Australian Journal of Basic and Applied Sciences, 5(3): 694-701, 2011
ISSN 1991-8178

Security in Wireless Sensor Networks Based On Service-Oriented Architecture

[1]Mohammad Ali Shamalizadeh, [2]Shahaboddin Shamshirband, [3]Mohsen Amiri, [4]Samiria Kalantari

[1]Imam Hossein University, Department of Marine Science
[2]Department of Basic Science, Chalous Branch, Islamic Azad University, Chalous, Iran.
[3]Chief Executive Officer of Andishe Pars Education and Research Institute, Iran.
[4]Young Research Club, Isamic Azad University, Sari Branch, Iran.

Abstract: In this article a new security model is introduced in which capabilities (such as loose connections, interactions independent of the technology and platform used among components, gradual development) and the service-oriented architecture, which is a new concept in architecture composed of (SOAP, WSDL, UDDI, …) standards, and the security measures of this architecture are used to address shortcomings in the security sections of wireless sensor networks (such as the fact that these sections are not concentrated, they are wireless, their cost cannot be reduced very much, they are dependent on nodes, their nodes perform several functions, etc.) So that a concentrated security system is established in the network and security shortcomings of WSN are reduced.

Key words: security measures, sensor nodes, service-oriented architecture, Wireless sensor networks.

INTRODUCTION

Wireless sensor networks are often used in military systems, but they are also employed in various other systems (in commerce, in the service industry, in medicine, etc). The main application of these networks is in monitoring environments and in detecting targets. Two design types are employed in wireless sensor networks:

1. Infra-structure which is based on a central and controlled structure the nodes send information to.
2. The mobile ad-hoc which does not obey a concentrated structure. And in which information is exchanged among nodes.

The main purpose in wireless sensor networks is to collect information from the physical world and to transmit it to the visual world. A secondary purpose in using these networks is to increase the life-time of the network as much as possible. Constraints in WSN_s, which are due to cost cutting and also result from the dimensions of these networks, cause weaknesses in security. In this article, the advantages of SOA (service oriented architecture) are used in an attempt to eliminate some of these weaknesses or to improve security.

Wireless sensor networks (WSN):

A wireless sensor network is composed of a large number of nodes in each of which there are a number of sensors. These sensors are placed manually or by random at desired locations; but sometimes no definite pattern is followed in placing the sensors so that they can be put in inaccessible or dangerous locations. These sensors evaluate conditions such as temperature, tremor, light intensity, pressure, etc. and the processed information is sent through radio signals to control stations in order to be used in the operations. The main components of a wireless sensor node are the sensors, the microwave and the radio frequency exchange device, and a power source. The sensor reaches the end of its life-time when this power source is used up.
The hardware components of a sensor node are as follows:

- The central processing unit
- Radio connector
- Auxiliary memory
- Various sensors
- Global positioning system
- Power source

In conventional sensor networks, the sensor connected man with the information base, but in modern wireless sensor networks the sensor is directly connected to the physical world.

Corresponding Author: Shahaboddin Shamshirband, Islamic azad University, chalous branch, Iran.

A wireless sensor network has the following characteristics: it

- Is dependent on the application
- Is interactive
- Is scalable
- Has components with limited power
- Is self-configuration
- Is reliable and of high service quality
- Is simple
- Is data-oriented

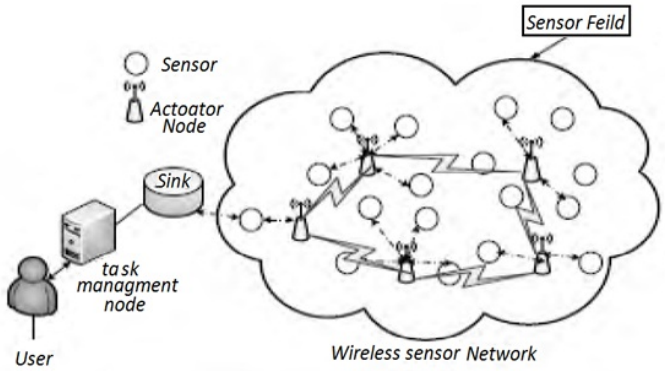

Fig. 1: Architecture of WSN

General characteristics of a sensor network:

