J. Sens. Actuator Netw. **2014**, *3*, 150-180; doi:10.3390/jsan3020150

OPEN ACCESS

Journal of Sensor and Actuator Networks

ISSN 2224-2708

www.mdpi.com/journal/jsan

Article

A Survey of Access Control Models in Wireless Sensor Networks

Htoo Aung Maw *, Hannan Xiao, Bruce Christianson and James A. Malcolm

Department of Computer Science, University of Hertfordshire, Hatfield, AL10 9AB, UK;
E-Mails: h.xiao@herts.ac.uk (H.X.); b.christianson@herts.ac.uk (B.C.);
j.a.malcolm@herts.ac.uk (J.A.M.)

* Author to whom correspondence should be addressed; Email: h.maw@herts.ac.uk

Received: 23 January 2014; in revised form: 20 May 2014 / Accepted: 11 June 2014 / Published: 20 June 2014

Abstract: Wireless sensor networks (WSNs) have attracted considerable interest in the research community, because of their wide range of applications. However, due to the distributed nature of WSNs and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Resource constraints in sensor nodes mean that security mechanisms with a large overhead of computation and communication are impractical to use in WSNs; security in sensor networks is, therefore, a challenge. Access control is a critical security service that offers the appropriate access privileges to legitimate users and prevents illegitimate users from unauthorized access. However, access control has not received much attention in the context of WSNs. This paper provides an overview of security threats and attacks, outlines the security requirements and presents a state-of-the-art survey on access control models, including a comparison and evaluation based on their characteristics in WSNs. Potential challenging issues for access control schemes in WSNs are also discussed.

Keywords: wireless sensor networks; access control schemes; security mechanisms; security vulnerabilities

1. Introduction

A wireless sensor network (WSNs) consists of hundreds or even thousands of distributed, autonomous, low-power, low-cost, small-sized devices, each with sensing, processing and communication capabilities. Typically, these devices, known as sensor nodes, monitor the real-world environment and send the collected information to a gateway node through an infrastructure-less *ad hoc* wireless network. Sensor networks are envisioned to play an important role in a wide variety of areas, ranging from critical military surveillance applications to forest fire monitoring. WSN technology has been of interest to scientists in many research areas, because of its potential to change our way of living, with applications in entertainment, travel, retail, industry, medicine, health-care, traffic monitoring, military, emergency management, *etc*.

Among these applications, the military and medical applications are the most security-oriented fields of WSNs and have received the most attention from security researchers. WSNs are rapidly becoming an important technology in the medical or healthcare domain. Sensor nodes are becoming smaller and more powerful, making them suitable to use in a wide range of medical applications, such as health monitoring, chronic disease management and measuring user vital signs. Wireless medical sensor network (WMSN) is the name of this form of WSN used in the medical and healthcare domain. In WMSN, sensors are attached to the human body to monitor healthcare information, like electrocardiogram (ECG), blood pressure, *etc*. Medical staff can access, collect and record medical data directly from a patient's sensor for remote healthcare monitoring services. However Garcia-Morchon [1] mentioned that there are security and privacy concerns about possible access to user's medical data. Therefore, security services are required to provide the confidentiality of medical records and privacy of patient information. In addition, the control of access to patient's data becomes another issue in WMSN, because there might be a number of medical staff and family members, who try to interact with the confidential medical data.

WSNs can also be used for a number of purposes in the military sector, such as enemy tracking, military activities monitoring and battlefield surveillance. The rapid deployment, self-organization and fault tolerant characteristics of sensor networks make them a very promising data gathering technique for military Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) [2]. In military applications, the sensor nodes are used to collect the information of enemies and tracking military vehicles. The data sensed and stored at the sensor nodes are highly confidential, so security services, such as confidentiality, integrity, *etc.*, need to be provide by using security and access control mechanisms.

Nowadays, a sensor node can capture pictures and multi-media data. A sensor node has the capability of sensing data from the environment. It stores the sensed data locally in a distributed fashion or transmits the sensed data to central storage in a centralized approach. In both the centralized and distributed approach, data security and data access control are important issues in WSNs. As a large amount of data is stored in the sensor nodes locally, aspects of data security (such as confidentiality and integrity) have become serious concerns, because the sensor nodes are not well equipped with tamper-proof or tamper-evident equipment. From a data-centric point of view, the most challenging issues in WSNs are how to store the highly sensitive sensor data and how to control the access of internal and external users.

Based on the above discussion, access control is a critical security requirement to protect sensitive sensor information from unauthorized access, but it has not received attention in the context of WSNs by researchers. Data in real-time WSNs applications are made available to users on demand. Faye *et al.* [3] mentioned that the sensed data may no longer be accessed only at the base stations, and users can access data at the sensor node directly from anywhere in an *ad hoc* manner. Depending on user's access control privileges, data access to the sensor nodes will be different. In this report, we will survey and discuss the state-of-the-art for access control schemes in WSNs.

