British Journal of Mathematics & Computer Science
16(6): 1-12, 2016, Article no.BJMCS.25839
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Integrating a Secured Access Control Policy on Wireless Sensor Networks

S. O. Olatunji[1*], B. K. Alese[1], O. S. Egwuche[1] and K. M. Adesiji[1]

[1]Department of Computer Science, Federal University of Technology, Akure, Nigeria.

Authors' contributions

This work was carried out in collaboration between all authors. Author BKA designed the study, wrote the protocol and supervised the work. Authors SOO and OSE carried out all laboratories work and performed the statistical analysis. Author KMA managed the analyses of the study. Author SOO wrote the first draft of the manuscript. Author OSE managed the literature searches and edited the manuscript. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJMCS/2016/25839
Editor(s):
(1) Dariusz Jacek Jakóbczak, Chair of Computer Science and Management in this Department, Technical University of Koszalin, Poland.
Reviewers:
(1) Sherin Zafar, Jamia Hamdard University, New Delhi, India.
(2) Carolina Del Valle Soto, Universidad Panamericana, Campus Guadalajara, Mexico.
(3) Anonymous, University of Maribor, Slovenia.
Complete Peer review History: http://sciencedomain.org/review-history/14681

Review Article

Received: 22nd March 2016
Accepted: 10th May 2016
Published: 18th May 2016

Abstract

A new generation of high-scale sensor networks suitable for a range of enterprise application is thriving by current advancements in electronics. In this work, we proposed a mechanism for securing data generation in a wireless sensor network. Wireless sensor networks (WSNs) are networks that provide a virtual layer where the information about the physical world can be accessed by any computational system. WSNs are made up of nodes from a few to several hundreds or even thousands where each node is connected to one or several sensors. The data generated can be easily compromised by an attacker if adequate security measures are not taken. Access and Authorization to the sensory data should be given to authorized users with the right attributes if data integrity and authentication (in a fine-grained manner) should be maintained. The increased security of the proposed system is achieved by the increased in the key size above the existing system. Achieving secure fine-grained access control policy over security challenges like sensor node compromise, accessibility of users to sensor nodes, data privacy, and protection of components on WSNs need a secure system that can precisely specify what the users can access, where and when to access any data at a particular time in the network.

**Corresponding author: E-mail: solatunji@futa.edu.ng;*

Keywords: Wireless Sensor Networks (WSNs); access control; fine-grained; security.

1 Introduction

Effective and efficient design and implementation of wireless sensor networks has attracted the attention of researchers in recent years because of the large potentials of sensor networks to enable applications that connect the physical world to the virtual world. By networking large number of tiny sensor nodes, it is possible to obtain data about the physical occurrences that was difficult or impossible to obtain in the conventional ways. WSNs consist of a large number of sensor nodes that can be easily deployed to various territories of interest to sense the physical environment, process or transmit the sensed data. The potential applications for large-scale wireless sensor networks exist in wide range of fields, including military domains, health sector, weather forecast, surveillance, home security and industrial monitoring [1-4].

The challenges in the hierarchy of detecting the relevant quantities, monitoring and collecting the data, accessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are numerous. The information needed by smart environments is provided by distributed wireless sensor network, which are responsible for sensing as well as for first stages of the processing hierarchy [5].

The basic components of a node are a sensor unit, an ADC (Analog to Digital converter), a CPU (Central Processing Unit), a power units and a communication unit. Sensor nodes are micro-electro-mechanical system [6] (MEMS) that produce a measurable response to a change in some physical condition like temperature and pressure.

There is not only ADC as basic components of a node. Nowadays, there are new high accuracy measurement methods and sensors which are much faster than ADC, such as: AT-cut quart crystal sensing devices and Temperature-Compensated Capacitance-Frequency Converter wit High Resolution [7,8] Sensor nodes sense or measure physical data of the area to be monitored. The continual analog signal sensed by the sensor is digitalized by an analog-to-digital converter and sent to controller for further processing. Sensor nodes are very small in size, consume extremely low energy. Each sensor node has a certain area of coverage for which it can reliably and accurately report the particular quantity that it is observing [9]. The attractive features of the wireless sensor networks attracted many researchers to work on various issues related to this type of networks. However, while the routing strategies and wireless sensor network modelling are getting much preference, the security issues are yet to receive extensive focus.