1. In modern networks, direct contact with the main station is not necessary. Instead, sensors are grouped into clusters and each cluster uses its cluster head to connect with the control station. The cluster heads are chosen by using complex algorithms and through following the protocols relevant to clustering.
2. The adaptive mesh architecture is used to increase or decrease the number of the nodes (in order to maintain a balance at the level of the sensors.)
3. Each sensor in the network has a sensor range which completely covers the points located within the range (in order to cover the whole area, the points in the area must be covered).

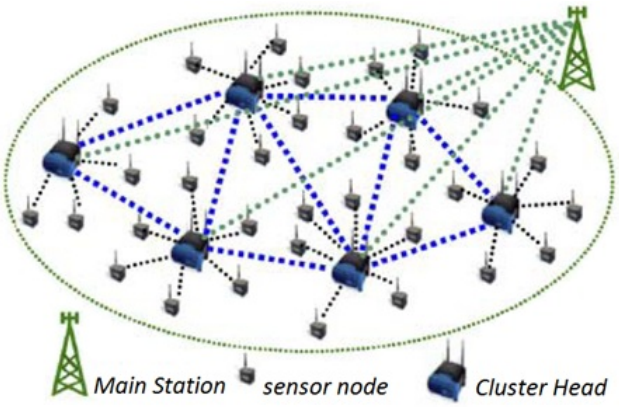

Fig. 2: Architecture of WSN

Problems encountered in extending WSN_s with the purpose of increasing network security:

- Joint radio channel for transmitting data
- Insecure operational environment
- Insufficient central power
- Limited resources
- Physical vulnerability
- Insufficient connections among nodes

Origin of the weakness in the security of WSN$_s$:

- Lack of infrastructure(solutions for security problems are not centralized)
- Use of wireless links(penetration without physical access to links)
- Multiple truncation of the nodes(nodes perform operations such as routing)
- Strong dependence of the performance of the network on the behavior of the nodes(unreliability)
- Autonomy of the nodes in changing their locations(the difficulty of routing)
- Lack of stable topology
- Limitation in power sources, processors, and memory.

Methods in WSN Security:

1. WEP (wired Equivalent Privacy)(secret communication):
   In WEP, the RSA method of cryptography based on the RC4 algorithm is used to prevent entry by unauthorized users. One of the shortcomings of WEP is that servicing of receivers is performed by manual adjustments.
2. SSID (Service Set Identifier)(identifier coding service):
   In this method, unique identifiers are determined for access to the network and these identifiers are placed at several access points.
3. MAC (Media Access Control) (control and access tools):
   In this method, the MAC list of addresses of a requesting computer is compared with the MAC list of addresses of the WSN in order to authenticate access. One of the shortcomings of this method is that in large networks it becomes difficult for these addresses to enter the access points.

Service-Oriented Architecture (SOA):

SOA is a style of architecture containing rules on patterns and criteria that lead to features such as modularity, loose connections, reuse, etc. As for as the structure of SOA is concerned, one component requests service and another component supplies it.

Advantages of SOA over other Architectures:

- Greater speed and agility in transactions (changes in the system)
- The capability of reuse
- The IT technology is kept coordinated with the profession
- Gradual development and implementation
- Independence of the systems and the architecture from the physical environment
- Reduced cost of extension and maintenance as well as the capability of being integrated and reused.
- Ensured interactiveness due to the fact the standards are followed.
- Explicit definition of the responsibilities of each service makes most parts of the organization accountable.
- Flexibility and ease of changing service providers (which provide internal and external services
- Etc.

