International Journal of Advances in Computer Science & Its Applications
Volume 6 : Issue 2 [ISSN 2250-3765]
Publication Date : 31 August, 2016

Analysing HTTP and COAP for IoT

Feda AlShahwan, Maha Faisal

***Abstract*—IoT is a simple idea of connecting all identified objects through wireless connection that they could communicate with each other [1]. Thus, it is a reality that allows connecting people, and also provides connectivity among those owned. This connectivity saves time, effort and enables things to be smart and work automatically. The goal is not just being connected in terms of computers, tablets and smart phones but it can be visualised as a world where everything is connected together with smart communication among them. In this paper, we discuss internet of things in the field of WPS (Wi-Fi Protected Setup), TCP (Transmission Control Protocol) and IEEE 802. Also, there are some tests that are evaluated between CoAP and HTTP which concludes that CoAP/UDP based protocols perform better for constrained networks compared to HTTP. In addition, there are some securities issues that are related to Internet of things are discussed in the paper.**

***Keywords*—Internet of Things, WSN, CoAP, RPL, REST,WS-**

I. Introduction

The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers. These objects are also given ability to transfer data over a network without requiring human-to-human or human-to-computer interaction [7]. The different elements in IoT include RFID (Radio-Frequency Identification), Internet and sensors (Fig. 1).

The RFID technology is one of the valued technologies of IoT deployments as it can store sensitive data. It can also track objects automatically and handle wireless communication with other objects [34].

The basic architecture for an RFID authentication scheme includes three entities: the RFID tag, the RFID reader, and the server [29]. Movements of an object are detected with RFID chip. There are different procedures for detecting movements of an object tagged with RFID chip [33].

There are also numbers of RFID tags classified based on cost, frequency and security. The RFID tags fall into three different frequency regions (Low frequency (LF, 30 - 500kHz) High frequency (HF, 10 - 15MHz) Ultra high frequency (UHF, 850 - 950MHz, 2.4 - 2.5GHz, 5.8GHz))[32]. Furthermore, the security requirements for RFID are discussed.

Feda AlShahwan
College of Technological Studies, Public Authority for Applied Education, Kuwait

Maha Faisal
College of Computing Science and Engineering/ Kuwait University Kuwait

Security Requirements for RFID communication includes Mutual authentication, Availability and Forward security. Mutual authentication is a process or technology in which both entities in a communications link prove their identities to each other.

To satisfy the various security requirements of RFID technology in IoT, many RFID authentication schemes have been proposed. Some of them are elliptic curve cryptography (ECC)-based RFID authentication schemes [29].The ECC-based RFID authentication scheme that use hash function operations are proposed [35] to get backward privacy. Backward privacy means that the adversary cannot track the tag's previous action when the adversary gets the secret information stored in it .But this scheme faced different demerits .One of the drawbacks of this scheme is the high computational cost.

Thus, a lightweight ECC-based RFID scheme was proposed [36] to achieve mutual authentication. However, Zhao et al. [37] pointed out that this scheme had a problem. The problem is that it failed to hide the secret information stored in the tag (key compromise problem). Adversary the secret information could be easily hacked. Thus, an improved scheme was proposed to overcome such a weakness.

Further [38] proposed an ECC-based RFID authentication scheme using ECC and a one-way hash function.But, unfortunately, Chou's scheme also faced various failures. In [39] it is pointed out that Chou' scheme suffers from the key compromise problem. Moreover, M.Farash [40] have shown that Chou's scheme was vulnerableto the impersonation attack and proposed an improved scheme to overcome those attacks.

The IoT provides significant services and technologies. One of these technologies that have gained its importance is MWS (Mobile Web Services) technology.