The remainder of this paper is organized as follows. Background information of security vulnerabilities and security requirements and the traditional access control models for information systems are discussed in Section 2. Section 3 reviews WSN access control models that are proposed as models in the literature. Section 4 compares the current access control models based on characteristics, such as network architecture, key management, *etc.* Section 5 evaluates these access control models qualitatively and quantitatively. Section 6 discusses the potential research issues of access control models in WSNs, and finally, Section 7 concludes the paper.

2. Background

In WSNs, there are several attacks that can break the security services, such as confidentiality, availability, integrity, authenticity, *etc.* These security services can be protected in WSNs by using security mechanisms. In this section, we discuss the security vulnerabilities and security requirements for WSNs. We then introduce the traditional access control models. Access control is one of the security mechanisms that needs to be provided in WSNs.

2.1. Security Vulnerabilities and Security Requirements

The nature of WSNs makes them vulnerable to various kinds of attack. Security attacks can be categorized as passive or active: malicious users could either intercept private information or send false messages to the sensor nodes in WSNs. The listening and monitoring of the communication channels by unauthorized and malicious users are regarded as passive attacks. Sensor nodes can sense and collect data from their environments in WSNs; as a result, the network becomes vulnerable to potential abuse of these data resources. Vella [4] mentioned that the data obtained by sensing nodes need to be kept private and confidential. Since the data are stored in the sensor nodes without tamper-proof or tamper-evident equipment, the privacy and confidentiality of data become important to protect from passive attacks, such as eavesdropping, passive monitoring and traffic analysis [5].

An active attack can monitor, listen and modify data streams in the communication channels, where an adversary can maliciously disturb the communication channels between the sensor nodes. In harmful active attacks, the adversary can alter and spoof the packets and interfere with the wireless signals to jam the network. Ng *et al.* [6] argued that even if the information is protected from eavesdropping by means of encryption, the attacker may blindly modify that encrypted information and turn the information into meaningless information. The common active attacks in WSNs include camouflage [7], Sybil [8], wormhole [9], replay, hello flood [10], sinkhole [5], denial of service (DoS) [11] and node replication [5].

Apart from the active and passive attacks, Perrig [12] suggested that there might be other types of attack, which are not yet identified in all layers of the TCP/IP protocol stack in WSNs. Securing WSNs against all of the attacks and threats is a challenging task. WSN is considered a highly distributed and *ad hoc* approach, and because of that, the security requirements and goals of WSNs should be well studied and provided. The aim of security is to protect the right thing in the right way. Gligor [13] pointed out that "A system without an adversary definition cannot be insecure. It can only be astonishing". WSNs are vulnerable to many attacks, because of the broadcast nature of the transmission links and the unprotected physical environment. Therefore, we need to analyze carefully which things need to be protected against which threats and how these attacks and threats can be detected and prevented. The security goals for WSNs are similar with other network technologies. Security properties, such as confidentiality, integrity, availability, access control, authorization, authentication, freshness and secure localization, need to be provided in WSNs.

In WSNs, there are two additional requirements which need to be investigated for the security of sensor networks because there may be situations like new sensor nodes are joined and deployed and old sensor nodes are failed to operate in the networks. Based on these requirements, Wang *et al.* [14] suggested that forward and backward secrecy need to be considered in WSNs. Forward secrecy means that an old sensor node should not be able to read any message after it leaves the sensor networks. Backward secrecy means that a new sensor node should not be able to read any previous message sent before it joined the sensor network.

Table 1. Security properties, security attacks and possible solutions in WSNs [6,9,15–17].

Security Properties	**Security Threats**	**Possible Solutions**
Confidentiality	Message Disclosure	Encryption, Access Control
Integrity	Message Modification	Digital Signature, Secure Hash Function
Availability	DoS (denial of service), Wormhole, Sinkhole, Hello Flood	Intrusion Detection, Pairwise Authentication
Access Control, Authorization	Unauthorized and Unauthenticated Access	Access Control, Key Distribution, Encryption
Authentication	Message Modification, Sybil, Replay and Spoofing Attack	Random Key Distribution, Digital Signature
Freshness	Replay and Spoofing attack	Time-stamp, One Way Secure Hash Function
Secure Localization	Node Capture and Note Replication Attack	Temper-proof and Temper-evident
Forward and Backward Secrecy	Message Disclosure	Key Distribution

Table 1 lists the security attacks and threats, which can violate the security properties, and the possible solutions to defend against them. Security mechanisms are essential to provide the required security properties in WSNs. An access control mechanism is one of them. Different users may have different privileges to access data based on their roles. An access control mechanism is one of the security mechanisms to prevent unauthorized usage in WSNs. Faye *et al.* [3] described how access control must be able to authorize and grant access privileges of users for data access in the sensor network and prevent unauthorized access from the malicious users. This paper only focuses on the access control models in WSNs, and the next sub-section will present the traditional access control models for information system.