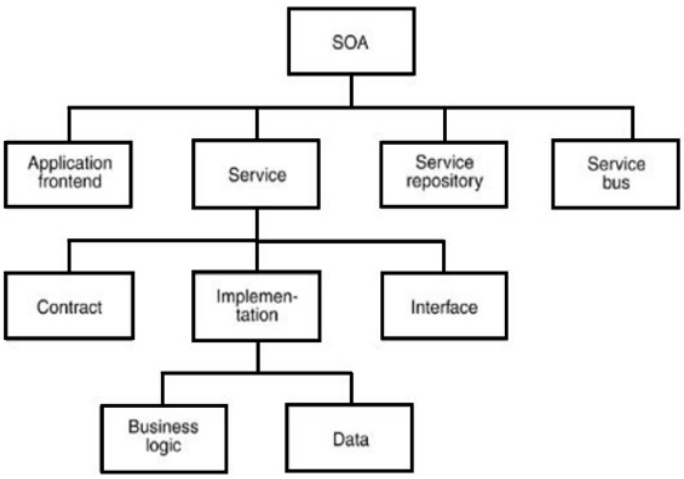

Fig. 3: Components of Service-Oriented architecture

SOA protocols:

1. The XSD language: the language part of the description of the XML schema has the responsibility of officially defining the hierarchical structure of XML documents. XML is an example of XSD.
2. Raw Object Access Protocol (SOAP): a structure for exchanging messages in the XML format among Web services.
3. Web Services Description Language (WSDL): a language based on XML used for describing the operational characteristics of Web services. It is composed of two parts: the description of the interface and the implementation.
4. Universal Description, Discovery and Integration (UDDI): an interface for propagation and identification of Web services. In consists of a repository from which providers broadcast and advertise their services so that others can identify the repository

The BPEL language: the language of executing the processes of the related profession. It has the following characteristics:

- It is independent of platform and based on XML.
- It is a language for describing the behavior of the processes of the related profession with the help of the services.
- It has structures for flow control and for conditions required for extensions
- It is capable of covering more complex cases such as sub processes.
- It is introduced as open source standard
- It uses WSDL to describe service interfaces

Security in SOA:

Security is an inseparable aspect of software and service-oriented architecture (because of the distributive, future interactive and reusable nature of this architecture), as compared with traditional applications, it has new and additional aspects. Some of the methods of ensuring security, which are efficient in centralized and conventional applications, cannot be of use in SOA.

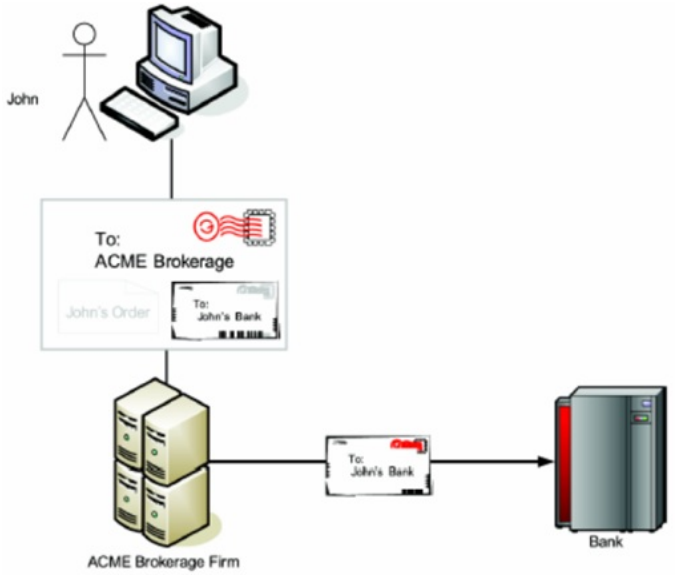

Fig. 4: security at message level point-of-view used for SOA (Ram 0.8)

Security in SOA:

1. Security at message level:

To establish security in the message the sender sends for the main receiver through the use of the interface, the security at the message level method is used. In this method, the different parts of a message are protected separately so that the message is only usable to intended sections located along the path.