There are not only large number of sensor device, as well as complete devices such as humidity chamber which is remote controlled and is constructed for sending and getting information, and where the security strategies are very important [10].

The remainder of the paper is organized as follows. In section 2, we give a background into security in wireless sensor networks and its implications, looked into the existing works of other authors so as to be guided well in our own analysis and design. In section 3, an overview of the proposed system is presented. While section 4 highlights the presentation and the discussion of the results.

2 Review of Related Works

Security is sometimes viewed as a standalone component of a system's architecture, where a separate module provides security. This separation is however a defective approach to network security. To achieve a secure system, security must be integrated into every component of the system designed because without security, the system can become a point of attack.

In WSNs, there are many attacks that can halt the services, such as confidentiality, availability, integrity, and authenticity e. These security services can be protected in WSNs by using security mechanisms which are

essential to provide the required security attributes in WSNs. An access control mechanism is regarded as one of the security mechanisms to prevent authorized users in WSNs where different users may have different privilege to access database on their role [11-13].

The nature of communication in WSNs makes it vulnerable to various attach for lacks of infrastructure and uncontrolled environment. Such attacks can be passive or active attack. The monitoring and listening to communication channels by unauthorized and malicious users are regarded as passive attacks. Sensor nodes can sense and collect data from the environments in WSNs: as a result, the networks become vulnerable to potential abuse of these data resources [14].

In active attack, adversaries can monitor, listen and modify data streams in communication channels in the sensor nodes. They can use wireless devices which are vulnerable to many attacks, because of the nature of the communication links that are unprotected in the environment. Therefore, it becomes imperative to analyze what need to be protected against which threats and how these attacks can be detected and prevented. The security aims of WSNs are the same as other network technologies [15].

Most of the access control models in WSNs are to provide data privacy and data confidentiality in the network. The privacy of users and sensor nodes has received less attention in most reviewed literature. The major aim of most users in user privacy is to hide their ID and other information relevant to them so that no user in the network would know their ID, except the trusted authority and the users himself. The PRICCESS model is related to RBAC and it was form by [9] and presented under users' privacy-preserving access control because its provide privacy for users in WSNs.

Distributed privacy-preserving access control (DP2AC) was proposed by [16] where the owner of the sensor network generates the token using a blind signature. Users need to buy tokens from the network owner before entering the sensor network. The tokens can be verified by any sensor node in the network, but no one can tell the identity of the token holder, including the network owner. There is no relationship between user identities and tokens, so privacy preservation for users is achieved. Once the token is validated by a sensor node, it provides the user with a certain amount of requested data, which is equivalent to the denomination of the token. The main objective of the proposed DP2AC model is that the network owner can prevent unauthorized access to sensed data, while users can protect their data access privacy.

However, a recent study [17] pointed out that DP2AC is not fine-grained access control, because each anonymous user has the same access privileges. Furthermore, the network user cannot sign query command, because of the blind signature. As a result, the adversary can easily intercept the tokens and impersonate authorized users to access data at the sensor nodes. The disadvantage of using tokens in a WSN is that the sensor nodes need more storage for the token detection mechanism. All of the used tokens have to be recorded and stored in the sensor nodes to prevent the tokens being reused by malicious and unauthorized users [18].

Shah and Rabacy [9] proposed the PRICCESS protocol for WSNs. The main contribution to the research community of this protocol is that it provides user privacy-preserving distributed access control in a single-owner multi-user sensor network. A ring signature is used to protect the anonymity of users by using a group ID and group signature. Each group of users has different access privileges, IDs and keys for signature. Users have to activate their information with a network controller to receive the group ID and keys for data access. Users with the same access privileges are likely to be put in the same group by the network controller. The major disadvantage of using ring signature is that the overhead of signature becomes large when there is a large number of user groups in the network and the classification of users were not well explanatory i.e. users cannot be classified based on their access privilege [7].

Bell and Lapadula [19] security model is a state machine model designed for capturing the confidential aspects of access control. It addresses security policy goal of preventing from unauthorized disclosure and delimitation of information and also prevents information flowing downwards from the higher security level

to a low security level, meaning that data are assigned a security level and the mode of access granted depends on this level and level of the subject.

