

A SECURED FINE-GRAINED ACCESS CONTROL POLICY ON WIRELESS SENSOR NETWORKS

ABSTRACT

A new generation of high-scale sensor networks suitable for a range of enterprise application is brought forth by current advancements in electronics. Wireless sensor networks (WSNs) is a such a network which 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.

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. (Intelle, 2002; Mainwaring et al, 2002; Amtepe et al, 2005; Lewis, 2004).

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 (Younis et al, 2002).

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 (Akyildez et al, 2002) (MEMS) that produce a measurable response to a change in some physical condition like temperature and pressure. 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

45 sensor node has a certain area of coverage for which it can reliably and accurately report the
 46 particular quantity that it is observing (Shah and Rabacy, 2002). The attractive features of the
 47 wireless sensor networks attracted many researchers to work on various issues related to this
 48 type of networks. However, while the routing strategies and wireless sensor network
 49 modelling are getting much preference, the security issues are yet to receive extensive focus
 50 Sensor node has limited sensing and computational capacities, communication performance
 51 and power. This large number of sensor devices are distributed over an area of interest for
 52 collection of information such as temperature, humidity, motion detection, and can
 53 communicate with each other for sending or getting information either directly or through
 54 other intermediate nodes and thus for a network, so each node in a sensor network acts as a
 55 router inside the network (Debnath and Kim, 2010; Ogundele, 2011). WSNs are dynamic in
 56 nature in the sense that radio range and network connectivity change with time. In some cases
 57 colluding nodes might have strong communications links available for coordinating
 58 prospective attacks (Kalita and Kar, 2009).

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

64 **2. REVIEW OF RELATED WORKS**

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

70 In WSNs, there are many attacks that can halt the services, such as confidentiality,
 71 availability, integrity, and authenticity e. These security services can be protected in WSNs
 72 by using security mechanisms which are essential to provide the required security attributes
 73 in WSNs. An access control mechanism is regarded as one of the security mechanisms to
 74 prevent authorized users in WSNs where different users may have different privilege to
 75 access database on their role (Alese, 2000; Olatunji, 2015; Alese et al 2015; Sen, 2009).

76 The nature of communication in WSNs makes it vulnerable to various attack for lacks of
 77 infrastructure and uncontrolled environment. Such attacks can be passive or active attack.
 78 The monitoring and listening to communication channels by unauthorized and malicious
 79 users are regarded as passive attacks. Sensor nodes can sense and collect data from the
 80 environments in WSNs: as a result, the networks become vulnerable to potential abuse of
 81 these data resources. (Wang et al, 2006).

82 In active attack, adversaries can monitor, listen and modify data streams in communication
 83 channels in the sensor nodes. They can use wireless devices which are vulnerable to many
 84 attacks, because of the nature of the communication links that are unprotected in the
 85 environment. Therefore, it becomes imperative to analyze what need to be protected against
 86 which threats and how these attacks can be detected and prevented. The security aims of
 87 WSNs are the same as other network technologies (Daojing et al, 2011).

88 Most of the access control models in WSNs are to provide data privacy and data
 89 confidentiality in the network. The privacy of users and sensor nodes has received less
 90 attention in most reviewed literature. The major aim of most users in user privacy is to hide
 91 their ID and other information relevant to them so that no user in the network would know
 92 their ID, except the trusted authority and the users himself. The PRICCESS model is related

to RBAC and it was form by (Daojing et al, 2011) 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 (Zhang et al, 2009) 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 (Li et al, 2010) 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 (Bender et al 2008).

(Daojing et al 2011) 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 (Bender et al, 2008)

Bell and Lapadula security model is a state machine model designed for capturing the confidential aspects of access control (Bell and Lapadula, 1969). 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.

