# Middleware Framework for Wireless Sensor Networks

Sajjad Hussain Shah, Ilyas Yaqoob, Wajid Ali, Sohail Jabbar

**Abstract—Wireless Sensor Network has large domain of application with different desires. The protocol and network infrastructure change as per application requirements for the purpose to gain the best network resource allocation and performance so network operation must be adapt based on application requirements. In this article we propose service oriented middleware framework for wireless sensor networks (WSNs) with security requirements. XML, SOAP and WSDL are used for network communication. The architecture provides an interface between user applications and the network which offer an automatic choice of the network configuration and data communication approaches.**

**KEYWORD:** middleware, sensor networks, security, web services.

## I- MOTIVATION

A Wireless Sensor Network (WSN) is collection of multiple sensors that communicate via wireless technology, collecting information and relaying them until a central data collector [1]. There are two types of nodes in the network: sensor nodes, responsible for collecting the data, the collectors, responsible for collecting and processing data gathered. The WSN must be able to meet certain requirements specific to their proper functioning. the devices composing the network are usually small and should be able to operate without intervention for some time, so must have an efficient power management for can do their jobs for as long as necessary. Furthermore, they must also have a data processing efficient, due to the low computational power of devices responsible for data collection. The development of applications for these networks involves knowledge and control of hardware and software available. Most projects assume WSNs existence of a strong coupling between the component application and the underlying levels, i.e., the stack of protocols and infrastructure [1] [2]. This coupling is justified by the need to achieve efficient systems in terms of energy. This coupling produces rigid systems and thereby generates networks built specifically to meet a few applications. However, WSNs can benefit from the existence of a middleware system located between the component includes applications and network components [2].

Manuscript Received August 18, 2012.

Sajjad Hussain Shah, Member, Bahria University Wireless Research Center (Email: sajjadmcse@gmail.com)
Ilyas Yaqoob,City University of Science & Information Technology Peshawar (Email: ilyas_danish@hotmail.com)
Wajid Ali, Member, Bahria University Wireless Research Center (Email: Wajid_6@yahoo.com)
Sohail Jabbar, PhD Scholar, Bahria University Wireless Research Center (Email: sjabbar.research@gmail.com)

Middleware is application based software which exist in the middle of application and supporting infrastructure by providing interfaces the reuse of services that can be composed and configured for easy application development which is consider more efficient for a distributed environment as a WSN [2] [3] [4]."

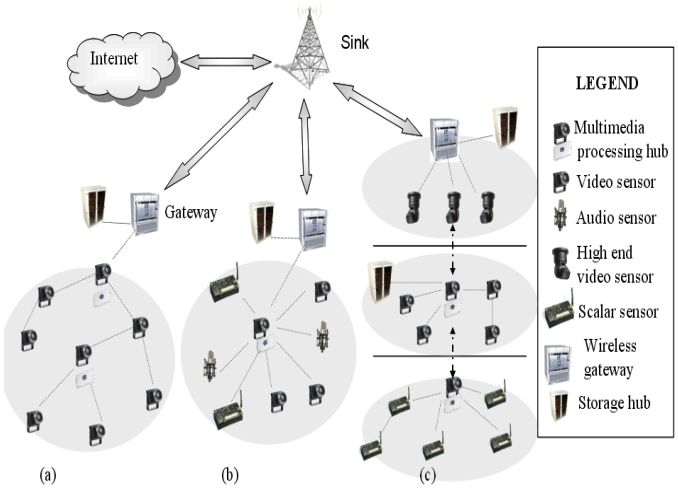


**Figure 1: Wireless Sensor Network Architecture**

A middleware system must allow communication between distributed components; cover up the applications the complexity of the network environment. The middleware must meet the specific requirements of WSNs and provide features that facilitate integration applications to the network and the work of developer's applications [2] [3] [4]. Examples of these features are providing an interface for accessing the sensors to get your data, activation / deactivation of sensors to performing tasks, network settings and security, among other. One approach that has been proposed recently in literature for the middleware of WSN is web services [3] [5] [6] [7] [8]. Web services are based on SOA (service-oriented architecture) to systems integration and provision of services, since its use makes it possible applications that can interact with each other, even acting in systems developed on different platforms [9]. Several middleware architectures using web services have been proposed in the literature for WSNs [3] [5] [6] [7] [8], but secure web services for WSNs have been studied. The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. Several proposals for security arrangements have been discussed in the literature, but many questions remain open [10] [11] [12] [13].