Del-Valle-Soto [20] proposed a security infrastructure for wireless sensor networks that is reactive to attacks. The model was tested under ordinary (without attacks) conditions (and combinations) and when it is subject to different types of jamming attacks (in particular, random and reactive jamming attacks), considering several positions for the jammer. There were no proactive components of the proposed model that could counter potential threats such as unauthorized users and every attempt to break into the system.

2.1 Attacks in wireless sensor networks

Wireless sensor networks are designed to gather information from the physical phenomenon. But in mission critical applications, there are high attempts by the unauthorized users to attack the central database. [21] summarized some of these attacks to include:

2.1.1 Denial of service (DoS)

Denial of Service (DoS) is produced by sudden and unintentional failure of nodes or malicious action. The simplest DoS attack attempts to exhaust the resources available to the attacked node, by sending excess unnecessary packets and thus prevent legitimate network users from accessing services or resources they are legally entitled to. DoS attack is meant not only for the adversary to halt the network, but also to prevent any event that diminishes a network's capability to provide a service.

2.1.2 Attacks on information in transit

In a sensor network, sensors monitor the changes of specific parameters in the target field and report the sensory data to the processing node according to the requirement. While sending the report, the transmitted information may be altered, spoofed, replay previously heard packets and many more. Sensor nodes typically have short range of transmission and scarce resource, an attacker with high processing power and larger communication range could attack several sensors at the same time to interrupt, intercept or modify the actual information during transmission to the sink node

2.1.3 Sybil attack

In many cases, the sensors in a wireless sensor network would need to collaborate together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can disguise to be more than one node using the identities of other legitimate nodes in the network. This type of attack where a node forges the identities of more than one node is called Sybil attack [22]. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to sybil attack. However, this attack can be prevented using some efficient protocols at the communication layer of WSNs.

2.1.4 Blackhole/Sinknode attack

In this attack, a malicious node presents itself as a black-hole to attract all the traffic in the sensor network. Basically, in a flooding based model, the attacker listens to requests for routes then replies to the target nodes that contains the high quality or shortest path to the sink node. Once the malicious node is able to insert itself between the communicating entities (that is, the sink and sensor nodes), it is able to do anything with the transmitting packets between them.

2.1.5 Hello flood attack

Hello Flood Attack was introduced in the work of [23]. This attack uses HELLO packets as a strategy to convince the nodes in WSN. In this type of attack, an attacker with a high radio transmission range and processing power sends HELLO message to a number of sensor nodes which are dispersed in a target region

within a WSN. The sensors tend to believe that the adversary is their neighbour. As a consequence, while sending the information to the sink node, the attacked nodes try to go through the attacker as they know that it is their neighbour and are ultimately spoofed by the attacker.

2.1.6 Wormhole attack

Wormhole attack is a critical attack in which the attacker records the packets at one location in the network and retransmits it to another location within the network. The tunnelling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because this type of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighbouring information.

3 System Model

WSNs architecture can be arranged or organized in two different forms: hierarchical and distributed form as show in Fig. 3.1.

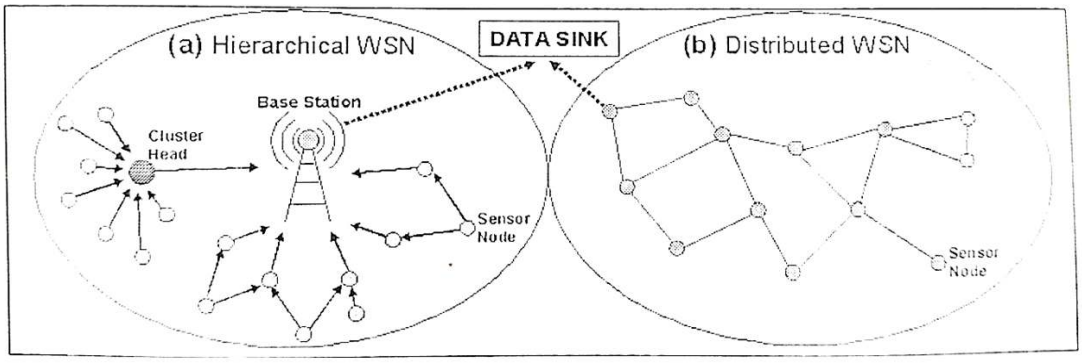

Fig. 3.1. Network architecture: Hierarchical and distributed WSNs

In hierarchical WSNs as shown in Fig. 3.1(a), there is hierarchy among the nodes based on their capacities, base stations, sensor nodes and cluster head-node with better resources which may be used to collect and merge local traffic and send it to Base Stations (BSs). Transmission power of a BS is usually enough to reach all sensor nodes, but sensor nodes depend on the ad hoc communication to reach base station (BS). Thus the data flow in such network can either be unicast, multicast and broadcast from the BS to the sensor nodes [1,23].