2.2. Traditional Access Control Models

There are two original access control models in information systems, which are mandatory access control (MAC) [18] and discretionary access control (DAC) [19]. MAC manages access control levels by means of an administrator in the organization. It uses a hierarchical approach to control access to the objects, which represent system resources here. The administrator defines an access control policy that cannot be modified by the subjects. MAC is mostly used in the systems where priority is placed on confidentiality, such as in military applications. In a DAC model, the owner of an object controls access to that object. This means that he has power to create the permissions for data access. By default, subjects without this permission cannot access the objects. Subjects mean users here.

The concept of an access control matrix, which defines the relationships between subjects, objects and the actions that the subjects want to perform on the objects, was introduced by Butler Lampson [20]. The subjects' identities are placed in rows and the objects' identities in columns. Each action that a subject wants to perform on an object is placed in the intersection of the corresponding row and column. The size of the access control matrix is directly proportional to the number of subjects and to the number of objects. Samarati and Vimercati [21] suggested that there are three possible approaches to implement the access control matrix in electronic systems, named authorization table, access control list (ACL) and capabilities. Among these, ACL and capabilities are commonly used in access control schemes. The three ways of representing the access control matrix are explained as follows:

- **Authorization Table**

  A three-dimensional table, corresponding to subjects, actions and objects, respectively. Each entry in the table corresponds to an authorization.

- **Access Control List (ACL)**

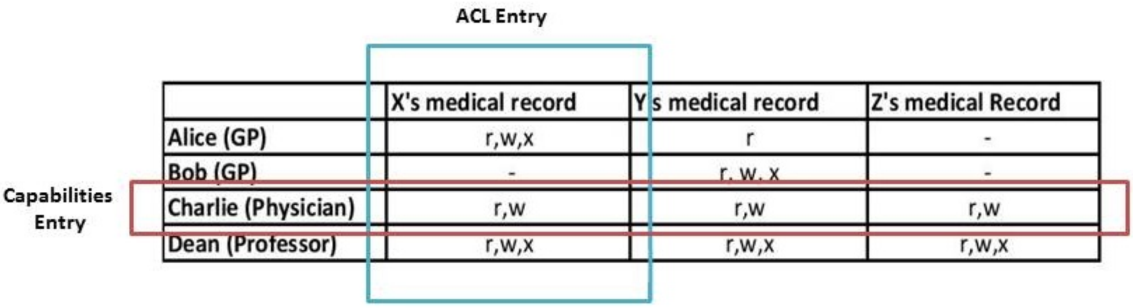
  Each ACL contains the list of subjects and their access permissions to a given object. When a subject tries to access an object, the ACL for that object is used to verify the request from the subject. If the subject access pair is in the ACL list, access will be granted. Otherwise, access will be denied. In the ACL approach, the lists of subject and action pair are stored for each object. An ACL is represented by a column in the matrix table as seen in Figure 1. In this figure, r, w and x stands for read, write and executable.

- **Capabilities**

  Capabilities are different from ACLs. Pairs of action and object are stored for each subject in the access control matrix. In a capability approach, the subject can get access to the object, when he presents the correct capability to the system. A subject's capabilities are represented by a row in the access control matrix.

The difference between ACLs and capabilities can be seen in Figure 1. One of the drawbacks of using an access control matrix is that when there are a large number of subjects and objects in the system, the administration of those subjects and objects becomes very difficult to handle. The role-based access control (RBAC) model [22] has been developed to model access control permissions in an organization in a more manageable way than the access control matrix does. The detailed description of RBAC and other different types of access control models in WSNs based on their architectural model, strength and weakness will be explained in the next section.

Figure 1. Difference between access control list (ACL) and capabilities.