2. Security as a service:

A security service can provide application programs with security capabilities (credit validation, authority validation, cryptography, etc.). This will not destroy the security sections in other services. The security service works fundamentally, and even indirectly. The security system is separated from the commercial logic (commercial services) in discussions on growth and development, because the security service is centralized and unrelated to applications; therefore, it is assigned to people who work as security personnel.

3. Policy-oriented security

Security requirements and mechanisms should not be attached to the application program, but should be separately declared (mostly manually) as the "security policy". The security logic is separated from the commercial logic and is placed at the hands of security specialists. The instruction capability is also increased; and in the W-S-Security Policy standard, this logic is employed.

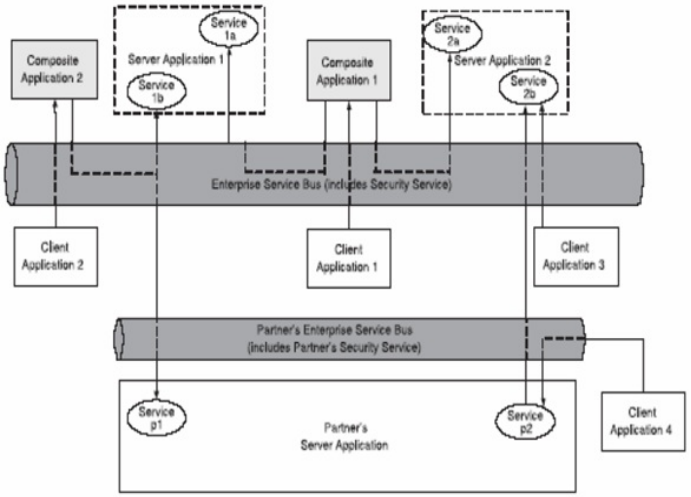

Fig. 5: implementation of the security logic as part of ESB [Ram 08]

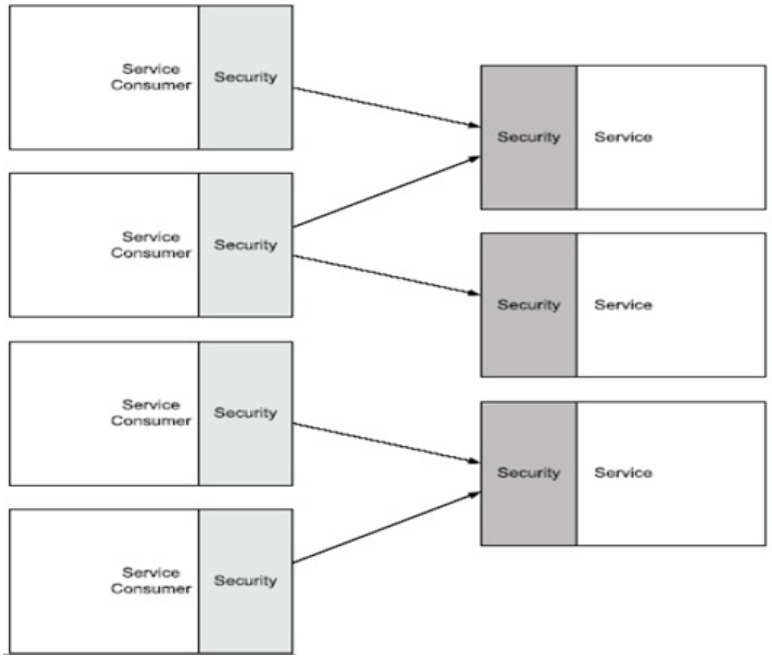

Fig. 6: implementation of the security logic as part of the service logic [Ram 08]