In Distributed WSNs, shown in Fig. 3.1(b), there is no fixed infrastructure, and network topology is not known prior to deployment. Sensor nodes are usually randomly scattered all over the target area or environment. Once they are deployed, each sensor node scans its radio coverage area to figure out its neighbors. The occurrence of data flow in distributed WSN is as it happens in hierarchical WSNs with a different that broadcast can be sent by every sensor nodes.

As a result of the increasing cases of the activities of unauthorized users like hackers and malicious user on enterprise networks, the security of information, data storage and data access is critical in developing any secure systems. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key.

The popular encryption method for data storage in WSNs is Attribute Based Encryption (ABE). ABE-based encryption as described by [24] is relative to other public key encryption methods because of its high promising approach to realize fine-grained access control in WSN. Data in the sensor nodes are encrypted

using attribute and keys from the trusted authorities. Access is given to user with the right access structure that matches the attributes and keys from the sensor nodes.

The ABE scheme consist of four major algorithms namely:

a. Setup algorithm: the system parameters are chosen by the key attribute authority and threshold is determine to produces the following public parameters:

$$T_1 = g^{t_1}, T_2 = g^{t_2}, \ldots, T_w, Y = e(g,g)^y \quad (1)$$

Where $(t_1, t_2, \ldots, t_w, y)$ are the master secret key, while $T_i \in G_1$ and $t_1 \in Z_q$.

G_1 and G_2 are cyclic groups, q is a prime power, T is sender and g_1, g_2, are the generator of the group G_1 and G_2 respectively.

b. Key Generation Algorithm: The server generates secret keys for the users, depending on the set of attributes it has and the group it belongs. It takes groups $\boldsymbol{G_1}$and$\boldsymbol{G_2}$, the threshold parameter d, the set of attributes that a user has as input and outputs the secret keys.

$$SK = (\boldsymbol{SK_1}, \boldsymbol{SK_2}, \ldots, SK_{n-1}) \quad (2)$$

c. Encryption Algorithm: The server generates public keys and encrypts the message using its public keys.

$$\boldsymbol{C'} = (\boldsymbol{B_n}, C = \boldsymbol{MY^{\rho}}, \{\boldsymbol{E_i}=\boldsymbol{T_i^{\rho}}\}\ i \in \boldsymbol{B_n}) \quad (3)$$

While C' is an output ciphertext, C is an input ciphertext, B_n is a set of attributes it has, M is a message and E is the stage during the implementation.

d. Decryption Algorithm: This algorithm enables a user with valid set of attributes to decrypt the message. The decryption process is performed at each node. It takes as input the ciphertext C, the group $\boldsymbol{G_1}$ and the parameters that a receiving user has and outputs the message M.

3.1 Access control policies

Access control is also concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access resources in the system or network. A given Information Technology (IT) infrastructure can implement access control systems in many places and at different level. Operating system uses access control to protect the resources of a computer system likewise database management systems apply access control to regulate access to tables and fields in the database. This restriction can either be informed of physical access control, mechanical access control or electronics access control [2,3].

Access control policies may be application-specific which are taken into consideration by the application vendor. Policies may pertain to resources usage within or across organization units or may be based on the need-to-know competence, authority, obligation, or conflict-of-interest factors. Although, there are many well-known access control policies such as fine-grained access control policy and coarse grained-access control policy. In fine-grained access control, policies are applied to network, information system or all authorized users in order to access a particular data on the network. It is also a kind of mechanism for deploying transparent security policies on a network or a strategy that state what type of data users can access with their various security levels. However, when using fine-grained access control, it creates security policy functions that are attached to the network based on the application which ensure that, the right statement implement the correct access control and also ensure that the same security is enforced no matter how a user accesses the data [25].