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. (Pathan et al, 2006) summarized some of these attacks to include:

2.1.1 Denial of Service (DoS)

Denial of Service (DoS) (Wang et al, 2004) 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 (Douceu, 2002). 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 blackhole 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 Karlof and Wagner (2003). 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 Figure 3.1

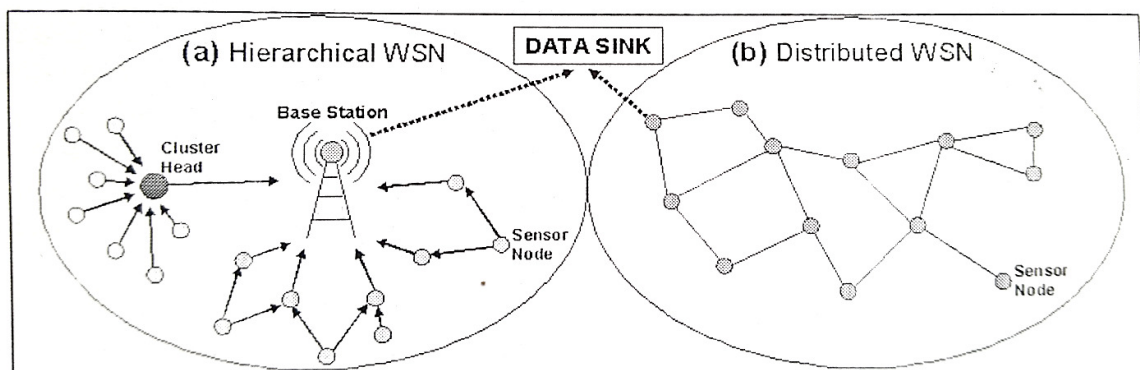


Figure 3.1 Network Architecture: Hierarchical and distributed WSNs

In hierarchical WSNs as shown in Figure 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 (Akyildez et al, 2002; Shah and Rabacy, 2002)

In Distributed WSNs, shown in Figure 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 ciphertext without using the key. The popular encryption method for data storage in WSNs is Attribute Based Encryption (ABE). ABE-based encryption as described by (Sahai and Water, 2004) 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:

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

Where $(t_1, t_2, \dots, t_w, y)$ 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 G_1 and G_2 , the threshold parameter d , the set of attributes that a user has as input and outputs the secret keys.

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

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

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

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 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 (Alese, 2000; Alese et al, 2015b)

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 (Wang et al, 2006; Arup, 2003).

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

268 content of the resources because the application will be compromised if the access control is
269 not properly enforced.

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

$$272 \quad 273 \quad S_1 = \{ S_G, S_{LG}, S_{Mjg}, S_{Brig} \} \quad (4)$$

$$274 \quad S_2 = \{ S_{col}, S_{Lcol}, S_{Lmaj}, S_{cpt}, S_{Liut}, \} \quad (5)$$

$$275 \quad S_3 = \{ S_{2ndlieut}, S_{mwo}, S_{wof}, S_{ssgt}, S_{sgt}, \} \quad (6)$$

$$276 \quad S_4 = \{ S_{rof}, S_{lcorp}, S_{corp} \} \quad (7)$$

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

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

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

$$286 \quad O_{L1} = \{ O_{ts}, O_s, O_c, O_{uc}, \} \quad (8)$$

$$287 \quad O_{L2} = \{ O_s, O_c, O_{uc}, \} \quad (9)$$

$$288 \quad O_{L3} = \{ O_c, O_{uc} \} \quad (10)$$

$$290 \quad O_{L4} = \{ O_{uc} \} \quad (11)$$

292 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
293 to be able to encrypt an object, the subject must belong to the group list that had registered
294 with the network administrator based on its attributes

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

298 S_n combined with O_y to give the following occurrences:

$$299 \quad S_n: O_y \rightarrow S_1 O_{L1}$$

$$300 \quad S_n: O_y \rightarrow S_2 O_{L2}$$

$$301 \quad S_n: O_y \rightarrow S_3 O_{L3}$$

$$302 \quad S_n: O_y \rightarrow S_4 O_{L4}$$

$$\text{Therefore, } A = \begin{cases} 1 & \text{iff } S \in S_n \text{ and } O_y \in \{1ts, 2s, 3c, 4uc\} \\ 0 & \text{iff } S \notin S_n \text{ or } O_y \end{cases}$$

(12)