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

This paper proposes an architecture using middleware secure web services to facilitate the development of applications in sensor networks with security requirements.

## II- ARCHITECTURE PROPOSAL

The components of SOA are essentially collections of services that communicate by exchanging messages. Information is represented in an XML (eXtensible Markup Language) standard language written in WSDL (Web Services Description Language) [9]. Calls to the operations, including input / output, are encoded in SOAP (Simple Object Access Protocol, based on XML) [9].

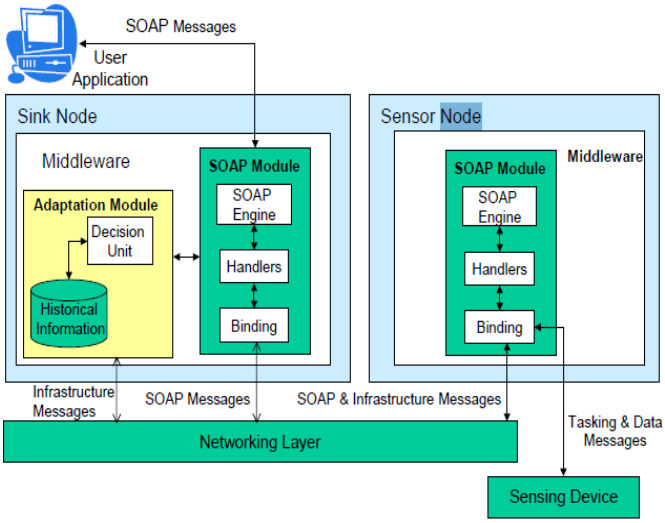


**Figure 2: Sink and Sensor Node Components**

WS-Security is used for security requirements [14], especially the XML Encryption [15] and XML Signature [16], which are part of WS-Security. The use of XML Encryption is one way to encrypt the data ensuring their confidentiality. The big difference with XML Encryption for secure protocols such as SSL (Secure Socket Layer) is the possibility of confidentiality persistent, i.e. in the secure protocols confidentiality occurs only during the session. Already in XML Encryption provides the same security due to encryption of data even with the end of the same [15]. This standard enables the encryption of some parts of document may leave parts of the insignificant Content visible to the attacker. For encryption to be selected algorithm (3DES, AES, etc.) and key encryption. The message data is then serialized and encryption is performed, generating the XML structure Match: Encrypted Data. The decryption must first determine the algorithm and key used for encryption in then decrypt the data. After the decryption can be processed XML elements. The algorithm used in this work was the AES. XML Signature is a standard developed by W3C as way to ensure authenticity SOAP messages [14] [16]. This type of signature is intended to give the receiver sure that a text was created by a particular entity and that has not changed. The processes consist of Extracts (Hash) of the text and then encrypt this summary to the signer's private key. The receiver must calculate the summary the text the same way and still decipher the abstract encrypted with the signer's public key.

The certainty of does not change the wording and the signer's identity is obtained if the two resumes are alike. The XML Signature can be used only in some parts of the message, allowing so the other can be modified without the signature to be impaired. The signature method used architecture was the RSA. Our proposed architecture shows information about different events in a given environment, through which data is collected by sensors that are further processed by a server (collector), using the services web, available on a website. A vision general architecture can be seen in Fig 3.