Access control mechanism requires that security attributes be kept about users and resources. Resources attribute can take a wide variety of form such as resources that carry sensitivity label, types, on access control lists. In determining the user's ability to perform operations on resources, access control mechanisms compare the user's security attributes to those of the resources. In achieving more secure fine-grained access control, the security label of the users must be greater than or equal to the security level of the resources for the user to read the content of the resources because the application will be compromised if the access control is not properly enforced.

For example, having four classes of subjects where users are grouped according to ranks in military order as shown below:

$$\boldsymbol{S_1} = \{ \boldsymbol{S_G}, \boldsymbol{S_{LG}}, \boldsymbol{S_{Mjg}}, \boldsymbol{S_{Brg}} \} \tag{4}$$

$$\boldsymbol{S_2} = \{\boldsymbol{S_{col}}, \boldsymbol{S_{Lcol}}, \boldsymbol{S_{Lmaj}}, \boldsymbol{S_{cpt}}, \boldsymbol{S_{Liut}}, \} \tag{5}$$

$$\boldsymbol{S_3} = \{ \boldsymbol{S_{2ndlieut}}, \boldsymbol{S_{mwo}}, \boldsymbol{S_{wof}}, \boldsymbol{S_{ssgt}}, \boldsymbol{S_{sgt}}, \} \tag{6}$$

$$\boldsymbol{S_4} = \{\boldsymbol{S_{rof}}, \boldsymbol{S_{lcorp}}, \boldsymbol{S_{corp}}\} \tag{7}$$

The subjects categories can be grouped together to form a general class given as: S= $\{\boldsymbol{S_1}, \boldsymbol{S_2}, \boldsymbol{S_3}, \boldsymbol{S_4}, \}$ in which $\boldsymbol{S_1} > \boldsymbol{S_2}, > \boldsymbol{S_3}, > \boldsymbol{S_4}$. This shows that group S_1 is the highest ranking in the classes of subjects, follows by $\boldsymbol{S_2}$ down to the least.

The objects are the encrypted information or data pre-deployed to all the nodes which are categorized as O= $\{\boldsymbol{O_{ts}}, \boldsymbol{O_s}, \boldsymbol{O_c}, \boldsymbol{O_{uc}}, \}$ where O stands for the object and the subscripts are the security classification level ranging from top secret to the least. That is, Top secret (ts), Secret (s), Confidential (c) and Unclassified (uc).

The access policies are formed from the subject and the object class. Let O be a Universal set and L_1 to L_4 be the level at which each subject can operate in the network, that is;

$$\boldsymbol{O_{L1}} = \{\boldsymbol{O_{ts}}, \boldsymbol{O_s}, \mathbf{O_c}, \mathbf{O_{uc}}, \} \tag{8}$$

$$O_{L2} = \{\mathbf{O_s}, \mathbf{O_c}, \mathbf{O_{uc}}, \} \tag{9}$$

$$O_{L3} = \{\mathbf{O_c}, O_{uc}\} \tag{10}$$

$$O_{L4} = \{O_{uc}\} \tag{11}$$

In view of these, $S_1 \rightarrow O_{L1}, S_2 \rightarrow O_{L2}, S_3 \rightarrow O_{L3}, S_4 \rightarrow O_{L4}$, this means that for a subject to be able to encrypt an object, the subject must belong to the group list that had registered with the network administrator based on its attributes

Let S_n denotes all subjects classes where ($n \in \{1, \dots, 4\}$) and O_y denotes all the object classes O_y where ($y \in \{ts, s, c, uc\}$). Assuming there is a direct mapping between the member of n and y, this implies that every member of n takes a corresponding value of y. So,

S_n combined with O_y to give the following occurrences:

S_n: $O_y \rightarrow S_1 O_{L1}$
S_n: $O_y \rightarrow S_2 O_{L2}$
S_n: $O_y \rightarrow S_3 O_{L3}$
S_n: $O_y \rightarrow S_4 O_{L4}$

Therefore, $A = \{^{1 \text{ iff } S \subset S_n O_y \in \{1ts,2s,3c,4uc\}}_{0 \text{ Iff } S \not\subset S_n \ O_y}$ (12)

Where A is an access

S =subject
S_n = subject Class
O_y = Objects class

4 Results and Discussion

The proposed model was implemented and simulated in Java programming language. The Java Virtual Machine was used for the creation of the virtual nodes of the wireless networks. The security analysis of the system was carried out based on some of the standard security services that are implemented in any security oriented-settings. Table 4.1 show the execution summary of our system where the data size and the response time vary irrespective of the key size. For example, when the data size of a parameter node is 5, it consumed a response time of 0.5 seconds. Here, we considered the execution time for establishing secure channels between the network users and senor nodes. The execution time measures the time duration for each operation.