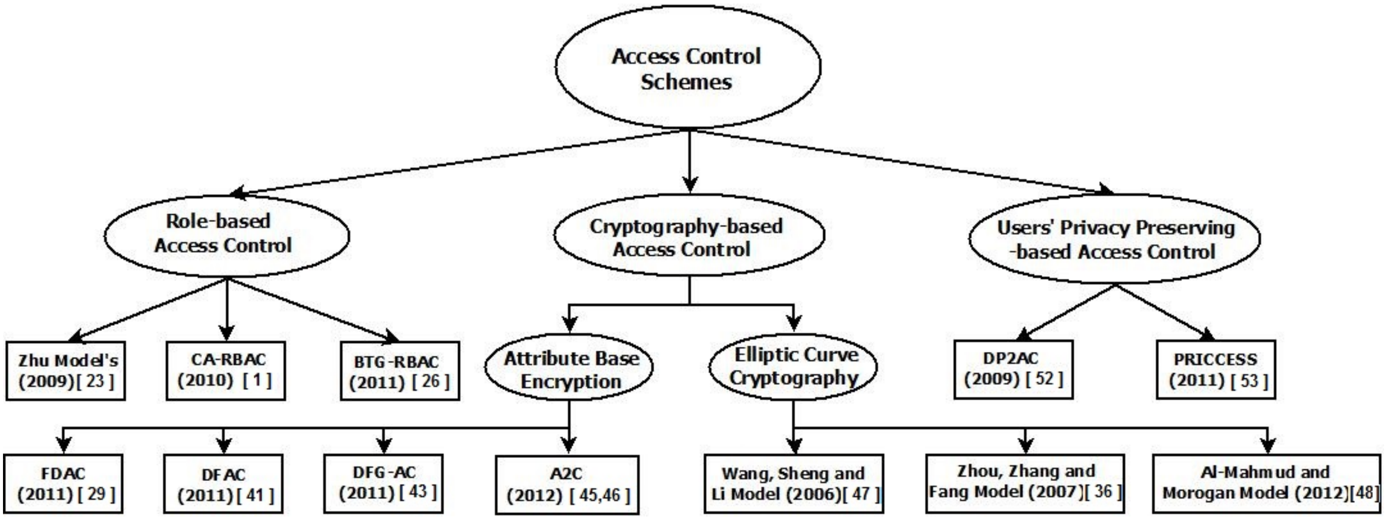

ACL Entry
Capabilities Entry

	X's medical record	Y's medical record	Z's medical Record
Alice (GP)	r,w,x	r	-
Bob (GP)	-	r, w, x	-
Charlie (Physician)	r,w	r,w	r,w
Dean (Professor)	r,w,x	r,w,x	r,w,x

3. Access Control Models in WSNs

A considerable number of access control models has been proposed for use in WSNs, though some of them are not yet implemented. In this section, we present the proposed access control models before we compare and contrast them in the next section. We group the proposed models into three main categories based on the nature of their architecture, namely: role-based access control (RBAC), cryptography-based access control (CBAC) and users' privacy preserving access control (UPPAC). A taxonomy of access control models for WSNs, including the publication year of each proposal, is shown in Figure 2.