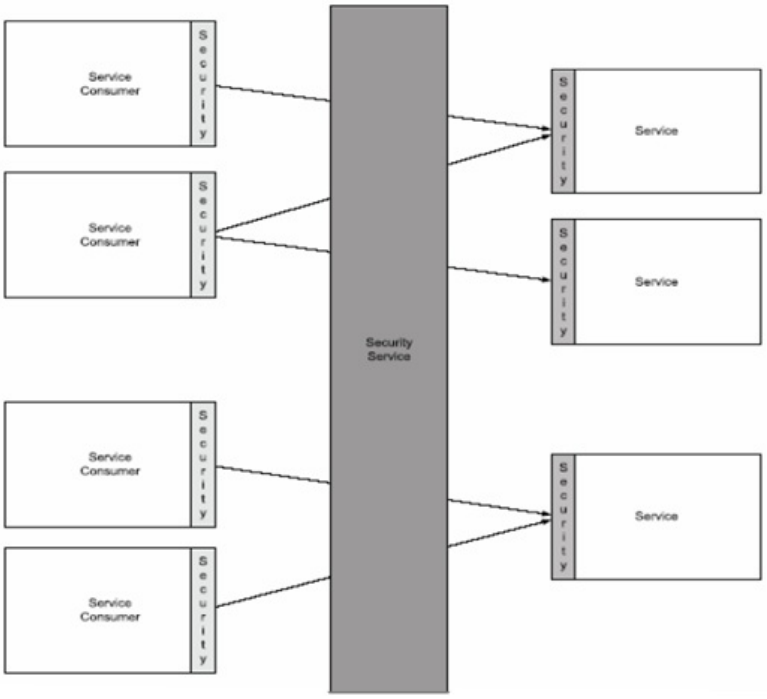

Fig. 7: implementation of the security logic as separate and independent service [Ram 08]

Task-related aspects of SOA

1. Credit validation (identity recognition)
2. Determination of authority
3. Protecting the secrecy of information
4. Maintaining the authenticity of data (keeping the data from being distorted)
5. Protection against attacks
6. Keeping users' information secret

Task-unrelated aspects of SOA:

1. Interaction capability
2. Management capability
3. Ease of development

The proposed security method for WSN through the use of SOA:

In this study, an attempt has been made to reduce to same extent the security shortcomings of wireless sensor networks through the use of the characteristics of service-oriented architecture (mostly in the security domain).

Since loose connections are used in SOA, there is slight dependence among components; and by taking advantage of this capability in wireless sensor networks, when one node is attacked the other nodes can continue their work. Moreover, by using SOA and the security as a service method, centralization in network security system becomes possible, as shown in the model in figure 8. A node is created next to the cluster head. This node, through interaction with the cluster head and the sensors, acts as an interface among the security sections of the cluster and the sensors and is of the cluster head type with a power source, a processor, etc.

The security node has capabilities including the following:

- Recognizes the identity of the sensors so that by using SOA and the security at message level method, the information related to one specific node is not usable by other nodes and is only used by the intended nod. Therefore, if an enemy penetrates a node, it cannot have access to infinite information and information accessible to it will be limited.
- Hides the information of other sensors so that this information is kept secret

- Sends messages in the text mode
- Reduces the volume of processed information in the sensor nodes; and because power is conserved, the life-time of the network is increased

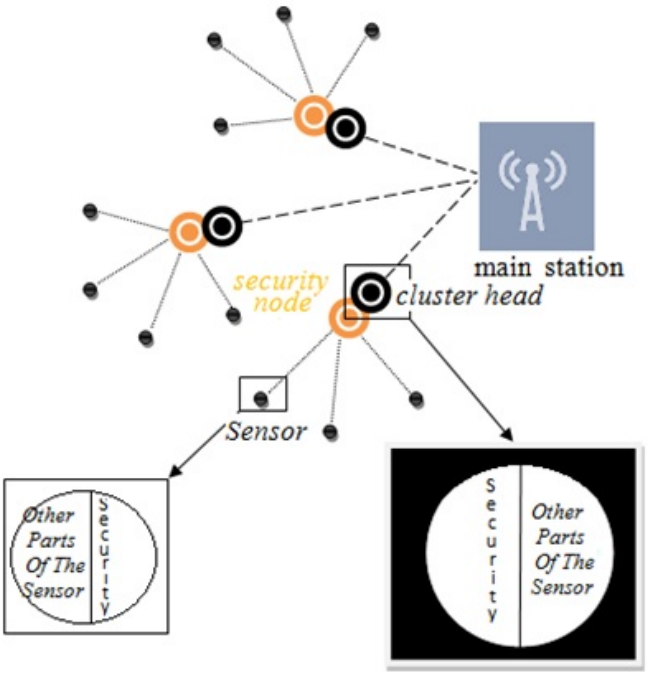

Fig. 8: the model presented for WSN security through the use of SOA

As can be seen in the model, this method does not cause the loss of the security of the sensors or other parts, and these parts carry on their duties as before.