The advancement in mobile technologies and internet services has led to an explosion in the use of web services in mobile computing environment. However, the chance of conventional web services to be spread out on mobile devices will bring new challenges in mobile computing in the coming future. Web services technology and mobile computing domains are converging at their intersection which leads to Mobile Web Services (MWS) MWS enables the service access in users' mobile device [15]. As the numbers of web services are increasing dramatically, the web service discovery becomes more important. This importance discovers the use of web services in effective and efficient manner in the field of IoT. As the information is available anytime and anywhere in mobile devices, the demand of MWS is growing rapidly. Thus developing these services connecting to IoT will play an essential role.

There is enormous number of applications that relies on MWS. For example, MWS can be very helpful in tracking the current location of goods and their delivery by embedding this technology with Global Positioning System (GPS) [41].Also, Mobile Web Services provides the services, security, and support to connect the Internet of

Things on a global scale. Mobile Cloud computing can be enhanced towards IoT as cloud. Cloud can connect computers, people and data at massive scale. Cloud computing acts as a front end to access Internet of Things.It can also increase capabilities of mobile devices.

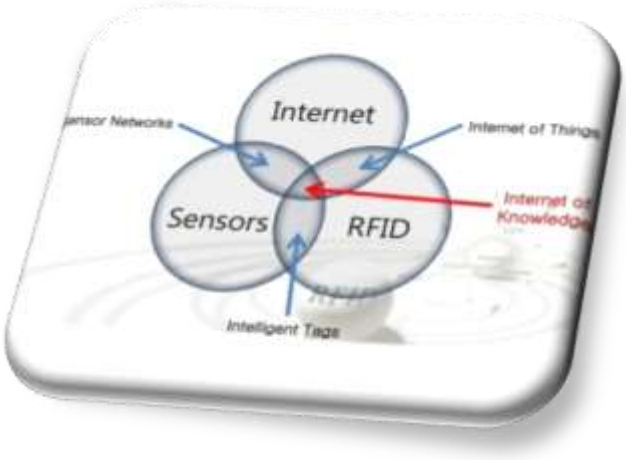

Figure1. IoT main Components

Currently, IoT is made up of a loose collection of purpose-built networks. It can be assumed as a machine which has multiple networks to control engine function, safety features, communications systems, etc. As IoT evolves, these networks, and many others, will be connected with added security, analytics, and management capabilities. This will allow IoT to become even more powerful in what it can help people [31]. Figure2 shows IoT as a network of networks. A very important element of IoT is Wireless Sensor Networks (WSNs).

A node in a sensor network capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network is a Sensor node. There are two types of sensor nodes as categorized in [9]. One is ordinary sensor or non-sink nodes. These are used to sense and monitor physical phenomena such as temperature, humidity etc., collect them. The other one is known as a sink (gateway) node that uses radio communication to collect data gathered by ordinary sensor. Moreover, sensor networks are connected to the external world through it. A sensor node Zolertia Z1is designed for general purpose development platform for WSN developers, researchers etc. Zolertia Z1 sensor node [10] is a low power WSN module. The two mostly employed operating systems are TinyOS 2.x [11] and Contiki [10], supported by Z1 sensor.

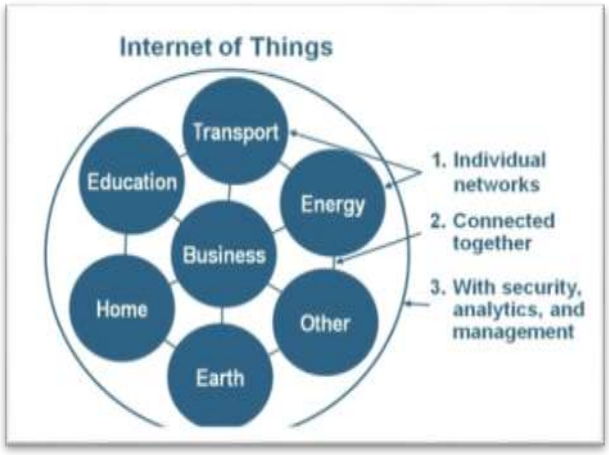

Figure2. IoT as a Network of Networks

WSNs establish a cheap sensory infrastructure to internet-connected devices. This flexibility causes any next descendant of Internet-enabled portable object to interact easily with the “Things” and create a new IoT. The specific components of WSN include gateways, nodes and a transparent data path between the application platform and the physical world [43]. Gateway is an interface between the application platform and the wireless nodes in WSN. The following is a briefly description of WSN characteristics:

1) Node mobility: more nodes can join to the network easily or disjoin when they move out of the range.
2) Unattended operation: it is the ability of reconfiguration the network by the nodes without any human intervention
3) Dynamic Network Topology: If a node or radio links fail, re-positioning of network topology is a must.
4) Limited power: Energy consumption is a major issue, and should be optimized at three stages, node communication, sensing and processing to reduce the energy consumption.
5) Large scale of deployment: The large scale of WSN from hundreds or thousands of nodes and some environmental parameters like noise, dispersion, interface and available bandwidth, that effects on the connection quality may causes some disconnection between the nodes even in tiny networks.

WSN has large number of applications, such as Structural Health Monitoring [6], networked control, signal processing, air pollution monitoring, etc. Some of WSN applications are inexpensive tool for monitoring diverse phenomena [3]. They also help in collecting data from vehicles and send them to the web portal [4], It also facilitates Water quality monitoring [5]. Since these applications were very useful, new technologies have been developed to implement WSN applications. Some of the standard based protocol stack includes 6LoWPAN, IEEE802.15.4e [8], (RPL Routing Protocol) and CoAP (Constrained Application Protocol) for the management of layer-related procedures.

6LoWPAN is the first wireless connectivity standard that was created for the IoT [44]. 6LoWPAN standard is defined by IETF to transmit IPv6 packets through computationally constraint networks

RPL stands for Routing Protocol for low power and lossy network. It can support a wide variety of different link

layers, including ones that are constrained, or typically utilized in conjunction with host or router devices with very limited resources. Also, it can build up network routes, to distribute routing knowledge among nodes and to adapt the topology in a very efficient way.
Constrained Application Protocol (CoAP) is a software protocol intended to be used in very simple electronics devices that allows them to communicate interactively over the Internet. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. Multicast, low overhead, and simplicity are extremely important for Internet of Things (IoT). CoAP can run on most devices that support UDP or a UDP analogue.Californium (Cf), Erbium (Er), and Copper (Cu) [14] are three implementations of CoAP. CoAP/UDP works well with IEEE802.15.4 since the MTU (Maximum Transmission Unit) is small. However, in a MAC with larger MTU at high rates, like WiFI IEEE802.11 family, with a MTU of 1500 Bytes, a HTTP transaction can be done with one packet at larger distances. CoAP uses the REST architectural style.

Representational State Transfer (REST) is a software architecture style consisting of guidelines and best practices for creating scalable web services.[42] REST is a coordinated set of constraints applied to the design of components in a distributed hypermedia system. It can lead to a more performant and maintainable architecture.[42].Thesis objective [13] offers a solution to integrate sensors into the Web using the principles of REST, the architectural model of the Web.

The main reason of using REST in IoT is the fact that it is more lightweight and IP based networking. The proposed framework in [41] defines a secure mobile web service and shows that this framework can enhance service performance and reliability in mobile network environments using REST principles.
In the following section a comparison between CoAP and HTTP is taken place to measure their transmission delays and response time.

II. Testing Results

A. *CoAP and HTTP*

A critical analysis of CoAP and Http is carried out experimentally. One of the experiments measure the packet reception delay against distances with different transaction sizes over CoAP application layer based on IEEE 802.154 communication protocol. The other is done on HTTP/TCP application layer based on 802.15.4 communication protocol [13].
Testing was carried out to measure the Transmissions delay and the Response time. Response time is the time taken by the server to react back to client. The components of the experiment include a client and server. Client queries an embedded server "Hello-World" resource. The response time was calculated for by keeping server at different distances with different transaction length.