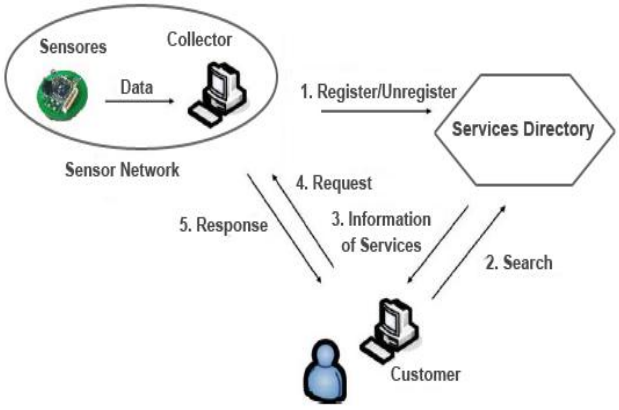


**Figure 3: Overview of the Proposed Architecture**

Data collected by sensors targeting requirements energy and processing of WSN. There is also a collector responsible for receiving data from sensors and store them in a database of information. Data sent in transmissions from the sensors to the collector using web services and SOAP messages. However, for communicating collector to the sensor, using protocol UDP (User Datagram Protocol). This protocol is used for the sensors do not need to provide a web service to the collector, which would imply a higher consumption of energy and processing the sensor node. After being collected by the sensors, the information is stored by the collector in a database where they can be accessed and displayed to the user so that this desired. This provision will be made using the services web requests and responses for the data, allowing so that there is the wish to another application case interoperability use the data collected. To this end, the WSN need to register their services in a directory service where the customer can seek services offered by various WSNs.

Services can then be directly accessed by request / response at the collector of WSN. For the provision of information to users is created a web page. The user looks in the directory which services are available and then make the request directly to the collector. The request / response between client travels through SOAP messages. To ensure the security, data is encrypted using XML Encryption and authenticated by XML Signature. In Figure 1 will show a WSN, but other systems can be added in the architecture, using the same directory services. The website is divided into two modules: one to access the information by the user, and another administrative character, allowing some of the actions sensors are controlled by the network administrator.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

## III- OPERATION OF ARCHITECTURE

After all the applications needed to be developed, you can check the operation of the architecture by complete, since the collection and transmission of data by prototypes of the sensors to the availability to users. The operation involves primarily two functions which are described in the following subsections: the collection and data storage and availability of these data.

### *A) Configuration, data collection and storage*

The process of data collection is done by the prototype the sensor nodes, which are responsible for capturing data and forward them to the sink node. The collector is responsible for store the data, making them available for client applications. The first step occurs when the sensor is the prototype activated, initiating the process of identifying the same. The public and private key of the RSA algorithm to be used are generated in XML Signature. When the prototype is executed, it sends a message to the sink node containing the set ID and its public key algorithm RSA. The server makes a query to the database and returns the other characteristics (energy, latitude, etc.) to Sensor in accordance with the code sent. The server must also generate your public key and private RSA algorithm and also the symmetric key AES algorithm to be used in XML Encryption, then server send its RSA public key algorithm and AES algorithm, encrypted with the public key previously sent by the sensor. The communication at this stage of WSN configuration is done using the UDP protocol. With the identification made, the sensor is ready to collect and submit data, but can only do so if your status is set to active. The collected data can then be sent to the collector using the web service receive value. Finally, when receiving the data sent on SOAP messages, the sink node is responsible for treating them and stores them in a database. The messages are SOAP service Receive value encrypted and authenticated using XML Encryption and XML Signature, respectively. The public and private keys of collector and the sensor are used by XML Signature for message authentication. Thus, both the collector and the sensors can ensure the integrity of messages receives. The collector also updates the database information data from sensor nodes, as the last date of collection. An overview of the setup cycle, collection and information Storage can be seen in Figure 4.