Where A is an access

S =subject

S_n = subject Class

O_y = Objects class

309

310 4. RESULTS AND DISCUSSION

311 4.1 Security Analysis

312 Some of the basic security services evaluated are;

- 313 I. User Authentication: user authentication needs to be enforced for sensor data in
314 WSNs so that the sensory information would not be accessed by unauthorized entities.
315 Therefore, the network owner enforces strict access control on the Data.
316 Through the registration procedure, administrator and network users are given the
317 interface to sign up. That is to create an account before access can be granted to the
318 information in the system. If sign up is successful, then the user is directed to the
319 home page for completion of profile. The information supplied at this stage is
320 encrypted in such a way that it cannot be edited. This ensures adequate security of the
321 information supplied by the users to the administrator. The confidentiality of the
322 information supplied is guaranteed.
- 323 II. Access Control: The design provides a strategy that specified the capability of
324 different kinds of users to access the sensor data with different types of security level.
325 The master key of the key sequence in each stage is encrypted under a certain set of
326 attributes. Without the master key, the adversary is not able to derive the data
327 encryption keys due to the one-wayness of the key chain, which is guarantee by
328 attribute based encryption. Therefore, the scheme is able to control the accessibility of
329 sensor data to only authorized users.
- 330 III. Integrity Protection of Query Command: The adversary may try to modify the query
331 command constructed by a user, and a secure access control method is put in place to
332 support the integrity protection of the query command. On the system, the Attribute
333 Based Encryption is implemented in the system with each private key associated with
334 an access structure or policy that specifies which type of cyphertexts the key can
335 decrypt. A user is able to decrypt a cyphertext if and only if the attributes associated
336 with a cyphertext satisfy the key's access structure or policy.
- 337 IV. Node Compromise Tolerance: In this design, it shows that compromising a sensor
338 node does not disclose the sensor data generated before the sensor was compromised.
339 This is because only the public key of the network owner and the group access list
340 pool are pre-loaded on every node. Therefore, even if an adversary compromises
341 some nodes without the private key of a network user, the adversary cannot imitate
342 any network user by compromising nodes meaning that, compromising one sensor
343 node does not give the adversary the advantages to obtain data generated by other
344 sensor nodes. This is easily achieved since each sensor encrypts data independently.
- 345 V. Limit of Access Privileges: this is achievable when the network owner is able to
346 restrict each network user's activities by grouping users based on their access level.
347 Based on this, each user has a limit at which they can access according to their access

348 privilege. Base on this, users are grouped in range from least to highest in the order of
349 military force.

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

354 The work of (Alese et al, 2015) only specified execution time for query generation. They
355 only assumed that members in a group were chosen to generate the key, as the group
356 increases, response time also increases, that is, the larger the group, the higher the response
357 time which makes their work faster than existing work as claimed; compared to our work, we
358 realized that both the encryption and decryption process take place which are important in
359 any system or network security. We considered, data, the response time and key sizes as
360 major matrices used on 64bits operating system. The key sizes remain because comparison
361 has to be made between new system and old one. Below tables show both the encryption and
362 decryption process with the above matrices.

363 Table 4.1 (a) show encryption process (b) decryption process

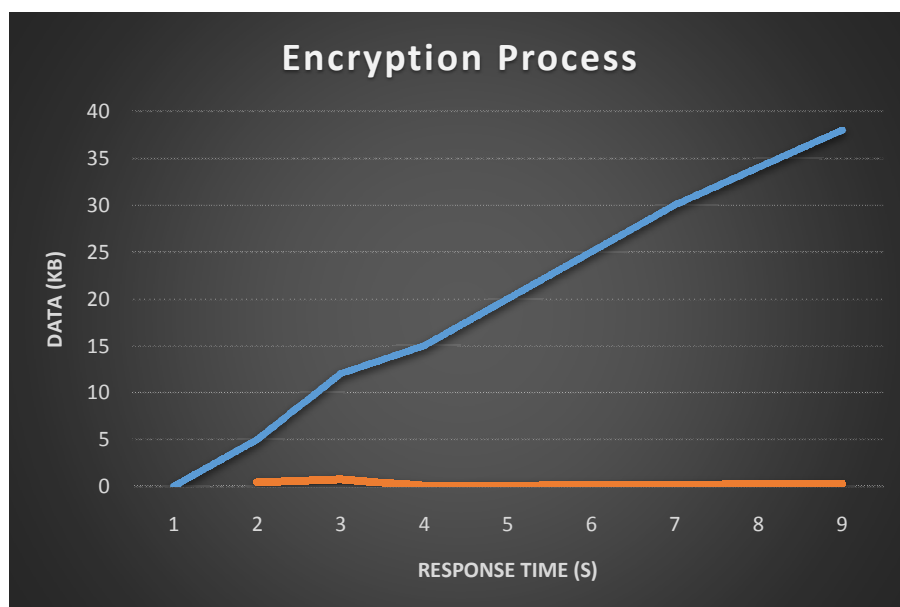
Data (kb)	Response time (s)	Key sizes	
		160	192
5	0.5	160	192
12	0.8	160	192
15	0.10	160	192
20	0.12	160	192
25	0.16	160	192
30	0.20	160	192
34	0.24	160	192
38	0.30	160	192