1) COAP Scenario

Table1 shows a few results taken to evaluate the transmission delay by increasing the distance between server node and border router with different transaction sizes (Eg:50 bytes,100 bytes etc)on the CoAP server. The total number of bytes transmitted shows the size of the transaction during a retrieval of a resource.

TABLE 1 Communication timing requirements for transferring data over CoAP/UDP based on 80.15.4

Place	Transmission delay for byte transaction (sec)					
	1 byte	*50 bytes*	*100 bytes*	*150 bytes*	*500 bytes*	*1000 bytes*
1	0.169	0.176	1.508	1.694	11.796	19.484
2	0.167	0.311	1.763	3.277	Not received	Not received
3	0.377	0.296	1.186	8.794		

2) HTTP Scenario

Like CoAP scenario, experiments on packet reception delay against distances with different transaction sizes are made over HTTP/TCP application layer based on 802.15.4 communication protocol. Transmission delay was evaluated and measured by increasing the distance between border router and HTTP server by keeping it in places 1, 2 and 3 for our experiments. Table2 presents the results taken to evaluate the transmission delay.

TABLE 2 Communication timing requirements for data transferring over HTTP/TCP based on 802.15.4

Place	Transaction delay (sec) for				
	1 byte	*50 bytes*	*100 bytes*	*150 bytes*	*More than 150 bytes*
1	0.378	0.366	0.777	0.802	Not received
2	0.49	0.7	0.643	0.907	
3	1.808	1.551	8.165	21.021	

The results of **testing** suggest that CoAP protocol works better in transferring small transaction as it just needs 2 packets to transfer the data compared to HTTP that needs 14 packets in the same case because of using TCP three way handshaking. In case of sending large data, both protocols divide the message to some blocks and add one extra packet per each segment. So the number of packets using by CoAP/UDP and HTTP/TCP increases significantly. CoAP uses Block wise transfer [45] while HTTP uses the TCP three-way-handshake messages and just divides the transaction to some smaller packets, so they are not suitable to transfer large data as it consumes more energy and generates more traffic.
In case of exchanging large data from long distance the CoAP provides the better performance. It is observed that by increasing the distance between devices, there were some retransmissions in this experiment due to the decreasing in wireless signal strength. Losses in HTTP/TCP required more

time for retransmitting the entire transaction rather than CoAP/UDP, as the TCP retransmission mechanism produce larger transaction delays than the simple CoAP retransmission mechanism.

CoAP has lower communication overhead, the number of messages is lower and uses simpler hardware requirements ,which caused CoAP/UDP based protocols perform better for constrained networks compared to HTTP based resource retrievals (Fig 3)

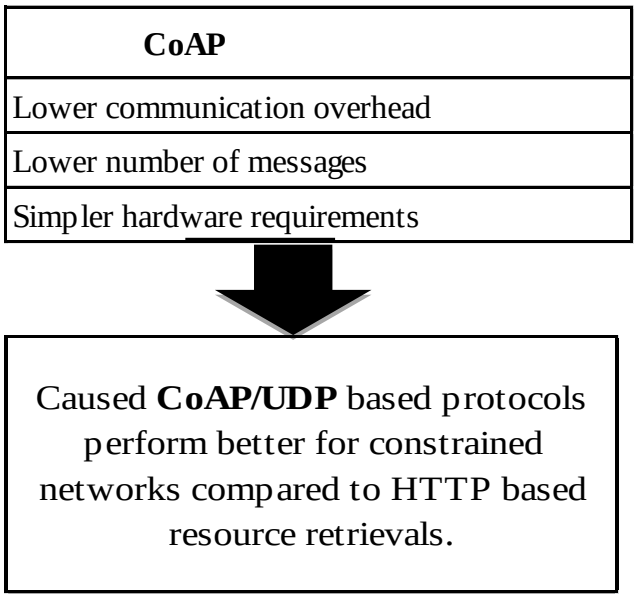

Figure3 shows the features of CoAP

After achieving the conclusion that CoAP is more suitable to IoT environment, some security issues evolved that need to be raised. In the next section, different security measures related to IoT are discussed.