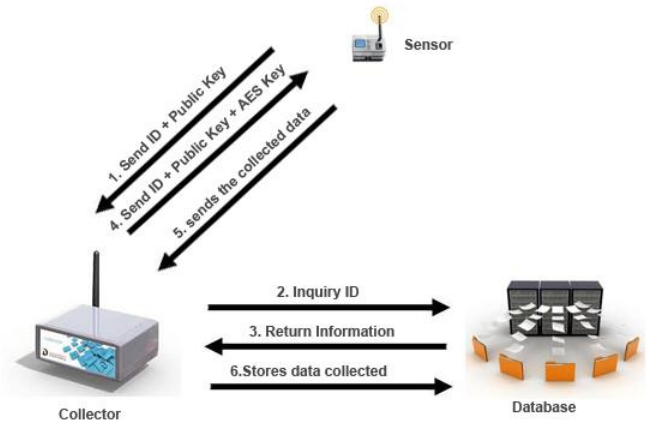


**Figure 4: Cycle Configuration, Collecting and Storing Information**

### *B) Provision of Information*

The process of making information available can occur from the moment that data are collected by the sensors, since from the first access to the page information has already been brought to the user. The objective of process is to show the user and dynamically updated all information collected by the sensors. The first step is to verify the user in the directory services which are WSN available. Once the home of the WSN is accessed, the service sending services web is called to bring and show the user the types of services available for WSN. After choose the type of service, the user is taken to another page JSP, which are presented more detailed information about the chosen service. In access, web services are two called to assist in the provision of information, they being the send value services, used to send the send data values collected and used to send only dates available for consultation. The page shows the value collection of the last performed, ie the current value of that type service, and a history of all the values gathered. The web services sending services and send value send data have their messages encrypted and authenticated with XML Encryption and XML Signature. At the end of the process, user can verify the data collected for that type of service, and to observe through the presentation of and historical charts. An overview of the entire cycle of process can be seen in Fig 5

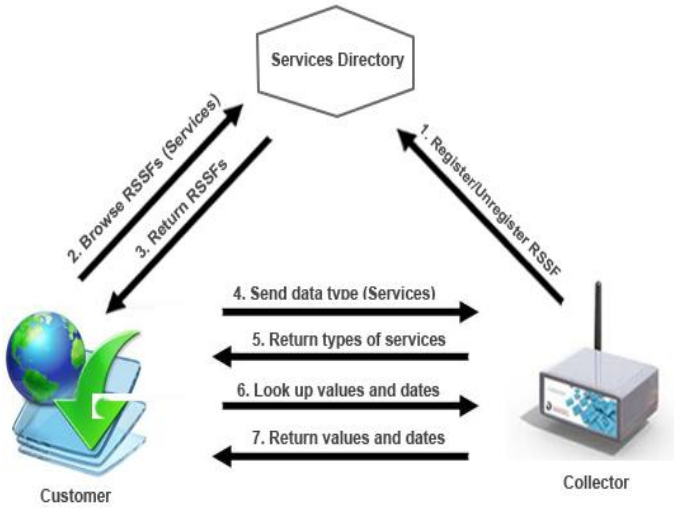


**Figure 5: Cycle Provision of Information**

## IV- RELATED WORK

MILAN [5] is existing middleware architecture for WSNs that collect a sketch of application requirements and select the best sensor and network configuration that meets such requirements while prolong network lifetime. MILAN incorporates state-based changes in application needs and it manages different network circumstances along the time. It does not address the issue of providing a standard representation for application needs and sensor generated data. In early version MILAN assume a centralized approach, which is not recommended for large scale wireless sensor networks.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

## V- CONCLUSION & FUTURE WORK

In this article we propose a middleware framework using secure web services to facilitate the development of applications in sensor networks with requirements safety. In this model the collector node allows access the WSN through web services that are accessible through external customers. The proposed middleware assists in developing secure applications for WSNs. Our Proposed framework works according to four main phases.