Due to the interaction of the network with the Policy-oriented security method, the security logic is separated from the system logic; and this will cause improvement in the following capabilities:

1. Capability to interact
2. Capability to manage
3. Ease of extension

REFERENCES

Abdolhossein Alipure, M.sc. student at Islamic Azad University, Department of Science and Research, and Mehdi Fesharaki, Assocate Professor at Malek Ashtar Polytechnic", Ontology of Services Required for Mixing Sensor Information in Monitoring the Environment".

Ali Movaghghar Rahimabadi, professor of the Faculty of computer Engineering, Sanati-shareef University, and Mohmmad Ebrahim Shiri Ahmadabadi, Assocate Professor, computer Science Department, Amirkabir Polytechnic, and Farzad Hemmati, Faculty of Computer Engineering, Islamic Azad University of Arak, "A management Schema Using Improved Keys for Large Wireless sensor Networks in Hostile Environments".

Alireza Hedayati, Ph.D. Student, Computer Engineering. Islamic Azad University, Department of Science and Research, and Mehdi Naghian Fesharaki, Assocate Professor. Mallek Ashtar Polytechnic, University Complex of Information Technology, Communications, and security. "Introduction of an Apocalyptic Model of Wideband Management for Communications Infrastructure of Network-Oriented War Based on Next Generation Networks".

Amir Reza Mahjourian, 2007. "Formulating the Methodology of Programming Service-Oriented Organization Architecure for the Purpose of Cmplete Coverage of the Zackmann Framwork", M.sc. thesis in computer Engineering, Software Major, Faculty of Electricity and computer Engineering. Shahid Beheshti University.

Amir Reza Mahjourian, Software Expert, M.sc., and Freidoun Shams, Faculty Member of the Electrical and Computer Engineering Department, Shahid Beheshti Univercity, "Application of Service-Oriented Architecture in the layers of Electronic-City Architecture".

Emad Dara, 2009. "Service-oriented Architecture: Study of Point of View Concerning ITs security", M.sc. seminar Report, the Computer and Mechatronics section, Islamic Azad University of Tehran, Department of Science and Research.

Neda Anaami, Payame Nour University of Tehran Student, and Kourosh Dadashtabar Ahmadi, Tarbiat Modarres University student, "Querry Processing Architecture in Wireless sensor Network".

Pouya Laalbakhsh and Nasrin Sohrabi, Students at Islamic Azad University of Boroujerd, and Mehdi Tadhiian Fesharai, Malek Ashtar Polytechnic University, Tehran", Exploiting the capabilityes of Service-Oriented Architecture in Generating Awareness at the Scence of Battle."

Sedigheh khoshnevis, 2000. "introduction of a method to formulate service-oriented organizational architecture though the use of model-driver organizational architecture through the use of model-driver architectural framework", M.sc. thesis, software computer Engineering, Islamic Azad University, Department of Science and Research

Sedigheh khoshnevis, 2006. "Study of Service Oriented Enterprise Architecture (SOEA)", M.sc. seminar Report, Computer Engineering Section, Islamic Azad University, Department of Science and Research.

Shahaboddin Shamshirband, Samira Kalantari, Zeinab Bakhshandeh, "Wireless Sensor Network Based on Fuzzy Logic Used in Gas-Pipe Gates".

Tarihi, Ali, 2007. "Study of the feasibility of using SOA (service oriented Architecture), point of view in the framework of MDA (Model Driver Architecture)", M.sc. seminar Report, by software Major students, the computer Department, Shahid Beheshti university.