III. Security of IoT

Security is the level to which the harm is resisted or protected.

The two reasons why security is an important factor to be considered, are Personal Protection of Information and Social Responsibility i.e., to protect the group you join when you connect your machine to the network [27]. Individuals or companies expect that their personal information contained in IoT products or systems

- Remains private
- Not to be subjected to unauthorized modification
- Be available to them.

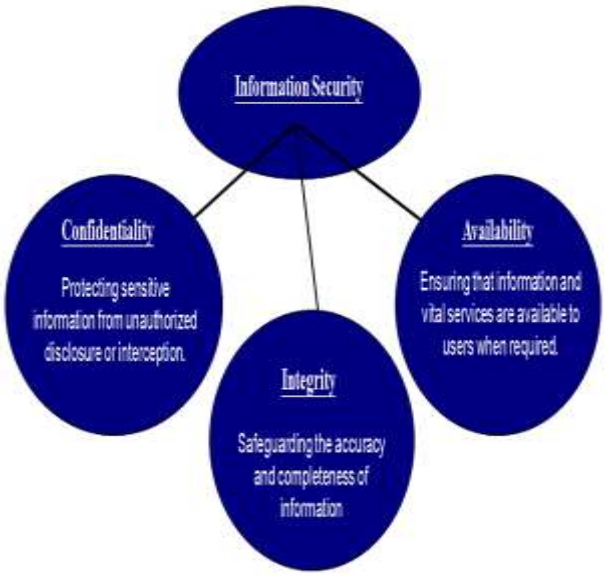

Figure4. Different Security Requirement

There are also legal framework for the protection of security and privacy [16]. Also, the Privacy Enhancing Technologies (PET) are described in order to ensure privacy. The security are guaranteed by supporting secure booting with hardware roots of trust, various access control mechanisms, secure package management and software updates, firewalling and IPS, and integration with network management and event correlation products [17].

According to the recent IoT security project [28], the following are the findings:

- Data security: Studies conducted to develop new computational models for securing data analytics and actuation on streams of real-time data.
- System security: Develop framework that quickly build IoT applications that use these new computational models.

Findings suggest that IoT applications need to first generate samples of data, and then filter them after processing. These are then combined with historical data, and then results generated for end applications to view.

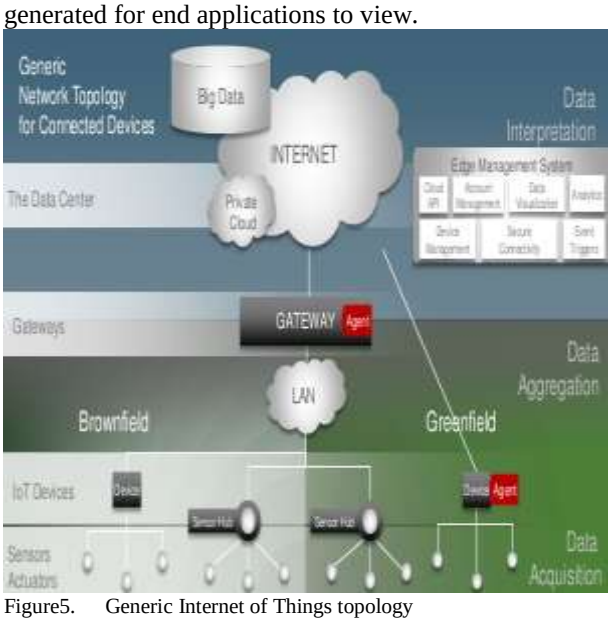

Figure5. Generic Internet of Things topology

The following section discusses the importance of mobile web services. The two types of service oriented architectures are compared to each other.