Figure 2. A taxonomy of access control schemes in WSNs

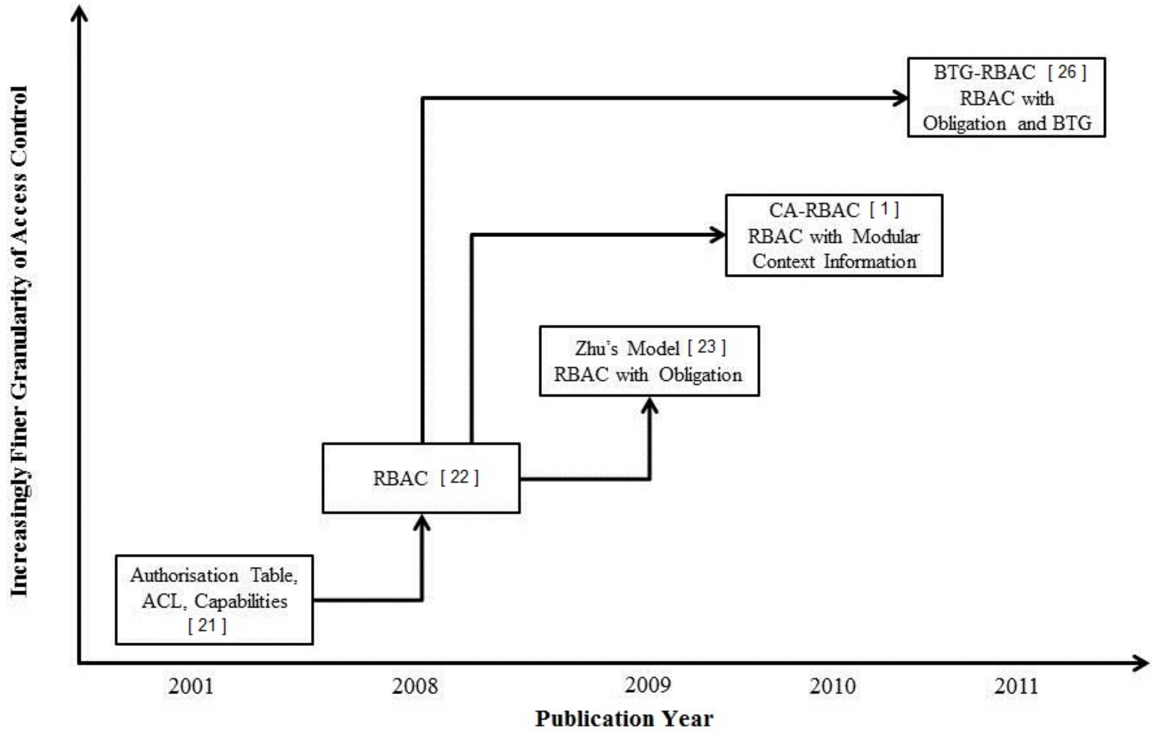

Access Control Schemes
Role-based Access Control
Cryptography-based Access Control
Users' Privacy Preserving -based Access Control
Zhu Model's (2009)[23]
CA-RBAC (2010) [1]
BTG-RBAC (2011) [26]
Attribute Base Encryption
Elliptic Curve Cryptography
DP2AC (2009) [52]
PRICCESS (2011) [53]
FDAC (2011) [29]
DFAC (2011) [41]
DFG-AC (2011) [43]
A2C (2012) [45,46]
Wang, Sheng and Li Model (2006)[47]
Zhou, Zhang and Fang Model (2007)[36]
Al-Mahmud and Morogan Model (2012)[48]

3.1. Role-Based Access Control (RBAC)

Most of the access control models in WSNs and WMSNs are based on traditional RBAC [22], which has been widely accepted as a policy-based access control model. Applications based on RBAC have been implemented and deployed in commercial companies and education industries. The principle of RBAC model is the role, defined as an intermediary concept relating a group of subjects to a set of access permissions. Any member from the subject group role has all of the permissions that are associated with that role. When a new subject is assigned to a group, he receives all of the associated access permissions, but these permissions are revoked when the subject leaves the group or is removed from the system. It is the same procedure to add and remove permissions from the roles. When a permission is added to a role, all of the members of the associated subject group will receive that permission. The permission will be revoked when it is deleted from the role. This feature helps to simplify system administration when there are many thousands of subjects and objects in an organization.

In RBAC, the access decision is a choice between two outcomes: permitted access or denied access. The following access control models are proposed based on the RBAC model with different extensions to provide further security properties in WSNs. Figure 3 shows how RBAC-based access control models have evolved in the WSN research community.

Figure 3. An evolution of role-based access control (RBAC)-based access control models in WSNs.


Increasingly Finer Granularity of Access Control
BTG-RBAC [26] RBAC with Obligation and BTG
CA-RBAC [1] RBAC with Modular Context Information
Zhu's Model [23] RBAC with Obligation
RBAC [22]
Authorisation Table, ACL, Capabilities [21]
2001
2008
2009
2010
2011
Publication Year

- **Zhu's Model** [2009]

  Zhu *et al.* [23] proposed a light-weight policy-based access control model, which used authorization and obligation policies to perform actions and make access decisions at the sensor nodes in a WMSN. The main idea of the proposed approach is to support sensor-level access control policy. A light-weight policy system, which is known as Fingers [24], enables policy enforcement and interpretation on the distributed sensors to provide fine-grained access control. Each sensor manages its own policies to implement both the policy decision point (PDP) and policy enforcement point (PEP). A PDP interprets policies and makes a policy decision, while a PEP enforces the policy by permitting and denying a subject from performing the requested actions. A controller (perhaps a PDA) uses a Diffie–Hellman (DH) key agreement to share keys with the sensor nodes. The sensor nodes can communicate between each other in a WMSN by using secret keys from the controller. An authentication process is used to prevent malicious nodes and users from joining the network. Only the sensor nodes that have keys from the same controller can communicate with each other. If a user has access to the network controller, he can request it to perform some actions at the sensor nodes. As an application, this approach can be used in WMSN to prevent unauthorized access to actuators, such as insulin or other drug pumps, that may harm the patients.

- **Context-Aware Role-Based Access Control (CA-RBAC)** [2010]

  Garci-Morchon and Wehrle [1] proposed the context-aware role-based access control (CA-RBAC) model based on a modular context structure for WMSNs. The aim of the model is to provide context awareness and adapt its security properties to ensure the users' safety in WMSNs. Wehrle *et al.* [25] pointed out that the RBAC model is not good enough to use in a WSN, because in traditional RBAC models, the roles and policies have to be predefined in advance. In the proposed model, the decision-making process is divided into three modular context situations: critical, emergency and normal condition. Based on these situations, the access privileges to sensed data will be different. The access control decision will be made based on context information, such as time, location, *etc*., and the access control policies of three different modules. In a WMSN, the sensor nodes are attached to the human body to sense and check medical information for a healthcare service. In the normal case, an authorized doctor needs to verify his access control role in order to access the medical data of a patient, but a nurse may not have the same level of privilege. When the system declares a critical or emergency case based on the modular context information, the doctor or nurse can perform any action and can access data, even though they may not be able to access that data in a normal condition. One of the disadvantages of this model is that there is no prevention or detection mechanism, as well as no verification process to check a user's data access, when the critical situation occurs.