(i) Publication of sensor description
(ii) Submission of application interests
(iii) Establishment of the WSN and configuration
(iv) Data advertisement.

One motivating improvement of the proposed system emerge when multiple protocols are simultaneously available and the best appropriate option is transparently chosen, based on information from the interest pretense by the user, So we can consider the work as initial and basic step to design a flexible and energy efficient Wireless Sensor Network.
The proposed framework can be deploy and simulate and security specification for Web services WS-Security, with the use of encryption and message authentication are guaranteed the principles of confidentiality, integrity and availability of data from the WSN. We recommend/ will use Java as programming language to implement and proof the concept of our proposed system architecture as extension of our existing work.

## REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam. e E. Cayirci. “A survey on sensor networks”. IEEE Communications Magazine, pp. 102-114, 2002.

[2] S. Hadim e N. Mohamed. “Middleware: Middleware challenges and approaches for wireless sensor networks”. IEEE Distributed Systems Online, vol. 7, no. 3, 2006.

[3] F. Delicato, P. Pires, A. Lages, J. F. Rezende, L. Pirmez “Middleware orientado a serviços para redes de sensores sem fio”. XXII Simpósio Brasileiro de Redes de Computadores, Gramado-RS, 2004.

[4] A. R. L. Ribeiro, L. C. Freitas, C. R. L. Francês e J. C. W. A. Costa.“SensorBus – A policy-based middleware for wireless sensor networks”, IEEE Latin America Transactions, vol. 6. no. 7, pp. 647-654, Dec. 2008.

[5] F. Ciancetta, B. D’Apice, D. Gallo, e C. Landi. “Plug-n-play smart sensornetwork with dynamic web service”. IEEE Transactions on Instrumentationand Measurement, vol. 57, no. 10, pp. 2136-2145, 2008.

[6] I. Amundson, M. Kushwaha, X. Koutsoukos, S. Neema. J. Sztipanovits. “Efficient integration of web services in ambient-aware sensor network applications”. Proc. of the 3rd IEEE/CreateNet International Workshop on Broadband Advanced Sensor Networks (BaseNets 2006), Outubro 2006.

[7] A. Sleman e R. Moeller. “Integration of wireless sensor networks services. into other home and industrial networks using DPWS”. 3rd International Conference on Information and Communication Technologies (ICTTA 08), April 2008.

[8] T. Ta, N. Othman, R. Glitho e F. Khendek. “Using web services for bridging end-user applications and wireless sensor networks”. Proc. of the 11th IEEE Symposium on Computers and Communications, Junho 2006.

[9] W3C (World Wide Web Consortium). “Web Services Architecture”. Disponível em: http://www.w3.org/TR/ws-arch. 2004.

[10] D. Djenouri, L. Khellladi e L. Badache. “A survey of security issues on mobile ad hoc and sensor networks”. IEEE Communications Surveys, vol. 7,no. 4, pp. 02-28, 2005.

[11] X. Du e H. Chen. “Security in wireless sensor networks”. IEEE Wireless Communications, vol. 1, pp. 60-66. 2008.

[12] M. Healy, T. Newe. e E. Lewis. “Security for wireless sensor networks: a review”. IEEE Sensors Applications Symposium, New Orleans, EUA, 2009.

[13] Y. Wang, G. Attebury.e B. Ramamurthy. “A survey of security issues in wireless sensor networks”. IEEE Communications Surveys, vol. 8, no. 2, pp.02-23, 2006.

[14] E. Mello, M. Wangham J. Fraga e E. Camargo. “Segurança em services web”, VI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), p. 1-48, 2006.

[15] T. Imamura, B. Dillaway, e E. Simon. “XML Encryption Syntax and Processing”. W3C. Disponível em http://www.w3.org/TR/xmlenc-core. 2002.

[16] M. Bartel, J. Boyer e B. Fox. “XML-Signature Syntax and Processing”.W3C. Disponível em http://www.w3.org/TR/xmldsig-core.2002.