IV. Mobile Web Services

IoT is exploring ways to connect "smart things" that are having the capability of communicating, such as mobile phones etc. Home appliances might communicate with each other, to optimize their energy consumption and to offer smarter heating systems [19]. For instance, sensor nodes are networked together so that environmental monitoring applications can be created [18]. However, the challenging task is developing applications that integrate the functionality of multiple smart things. This is because it requires deep knowledge of each platform. The researchers put out the solution by trying to provide uniform interfaces, which can create a loosely coupled ecosystem of smart things services. To provide uniform interfaces to smart objects, there are two types of service-oriented architectures developed.

TABLE 3 Representational State Transfer (REST) via WS-Web Services

REST and WS	A Web Services Description Language (WSDL) file declares Functionality and interfaces.
REST	software architecture style consisting of guidelines and best practices for creating scalable web services. Resources are uniquely identified through URIs. (URI stands for Uniform Resource Identifiers Several representation formats like HTML are supported by resources that are negotiated at run time with the help of HTTP content negotiation. Designed to run on business or Web servers
WS-*	defines concepts like addressing, discovery and security Made to adapt to the needs of resource constrained devices. Lighter forms of Web Services, were proposed. preferred for "professional enterprise application integration scenarios"

When analyzed the performance of WS-* and RESTful applications [21] by deploying on WSN with limited resources, result concluded that REST performs better in [22, 23]. Readings from [24] show that Web services are very feasible for sensor networks utilizing less power. One of the major benefits of RESTful API is that it is flexible for data representation, for example we could serialize our data in either XML or JSON format. RESTful APIs are easier to understand because they add an element of using standardized URIs and gives importance to HTTP verb used (i.e. GET, POST, PUT and DELETE).

RESTful services are also lightweight, that is they do not have a lot of extra xml markup. To invoke RESTful API, the only requirement is a browser or HTTP stack and a condition that every device or machine connected to a network has that.

Finally, whichever architecture we choose, important aspect is to make sure it's easy for developers to access it, and well documented.

For Mobile Phones: During testing, participants were asked about how suitable each platform was, because mobile phone plays an important role in creating IoT applications.

A. *TESTING RESULTS*

Some participants also suggested: "I would use REST, since customers prefer speed and fun over security for smaller devices". Thus, we conclude that WS-* services are best for "professional enterprise application integration scenarios" and RESTful services for tactical integration over the Web.
While coming to application part of IoT and Wireless sensor networks (WSNs), they are used in several e-Health systems. Here, a physician can monitor a patient continuously and real time, either locally or remotely, at lower cost and being less intrusive in the routine than the traditional monitoring equipment. Physical therapy aiding systems are a particular case of such systems. The work [28] presents a system aimed at assessing joint angle and vital signs to assist physical therapists.

% of people	REST	WS-*
Favouring	53%	16%
Web Services	Easier to learn	Comparatively difficult
Programming IoT applications	More suitable	Less suitable
Undecided among people	32%	
Amount of data processed	Smaller	Larger
Android	Supported	Not supported, supports HTTP.
Advantages	intuitiveness, flexibility, and lightweight	support more advanced security requirements

v. Conclusion

In this paper, we have discussed internet of things in the field of WPS, TCP and IEEE 802 considering testing results. Paper also discussed the security issues of things and the mobile Web services.

Papers Based on Web services survey, further studies should conduct a wide attention to developers' experience. We have also presented testing results to conclude that WS-* architecture can be chosen when considering business applications, but in some other cases, REST was more important.

Also we must give attention to participants' remarks or suggestions so that clear cut idea between REST and WS-*.

As a future Scope in this field, a wide study must be conducted in the area of challenges regarding the limitation of mobile devices. The limitations to CPU processing power, smaller memory, and low battery power etc. New and unique characteristics for web services regarding IoT in mobile environment must be developed.