- **Break-the-Glass Role-Based Access Control (BTG-RBAC)** [2011]

  Ferreria *et al.* [26] proposed the break-the-glass role-based access control (BTG-RBAC) model based on the RBAC model. The main idea of this model is to gather necessary information from the end users with their collaboration for a usable access control policy that can perform the BTG action in emergency situations. The break-the-glass (BTG) rule allows the users' to have emergency and urgent access to the system when a normal authentication does not perform or work properly. They introduced BTG rules in order to override access policy whilst providing non-repudiation mechanisms for its usage. In a real environment, unanticipated situations may occur because it is impossible to predict all of the access permissions in advance for all situations. The BTG extension is used for emergency and important cases whenever a user wants to access data urgently and immediately. When the user tries to perform BTG actions, the system will ask him if he really wants to perform that action on a specific object. If the user answers affirmatively, the system will activate the BTG operation and trigger the associated obligations, like alarms, log file, *etc.* The BTG-RBAC model made the system much more flexible than normal RBAC, but one of the disadvantages is that human processes are needed in order to enforce the BTG rules.

3.2. Cryptography-Based Access Control (CBAC)

Cryptography-based access control (CBAC) is another form of access control model for the information systems. Ghani *et al.* [27] mentioned that the CBAC mechanism is designed for untrusted environments, where a lack of global knowledge and control are defining characteristics. It absolutely relies on cryptography to control data access and to ensure data confidentiality and integrity. The main idea is to use a unique key for each data resource. Users who are allowed to access that data resource are assigned the key for data access [28]. Cryptography methods in WSNs should meet the constraints of sensor nodes, such as limited power, resources and memory shortage. Therefore, choosing a suitable cryptography method is important in WSNs. There are two types of cryptographic method; asymmetric encryption, known as public key cryptography (PKC), and symmetric encryption, known as symmetric key cryptography (SKC). The PKC-based scheme provides better data access security than SKC in the open multi-user environment [29]. The nature of PKC is using two keys: one for encryption and one for decryption. In PKC, the data encryption is usually targeted to only one recipient or one group. This means that any message encrypted by using a public key can be decrypted only with the corresponding private key.

Many researchers considered that PKC schemes, such as Rivest–Shamir–Adleman (RSA) [30] and the DH key agreement scheme [31], were unsuitable for applications in WSNs, because of the big size of the code, message and data, the long processing time and the high power consumption. Sen [5] suggested that public key algorithms are computationally intensive and usually execute lots of multiplication instructions to perform a single-security operation. Therefore, one-to-one encryption is not efficient to be used in WSNs, because the overhead of encryption and the amount of cipher text are directly proportional to the total number of authorized users. Broadcast encryption [32] is an alternative solution to provide a one-to-many encryption method, but it requires the users to present their keys and other information individually. However, recent studies [33–35] argued that it is feasible to employ PKC in WSNs by using the right selection of algorithms and associated optimization, parameters and low power methods.

Many researchers in WSNs are interested in SKC schemes because of the lower computation overhead of SKC. SKC uses the same key for both encryption and decryption between two communicating hosts, who share the secret key. SKC seems to be suitable for low-end devices, like sensor nodes, because of their low overhead [36]. One major issue of using SKC methods is how to securely distribute the key between communication nodes. It is a major problem of using SKC, because key pre-distribution is not always feasible and reliable in WSNs. Even many symmetric ciphers are still too expensive to implement on sensor nodes.

Key management in WSNs has received lots of attention from researchers. Key management is an essential mechanism to ensure security in network services and applications, when cryptographic schemes are applied in the sensor networks. The main idea is to establish keys between nodes, trusted authorities and users in a secure and reliable manner. There are three different tasks in key management, namely key establishment, key revocation and key update. Key management is a big challenge in WSNs, because the sensor nodes can be deployed in any location and they know nothing about their neighbour nodes before deployment.

