attacks. Keys used for encryption, gaining access, and certification are safeguarded with cipher key management. Hydra also offers a procedure to safeguard the cached information in database from gaining illegal access. WiFi protected access-2 (WPA-2) is a wireless security uses AES and supports data integrity to prevent illegal access in WiFi. Pre-shared symmetric key encryption is performed in Bluetooth supporting confidentiality, integrity, authentication, access control and authorization. Zigbee uses 128-bit symmetric key for encryption and has security architecture based on Counter with CBC-MAC (CCM) which provides confidentiality and verification. Passive RFid tag if used can be utilized elliptic curve cryptography (ECC) [16] which is public key cryptography suitable for resource constrained device providing good security. Finding discrete logarithm for an arbitrary elliptic curve with known point is impossible thus it gives a good security level with the small key size and adequate computation. RFid reader can be attached to the proxy device through USB or using wireless technology. Proxies supporting these security attributes and safe key management with the help of middleware makes the health monitoring system secure.

TRAFFIC

Continuous and periodic monitoring can be done based on patient condition after acute care. The continuous transmission of medical data to the hospital server from a number of patients will drown the physician so intelligent application should be built at patient side such that it will analyse the data to make intelligent decisions like able to differentiate normal and abnormal values and inform in case it encounters an abnormal value to physician with SMS being cost-effective. The measured data can be temporarily stored in end device and can be transmitted as a bulk message to a database which should have the ability to compress the history of patient relevant to medical data. Frequency of measuring medical parameter based on health status can be done as given by Mersini Paschou et al. To take care of diabetes patient blood pressure, breath rate, and oxygen saturation are measured 3 times per week [3] and blood glucose 3 times per day. The medical parameters measured are transmitted to the server immediately in case of detecting any abnormal value by end application or else in bulk mode to a server which helps to reduce the traffic due to medical data.

Physicians analyse these medical records and can send changed prescription if needed or any medical relevant advices can be sent to the patient through hydra network. Intelligent application in the mobile phone can remind the patient about medicine intake or health advices based on prescription.

CONCLUSION

In summary, taking into account the health monitoring system requires intense and reliable monitoring so web based access provided by embedded Hydra middleware in monitoring equipments offer remote and reliable monitoring. In this particular case, internet of things creates smart environments for remote health monitoring of elderly patient having chronic illness. Moreover, it creates a pervasive environment to lead a comfortable easy way of living along with the quality of healthcare. On the other hand, the work at initial stage briefly describes an architecture making use of the Hydra middleware which allows interoperability between heterogeneous devices and comforts both application and device developers by providing transparency. Furthermore, hydra holding devices like smart phones is being developed so it will be easy to develop such a health monitoring system. After developing hydra deployed devices, applications need to be developed using facilities offered by Hydra. Undoubtedly, this work proposes hydra middleware based remote healthcare monitoring system for elderly patient which give rise to advantages like using existing technology, easy integration, trust & security, mobility support, reduced cost and labour, continuous assessment, fast diagnosis and treatment, increased efficiency and service, lifesaving, physicians are informed, and easy analysis of disease with medical history. Among existing iot-middleware, hydra suits well for the healthcare domain because of its interoperability, portability, and security. It is always better to prefer substantial evidence to wishful thinking and in this case, the future work includes the development of intelligent applications to find out abnormalities and use of context awareness for decision making to make this world a better place to live in.

REFERENCES

1. Technologies for remote patient monitoring in older adults. Available online at http://www.techandaging.org/RPMPositionPaper.pdf|| 2. Isabel Laranjo, Joaquim Macedo, and Alexandre Santos, "Internet of Things for Medication Control: Service Implementation and Testing", International conference on health and social care information systems and technologies, 2012, Elsevier.|| 3. Mersini Paschou, Evangelos Sakkopoulos, Efrosini Sourla, and Athanasios Tsakalidis, "Health Internet of Things: Metrics and methods for efficient data transfer", simulation modelling practice and theory, 2013, Elsevier.|| 4. Antonio J. Jara, Miguel A.Zamora, and Antonio F. Skarmeta, "Knowledge acquisition and management architecture for mobile and personal Health environments based on the Internet of Things", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.|| 5. Vandana Milind Rohokale, Neeli Rashmi Prasad, and Ramjee Prasad, "A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring and Control", 2012, IEEE.|| 6. Soma Bandyopadhyay, Munmun Sengupta, Souvik Maiti, and Subhajit Dutta, "Role of middleware for internet of things: a study", International Journal of Computer Science & Engineering Survey, 2011, Vol.2, No.3.|| 7. Luigi Atzori, Antonio Iera, and Giacomo Morabito, "The Internet of Things: A survey", computer networks, 2010, Elsevier. || 8. Amro Al-Akkad, Ferry Pramudianto, Marco Jahn, and Andreas Zimmermann, "Middleware for building pervasive system", Fraunhofer institute for applied information technology, Germany.|| 9. Heinz-Josef Eikerling, Gernot Grafe, Florian Rohr, and Walter Schneider, "Ambient healthcare systems using the hydra embedded middleware for implementing an ambient disease management system".|| 10. Marco Jahn, Ferry Pramudianto, and Ahmad-Amr Al-Akkad, "Hydra middleware for developing pervasive systems: A case study in the e-health domain", Fraunhofer institute for applied information technology, Germany. ||11. Lei You, Chungui Liu, and Sen Tong, "Community Medical Network (CMN): Architecture and Implementation", 2011, IEEE.|| 12. Mario Hoffmann, Atta Badii, Stephan Engberg, Renjith Nair, Daniel Thiemert, Manuel Matthess, and Julian Schutte, "Towards Semantic Resolution of Security in Ambient Environments".|| 13. "Hydra middleware project" information available online at http://www.hydramiddleware.eu/news.php|| 14. Weishan Zhang and Klaus Marius Hansen, "Towards Self-managed Pervasive Middleware using OWL/SWRL ontologies", Fifth Internaional Workshop Modeling and Reasonong in context (MRC 2008), Held at HCP 08.|| 15. Peter Kostelnik, Martin Sarnovsky, Jan Hreno, Matts Ahlsen, Peter Rosengren, Peeter Kool, and Mathias Axling, "Semantic Devices for Ambient Environment Middleware", internet of things workshop, Sophia Antopolis, Sep 2008.||16. Yi-Pin Liao, and Chih-Ming Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol", Ad hoc networks, 2013, Elsevier.