As no previous research was conducted on the practical part of privacy and security, thus it exposes the information to intermediate nodes while confidentiality is only meant for end-to-end. The theoretical part is explained very deeply. Also, there are limitations in sensors, for example, low cost devices cannot be very accurate, and there can be problem of non-linearity. The end-to-end security must be adopted because gateways and cloud will remain unaware of the data even if its operating on it. The permission to decrypt and view data will be confined to end applications only

Acknowledgment

This work was supported by Kuwait Foundation Advancements of Sciences (KFAS) grant P11418EO02.

References

[1] Dr.OvidiuVermesan SINTEF, Norway Dr. Peter Friess EU, Belgium. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. 2013

[2] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. RFC 4944: Transmis-
sion of IPv6 Packets over IEEE 802.15.4 Networks. 2007

[3] J. Yick, B. Mukherjee, and D. Ghosal. Wireless sensor network survey.Journal of Computer Networks, Volume 52(Number 12):22922330, 2008

[4] RAFAEL BASSO. Wireless Sensor Networks in a Vehicle Environment. 2009

[5] T. Le Dinh, W. Hu, P. Sikka, P. Corke, L. Overs, and S. Brosnan. Design and deployment of a remote robust sensor network: Experiences from an outdoor water quality monitoring network. In Local Computer Networks, 2007.LCN 2007.32nd IEEE Conference on, pages 799806. IEEE, 2007

[6] BengiAygün, VehbiCagriGungor. Wireless sensor networks for structure health monitoring: recent advances and future research directions. Journal: Sensor Review Volume: 3 Number: 3 Year: 2011

[7] Jebah Jaykumar, Prameetha Pai, Prarthana T.V"Secure implementation of IOT based on RFID with key authority mechanism"

[8] S. Hara, D. Zhao, K. Yanagihara, J. Taketsugu, K. Fukui, S. Fukunaga, and K. Kitayama, "Propagation Characteristics of IEEE 802.15.4 Radio Signal and Their Application for Location Estimation,", June 2005.

[9] List of wireless sensor nodes:
http://en.wikipedia.org/wiki/List_of_wireless_sensor_nodes#List_of_gateway_sensor_no
des.

[10] Contiki operating system official website: http://www.contiki-os.org/
.

[11] TinyOS official website: http://www.tinyos.net/.

[12] MSP430F2617 datasheet: http://www.ti.com/lit/ds/symlink/msp430f2617.pdf

[13] Farnoosh Farokhmanesh ,"ANALYZING AND EVALUATING NETWORK PROTOCOLS IN IoT", December, 10, 2014

[14] The main web page of CoAP: http://people.inf.ethz.ch/mkovatsc/

[15] Nor Azizah Saadon, Radziah Mohamad, "A Comparative Evaluation of Web Service Discovery Approaches for Mobile Computing ",2011

[16]Rolf H. Weber," Internet of Things – New security and privacy challenges, University of Zurich, Zurich, Switzerland, and University of Hong Kong, Hong Kong, January 2010

[17] Wind River, "Security in IoT", world leader in embedded software for intelligent connected systems, January 2015.

[18]DoganYazar and Adam Dunkels. Efficient application integration in IP-based sensor networks.

[19]Dominique Guinard, VladTrifa, and Erik Wilde. A Resource Oriented Architecture for the Web of Things, Mar 21, 2015

[20] R. Fielding. Architectural styles and the design of network-based software architectures

[21] DoganYazar and Adam Dunkels. Efficient application integration in IP-based sensor networks, Berkeley, CA, USA, November 2009.

[22] CesarePautasso and Erik Wilde. Why is the web loosely coupled?: a multi-faceted metric for service design., Madrid, Spain, April 2009. ACM.

[23] CesarePautasso, Olaf Zimmermann, and Frank Leymann. Restful web services vs. big web services: making the right architectural decision, New York, NY, USA, 2008. ACM.