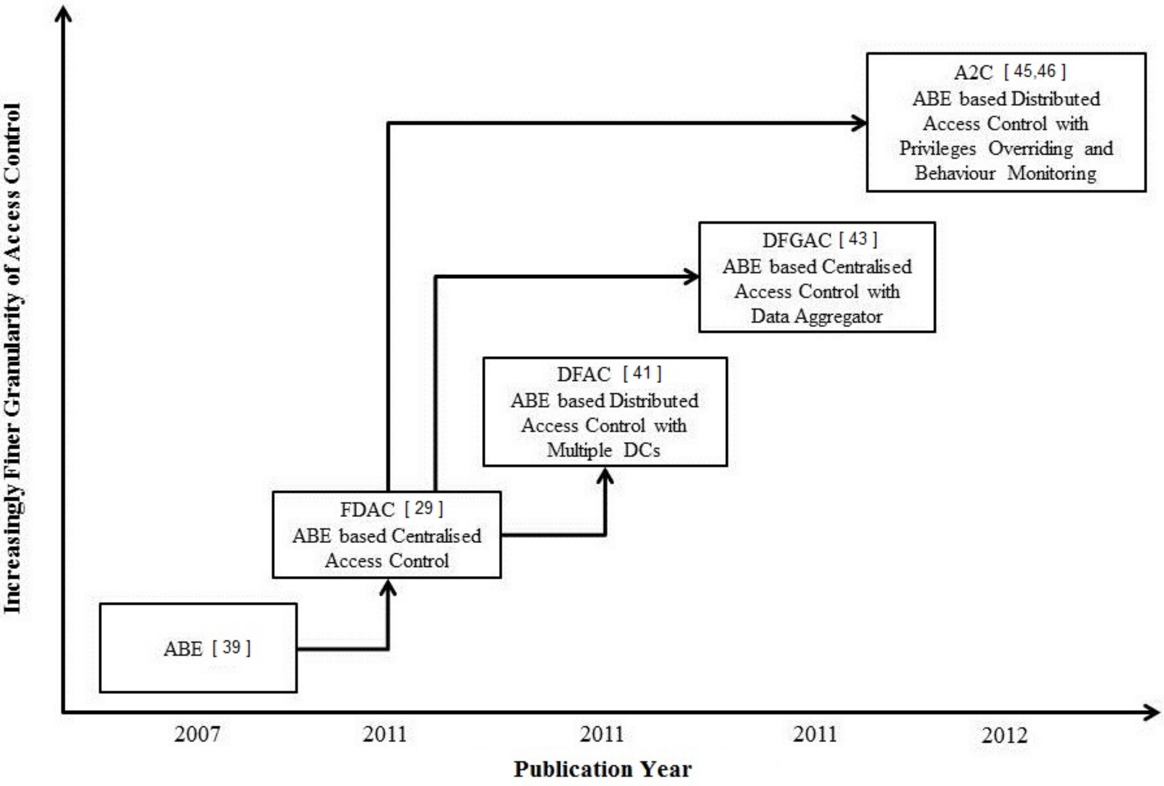
Choosing a suitable cryptography method is important in WSNs. In this section, we will explain two different types of CBAC models, namely elliptic curve cryptography (ECC)-based access control and attribute-based encryption (ABE)-based fine-grained access control.

3.2.1. Attribute-Based Encryption (ABE)-Based Fine-Grained Access Control

Sahai and Waters [37] proposed the ABE scheme to model and design a scalable and flexible access control system. ABE is a public key cryptography primitive generalising identity-based encryption (IBE) [38], which is associated with user's identity in a single user message. In ABE, a group of users is described by the combination of several descriptive attributes and access structures, which is also called an attribute policy. In ABE, the public key encryption is based on one-to-many encryption. There are two different types of ABE, which are proposed by Sahai and Waters [37], namely key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, data that is sensed and stored in the sensor node is encrypted with a set of attributes; the user's private key is associated with an access structure that specifies which types of ciphertexts the key can decrypt. Only the users that have the right access structure and the key can access and decrypt the sensed data. In CP-ABE, the ciphertext is associated with the access structure. The user's private key is associated with the attributes that specify which type of the ciphertext the key can decrypt. Some ABE-based fine-grained access control models use ECC for key management and distribution.

The ABE [39] method is commonly used in the access control models for data encryption and storage in WSNs. Li *et al.* [40] suggested that ABE is a highly promising public key encryption approach to realize scalability and fine-grained access control, where the flexible access permissions and rights are assigned to each individual user. Fine-grained access control facilitates granting different kinds of access permissions to a number of users. The sensors may sense or collect various types of information, like medical and battlefield information, which may belong to different security levels. Fine-grained access control is a security requirement to protect sensitive information from unauthorized access. One alternative way of providing fine-grained access control in WSNs is using an ABE scheme. The step-by-step development of ABE-based access control models in the WSN research community is shown in Figure 4. Based on this Figure, the four access control models, which use ABE-based encryption to provide fine-grained access control, are discussed next.

Figure 4. An evolution of attribute-based encryption (ABE)-based access control models in WSNs.


A2C [45,46]
ABE based Distributed Access Control with Privileges Overriding and Behaviour Monitoring
DFGAC [43]
ABE based Centralised Access Control with Data Aggregator
DFAC [41]
ABE based Distributed Access Control with Multiple DCs
FDAC [29]
ABE based Centralised Access Control
ABE [39]
Increasingly Finer Granularity of Access Control
2007
2011
2011
2011
2012
Publication Year

- **Fine-Grained Distributed Data Access Control (FDAC)** (2011)

Yu *et al.* [29] proposed the fine-grained distributed data access control (FDAC) model based on ABE. The main idea of their approach is to provide a distributed data access control, which is able to support fine-grained access control over sensor data and is resilient against attacks, such as user collusion (unauthorized users may collude to compromise the encrypted data) and node compromise (the sensor node could be compromised by a malicious user, due to lack of compromise-resistant hardware.). A network controller, which stores access structures, acts like a central distribution centre and distributes keys to users in FDAC. Only users with the right access structure and the right key can access data at the sensor nodes. The access structures will be different for each user depending on the access privileges of users.