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

370 (a)

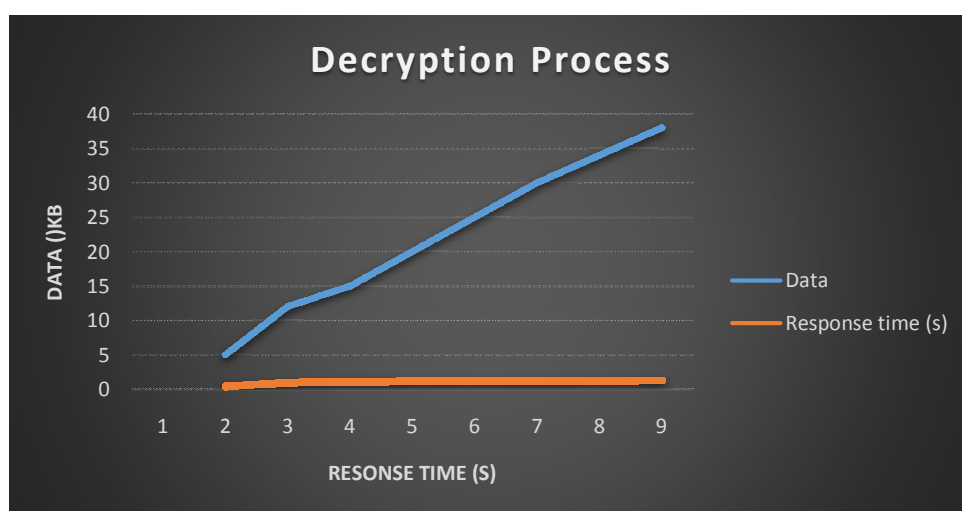
(b)

371 Figures 4.2 and 4.3 show the graphical representation of the result. In figure 4.2, as the data
372 encrypted increase, there is higher response time. However, in figure 4.3, there is increase in
373 response time as the Data increase but the stability of the system response time goes along
374 with the data which make the system more secure, efficient and accurate.



375

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



377

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

379 5. CONCLUSION

380 The study appraised some important issues on fine-grained access control, WSNs attacks, and
 381 various security models that enable network owners to achieve a secure access control on
 382 WSNs. The design of access control policies in any WSNs must satisfy the following:
 383 confidentiality, integrity of the data, authorization, authentication, efficient, scalability and
 384 reliability. Having reviewed the exiting related work, where PRICCESS protocol model was
 385 adopted, this enable us to achieved user privacy in the network, Bell and Lapadula model was
 386 also adapted to group both the users (subjects) and the objects. The combination of these
 387 models in the network provides a valid and a well secured access control on the network.
 388