[24] DoganYazar and Adam Dunkels. Efficient application integration in IP-based sensor networks. In Proceedings of the First ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings, Berkeley, CA, USA, November 2009

[25] Z1 datasheet, http://zolertia.sourceforge.net/wiki/images/e/e8/Z1_RevC_Datasheet.pdf

[26]Drytkiewicz, W., Radusch, I., Arbanowski, S., Popescu-Zeletin, R.: pREST: a REST-based protocol for pervasive systems. In: 2004

[27] Anne-Laure SIXOU,Thierry BOUSQUET Frederic VAUTE, " Embedded Java & Secure Element for high security in IoT systems-Java one, September 2014

[28] Philip Levis "Secure Internet of Things Project (SITP) ", Stanford University, August 11,2014

[28] Alves, R.C.A. , Brazil Gabriel, L.B. ; Trevizan de Oliveira, B. ; Borges Margi, C., Dept. of Computer Eng. & Digital Syst., Univ. of Sao Paulo, Sao Paulo ,"Assisting Physical (Hydro)Therapy With Wireless Sensors Networks",

[29] Debiao He and SheraliZeadally; "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography", February 2015

[30] SecureRF: Securing the Internet of Things | Security and anti-counterfeiting solutions.

[31] Dave Evans ,"The Internet of Things How the Next Evolution of the Internet Is Changing Everything ", April 2011

[32]ChristophJechlitschek,"Radio Frequency IDentificationtrends",Nov 2013

[33] B. Jiang, K. P. Fishkin, S. Roy, and MatthaiPhilipose, "Unobtrusive Long-Range Detection of Passive RFID Tag Motion", IEEE Transactions On Instrumentation And Measurement, 2006

[34] R. Weinstein, "RFID: A technical overview and its application to the enterprise," IEEE IT Prof., vol. 7, no. 3, pp. 27–33, May/Jun. 2005.

[35] S. Wang, S. Liu, and D. Chen, "Analysis and construction of efficient RFID authentication protocol with backward privacy in Advances in Wireless Sensor Networks". Berlin, Germany: Springer-Verlag, 2014,

[36] Y. Liao and C. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," Ad Hoc Netw., 2014.

[37] J. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," J. Supercomput., vol. 70, no. 1, pp. 75–94, 2014.

[38] Z. Zhao, "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem," J. Med. Syst., vol. 38, no. 5, 2014

[39] Z. Zhang and Q. Qi, "An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography," 2014

[40]M. Farash, "Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography,"J. Supercomput., 2014

[41] FedaAlShahwan, Maha Faisal," Security Framework for RESTful Mobile Cloud Computing Web Services",2015

[42]Pautasso, Cesare; Wilde, Erik; Alarcon, Rosa (2014), "REST: Advanced Research Topics and Practical Applications",2014

[43] J. Cecílio, P. Furtado, "Wireless Sensors in Heterogeneous Networked Systems",2014

[44] Gil Reiter, " Wireless connectivity for the Internet of Things", June 1,2014

[45] Z. Shelby ARM, K. Hartke, C. Bormann Universitaet Bremen TZI, The Constrained Application Protocol (CoAP), June 2014

Feda AlShahwan is currently an Assistant Professor at the Electronic Engineering Department/Computer Section of the College of Technological Studies in the Public Authority for Applied Education & Training. Has a diverse research interest in Mobile Web Services and their applications. Born in Kuwait, obtained her B.Sc., M.Sc. in Computer Engineer from Kuwait University 1992, 2004 respectively. Her Ph.D. degree was in "Adaptive Service Provision and Execution in Mobile Environments" from Centre for Communications Systems Research in University of Surrey. The current research interests included studies of Adaptive Mobile Web Services, Social networks and Mobile Cloud Computing.

Maha Faisal was born in Kuwait. She earned her B.Sc. and M. Sc. in computer engineering from Kuwait University at 1997 and 2000 respectively and her Ph.D. from the University of Colorado at Boulder, 2005.
Dr. Faisal is currently an Assistant Professor at the Computer Engineering Department, Kuwait University. Her research interests include: human computer interaction, social networks, mobile computing and software system modeling.