4.1 Security analysis

Some of the basic security services evaluated are;

I. User Authentication: user authentication needs to be enforced for sensor data in WSNs so that the sensory information would not be accessed by unauthorized entities. Therefore, the network owner enforces strict access control on the Data.
Through the registration procedure, administrator and network users are given the interface to sign up. That is to create an account before access can be granted to the information in the system. If sign up is successful, then the user is directed to the home page for completion of profile. The information supplied at this stage is encrypted in such a way that it cannot be edited. This ensures adequate security of the information supplied by the users to the administrator. The confidentiality of the information supplied is guaranteed.

II. Access Control: The design provides a strategy that specified the capability of different kinds of users to access the sensor data with different types of security level. The master key of the key sequence in each stage is encrypted under a certain set of attributes. Without the master key, the adversary is not able to derive the data encryption keys due to the one-wayness of the key chain, which is guarantee by attribute based encryption. Therefore, the scheme is able to control the accessibility of sensor data to only authorized users.

III. Integrity Protection of Query Command: The adversary may try to modify the query command constructed by a user, and a secure access control method is put in place to support the integrity protection of the query command. On the system, the Attribute Based Encryption is implemented in the system with each private key associated with an access structure or policy that specifies which type of cyphertexts the key can decrypt. A user is able to decrypt a cyphertext if and only if the attributes associated with a cyphertext satisfy the key's access structure or policy.

IV. Node Compromise Tolerance: In this design, it shows that compromising a sensor node does not disclose the sensor data generated before the sensor was compromised. This is because only the public key of the network owner and the group access list pool are pre-loaded on every node. Therefore, even if an adversary compromises some nodes without the private key of a network user, the adversary cannot imitate any network user by compromising nodes meaning that, compromising one sensor node does not give the adversary the advantages to obtain data generated by other sensor nodes. This is easily achieved since each sensor encrypts data independently.

V. Limit of Access Privileges: this is achievable when the network owner is able to restrict each network user's activities by grouping users based on their access level. Based on this, each user has a limit at which they can access according to their access privilege. Base on this, users are grouped in range from least to highest in the order of military force.

VI. Revocation: user revocation simply means that the users' service subscription is expired, the user is compromised or the user changes to a different group intentionally. This provides a time limit for every user on the system, when the user's time expired, the system logouts automatically.

Encryption and decryption processes must take place before any network security operations can be considered successful. The work of [3] used execution time where the authors did not actually specify whether the execution time was taken during encryption or decryption processes. The study was based on the assumption that members in a group were chosen to generate the key, as the group increases, response time also increases, that is, the larger the group, the higher the response time which is not effective and efficient for any mission critical application or system. The major metrics considered in this work include the response time and the key sizes used on 64 bits operating system. Table 4.1 show the generated values based on our metrics for both the encryption and decryption processes.

Table 4.1 (a) Encryption process

Data (kb)	Response time (s)	Key sizes 160	192
5	0.5	160	192
12	0.8	160	192
15	0.10	160	192
20	0.12	160	192
25	0.16	160	192
30	0.20	160	192
34	0.24	160	192
38	0.30	160	192

(b) Decryption process

Data	Response time (s)	Key sizes 260	292
5	0.50	260	292
12	1.00	260	292
15	1.20	260	292
20	1.22	260	292
25	1.24	260	292
30	1.28	260	292
34	1.32	260	292
38	1.38	260	292

Figs. 4.2 and 4.3 show the graphical representation of the result. In Fig. 4.2, as the encrypted data increases, there is higher response time. However, in Fig. 4.3, there is increase in response time as the data increase but the stability of the system response time goes along with the data which make the system more secure, efficient and accurate.