References

1. Akyildiz I., Su W., Sankarasubramanian Y. and Cayirci E. (2002). Wireless sensor network, a survey. Elsevier: computer and networks.
2. Alese B. K. (2000). Vulnerability Analysis of Encryption/Decryption Techniques of Computer Network Security. M.Tech. Thesis, Federal University of Technology, Akure Nigeria.
3. Alese B.K, Olatunji S.O, Agbonofo O.C and Thomson A.F (2015). A Fine-Grained Data Access Control System in WSNs. *Acta Informatica Pragensia*, 2015, 4(3): 276–287 DOI: 10.18267/j.aip.74
4. Amtepe S. and Yener B. (2005). Key Distribution Mechanisms for Wireless Sensor Networks: a Survey, Technical Report TR-05-07 Rensselaer Polytechnic Institute, Computer Science Department.
5. Arup N. (2003). Fine Grained Access Control. International Oracle users group publication.
6. Bell D. and Lapadula L. (1969). Secure computer systems. Unified exposition and MULTICS interpretation, mitre corporation.
7. Bender A., Katz J. and Morselli R. (2008). Ring Signatures Stronger Definition and Constructions without Random. *Oracles J. Cryptol*, pp 114-138.
8. Daojing H., Jiaju B., Sencun Z., Sammy C. and Chun C. (2011). Distributed Access Control with Privacy Support in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications*. Pp 3472-3481
9. Debnath B., Kim T., Pal S. (2010). A Comparative Study of Wireless Sensor Network & their Routing Protocols. Department of Multimedia Engineering, Hannam university Daejeon Korea. *Open Access Sensor Network Journal* ISSN 1424-8221. Pp 506-523.
10. Douceur J. R. (2002). The Sybil Attack. 1st International Workshop on Peer-to-Peer Systems. Published by the Association for Computing Machinery.
11. Intel S. (2002). Designing a home of future. *IEEE Pervasive Computing* Vol 1: pp76-82
12. Kalita H. K. and Kar A. (2009). Wireless Sensor Network Security Analysis, *International Journal of Next-Generation Networks (IJNGN)*, Vol.1, No.1,
13. Karlof C. and Wagner D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's Ad Hoc Network Journal*, Special Issue on Sensor Network Applications and Protocols. Pp. 293-315.
14. Lewis F. (2004). Wireless Sensor Networks. Automation and Robotic Research Institute. The University of Texas at Arlington: Ft. worthy Texas, USA, pp 1-18
15. Li M., Wenjing L. And Ren K. (2010). Data Security and Privacy in Wireless Body Area Networks. *IEEE Wireless Communications*. Vol. 17, No. 1. Pp. 51-58.
16. Mainwaring A., Polastre J., Szewczyk R., Culler D., and Anderson J. (2002). WSNs for habitat monitoring. In proceedings of the ACM international workshop on WSNs and Applications (WSNA).
17. Ogundele S. (2011). Design of Multilevel Access Control Model for Delegation Based on Attributes Separation of Duty and Trust". M.Tech Thesis, Federal University of Technology, Nigeria.
18. Olatunji S. O. (2015). Design and Implementation of Fine-grained Access Control System on Wireless Sensor Network. M.tech Thesis, Federal University of Technology, Akure, Nigeria.

- 437 19. Pathan A. K., Lee H., Hong C. S., (2006); Security in Wireless Sensor Networks:
438 Issues and Challenges. International Conference on Advanced Communications
439 Technology. Pp 1-6.
- 440 20. Sahai & Water B. (2004). "Cyphertext-policy Attribute-based Encryption" in IEEE
441 Symposium on Security and Privacy. Pp. 321-334.
- 442 21. Sen J. (2009). A survey on WSN Security. International Journals of Communication
443 Network. Pp 55-78.
- 444 22. Shah R., Rabacy J. (2002). Energy-aware Routing for Low Energy Ad hoc Sensor
445 Networks. In Proceedings of the IEEE Wireless Communication and Networking
446 Conference (WCNC), Orlando, FL, USA, 2002.
- 447 23. Wang B. T. and Schulzrinne H. (2004). An IP Traceback Mechanism for Reflective
448 DoS Attacks. Canadian Conference on Electrical and Computer Engineering, Volume
449 2, 2-5. Pp. 901 – 904.
- 450 24. Wang Y., Attebury G., Ramamurthy B. (2006). A Survey of Security Issues in WSNs
451 IEEE Communication Survey and Tutorials. Vol. 8. No. 2. Pp 20-23.
- 452 25. Younis M., Youssef M., Arisha K. (2002). Energy-aware Routing in Cluster-based
453 Sensor Networks. In Proceedings of the 10th IEEE/ACM International Symposium on
454 Modelling, Analysis and Simulation of Computer and Telecommunication Systems
455 (MASCOT2002), Fort worth, Tx, USA.
- 456 26. Zhang R., Zhang Y., Ren K. (2009). Distributed Privacy-Preserving Access Control in
457 Sensor Networks. In proceedings of the 28th IEEE international conference on
458 computer communications joint conference of the IEEE computer & communication
459 societies (INFOCOM 2009), Rio de janeiro, Brazil. Pp 1251-1259.