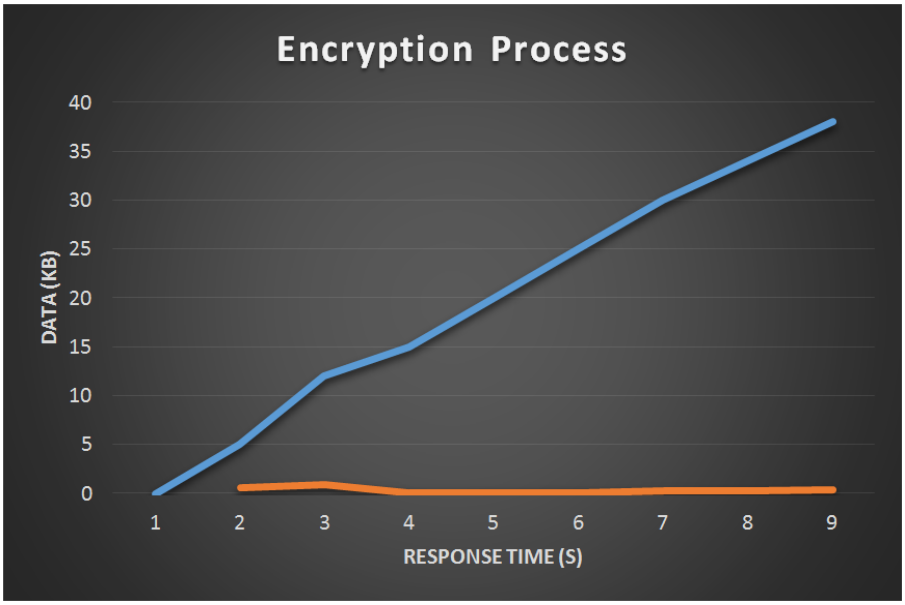

Fig. 4.2. Graphical representation of Table 4.1(a)

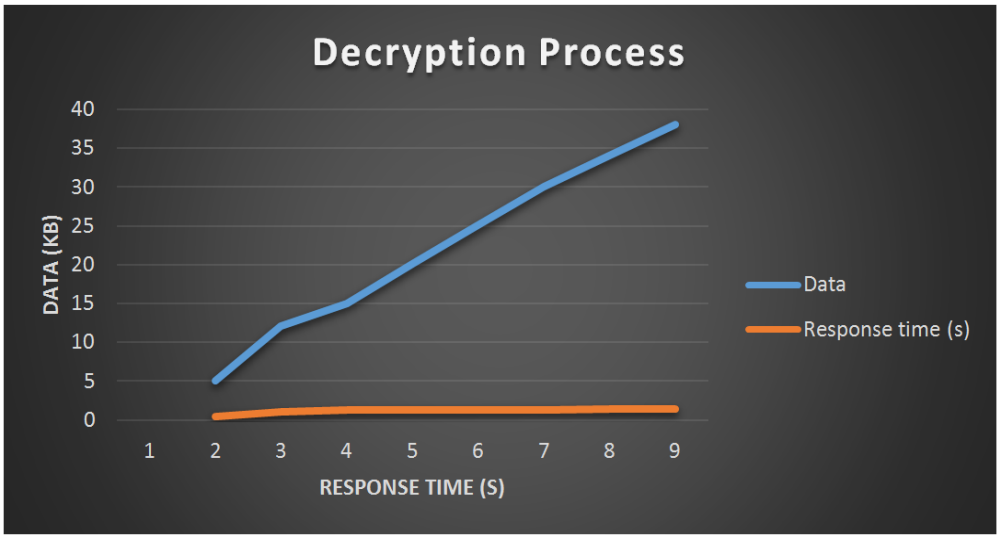

Fig. 4.3. Graphical representation of Table 4.1(b)

5 Conclusion

The study appraised some important issues on fine-grained access control, WSNs attacks, and various security models that enable network owners to achieve a secure access control on WSNs. The design of access control policies in any WSNs must satisfy the following: Confidentiality, integrity of the data, authorization, authentication, efficient, scalability and reliability. The adoption of PRICCESS protocol model enables us to achieved user privacy in the network, Bell and Lapadula model was also adapted to group both the users (subjects) and the objects. The combination of these models in the network provides a valid and a well secured access control on the network. High performance and security level of the proposed model was achieved by the increased in the key size above the existing model during the encryption and decryption processes. The security analysis and the requirements show that our approach is feasible for real-time systems

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Intelle S. Designing a home of future. IEEE Pervasive Computing. 2002;1:76-82.

[2] Mainwaring A, Polastre J, Szewezyk R, Culler D, Anderson J. WSNs for habitat monitoring. In proceedings of the ACM international workshop on WSNs and Applications (WSNA); 2002.

[3] Amtepe S, Yener B. Key Distribution mechanisms for wireless sensor networks: A survey. Technical Report TR-05-07 Rensselaer Polytechnic Institute, Computer Science Department; 2005.

[4] Lewis F. Wireless sensor networks. Automation and Robotic Research Institute. The University of Texas at Arlington: Ft. worthy Texas, USA. 2004;1-18.

[5] Younis M, Youssef M, Arisha K. Energy-aware routing in cluster-based sensor networks. In Proceedings of the 10th IEEE/ACM International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOT2002), Fort worth, Tx, USA; 2002.

[6] Akyildez I, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor network, a survey. Elsevier: Computer and Networks; 2002.

[7] Matko V, Milanović M. Temperature-compensated capacitance-frequency converter with high resolution. Sens. Actuators A. 2014;220:262-269.
Available:http://authors.elsevier.com/sd/article/S0924424714004178
DOI: 10.1016/j.sna.2014.09.022

[8] Matko V. Next generation. AT-cut quartz crystal sensing devices. Sensors. 2011;5(11):4474-4482.
DOI: 10.3390/s110504474

[9] Shah R, Rabacy J. Energy-aware routing for low energy ad hoc sensor networks. In Proceedings of the IEEE Wireless Communication and Networking Conference (WCNC), Orlando, FL, USA; 2002.

[10] Brezovec B, Matko V. Software and equipment for remote testing of sensors. Sensors. 2007;7(7):1306-1316.
Available:http://www.mdpi.org/sensors/papers/s7071306.pdf

[11] Alese BK. Vulnerability analysis of encryption/decryption techniques of computer network security. M.Tech. Thesis, Federal University of Technology, Akure Nigeria; 2000.

[12] Olatunji SO. Design and implementation of fine-grained access control system on wireless sensor network. M. tech Thesis, Federal University of Technology, Akure, Nigeria; 2015.

[13] Alese BK, Olatunji SO, Agbonofo OC, Thomson AF. A fine-grained data access control system in WSNs. Acta Informatica Pragensia. 2015;4(3):276–287.
DOI: 10.18267/j.aip.74

[14] Sen J. A survey on WSN security. International Journals of Communication Network. 2009;55-78.

[15] Daojing H, Jiaju B, Sencun Z, Sammy C, Chun C. Distributed access control with privacy support in wireless sensor networks. IEEE Transactions on Wireless Communications. 2011;3472-3481.

[16] Zhang R, Zhang Y, Ren K. Distributed privacy-preserving access control in sensor networks. In proceedings of the 28th IEEE International Conference on Computer Communications Joint Conference of the IEEE Computer & Communication Societies (INFOCOM 2009), Rio de Janeiro, Brazil. 2009; 1251-1259.

[17] Li M, Wenjing L, Ren K. Data security and privacy in wireless body area networks. IEEE Wireless Communications. 2010;17(1):51-58.

[18] Bender A, Katz J, Morselli R. Ring signatures stronger definition and constructions without ramdom. Oracles J. Cryptol. 2008;114-138.

[19] Bell D, Lapadula L. Secure computer systems. Unified exposition and MULTICS interpretation. Mitre Corporation; 1969.

[20] Del-Valle-Soto C, Mex-Perera C, Monroy R, Nolazco-Flores J. On the routing protocol influence on the resilience of wireless sensor networks to jamming attacks. Sensors Journal. 2015;15(4):7619-7649.

[21] Pathan AK, Lee H, Hong CS. Security in wireless sensor networks: Issues and challenges. International Conference on Advanced Communications Technology. 2006;1-6.

[22] Douceur JR. The sybil attack. 1st International Workshop on Peer-to-Peer Systems. Published by the Association for Computing Machinery; 2002.

[23] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols. 2003;293-315.

[24] Sahai, Water B. Cyphertext-policy attribute-based encryption. In IEEE Symposium on Security and Privacy. 2004;321-334.

[25] Arup N. Fine grained access control. International Oracle users Group Publication; 2003.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/14681