For example, in a battlefield application, the sensor nodes may be responsible for collecting different types of data, such as vibration, smoke, *etc.*, in different locations (village, forest). Therefore, the attributes, such as {location = village, data type = (vibration, smoke), owner = (explosion experts, officers)}, are used to specify the data access privileges of users. Based on the above example, the access structure of a user is designated as "(location is village) AND (type is vibration)", which allows the user to obtain the vibration data within the village area. More sophisticated access structures can be defined based on the application requirements. If the network controller is compromised by a malicious user, there will be no security provisioning in the system anymore. User revocation (user revocation may be one of the following: the service subscription is expired, the user changes group intentionally or the user or group key is compromised) can be done by updating the master secret key that is embedded in the user secret key via broadcasting. In this approach, CP-ABE-based selective broadcast is used for user revocation, but there are no details on how to use it.

- **Distributed Fine-Grained Access Control (DFAC)** (2011)

  Ruj *et al.* [41] proposed a fully distributed fine-grained access control (DFAC) scheme using multi-authority ABE [42] to prevent a single point of failure. Instead of using one authority, like FDAC, several distribution centres (DCs) are used to store and distribute different access structures, sets of attributes and cryptographic keys to users and sensor nodes. All DCs are disjoint from each other. Each DC has its own access subtree (a subtree contains attributes at the leaf nodes of that subtree.) for each sensor node. Users, who want to access data at the sensor node, need to activate their ID with each DC to obtain access structures, access subtrees and keys. All of the subtrees from each DC are ANDed together to build a complete access structure for a single user, but the user has to store all of the access structures in order to access different types of data from the sensor network. This model facilitates modification and secret key distribution when the access rights of a user are changed, but the communication overhead of the user's revocation process is higher than with FDAC.

- **Distributed Fine-Grained Data Access Control for Distributed Sensor Networks (DFG-AC)** (2011)

  Hur [43] proposed an access control model called distributed fine-grained data access control (DFG-AC). It uses both a network controller and a data aggregator for central key management and central storage. The collected data from sensor nodes are transferred to the data aggregator by using a distributed sensor data collection protocol, such as the Two-Tier Data Dissemination protocol (TTDD) [44]. The main idea of using the data aggregator as central storage is to perform more data encryption. Additionally, the users can get all of the information by accessing the data aggregator. The data aggregator is more powerful than the sensor nodes, and it can use complex encryption methods. The advantage of the proposed model is that it considers the stateless receiver problem. (Practically, users may miss a key update message. Therefore, they cannot keep their key states up-to-date. This problem is known as the stateless receiver problem.) To solve this problem, key revocation is done with a stateless group key distribution mechanism using a binary tree. One of the disadvantages is that the transmitting data from sensor nodes to the data aggregator consumes lots of battery power and energy. In addition, there might be a single point of failure because of the centralised data storage. This model provides user revocation by using the KP-ABE scheme with the attributes for distributed WSNs.

- **Adaptive Access Control** (A2C) (2012)

  Htoo *et al.* [45,46] proposed an adaptive access control (A2C) model with privilege overriding and behaviour monitoring to provide fine-grained access control for medical data in WSNs. A2C incorporates the concept of possibility-with-override and a user behaviour trust model into WSNs for hard-to-define and unanticipated situations. This model has a similar structure to BTG-RBAC, but the main difference is that no human effort is needed to override rules and policies, because of the introduction of the overriding access privileges, the users' behaviour trust model and the prevention and detection mechanism. In this model, the users may be able to override a denial of access, when unexpected events occur. In addition, the users' behaviour trust model is used to check user's action, location, time, *etc*. The advantage of this model is that all of the user behaviour information is kept by the prevention and detection mechanism as an audit record to detect and prevent abnormal and unauthorised access, whenever the users try to access data from WSNs. ABE-based encryption and TTDD are used for data storage and data transmission. The main contribution of the proposed model is to adapt to unexpected situations by using privilege overriding and also to adjust its decision based on users' behaviour trust values.

3.2.2. Elliptic Curve Cryptography-Based Access Control (EC-CBAC)

Elliptic curve cryptography-based access control (EC-CBAC) models [36,47,48] use ECC to authorize and grant users access to data. They prevent the malicious nodes from joining the sensor network. ECC has become popular as the solution for WSN due to low computational overhead and small key size. Unlike for the RBAC and ABE-based access control models, there is no table for the evolution of ECC-based models in this section. The similarity of the proposed models is simply that they used ECC-based encryption.

- **Wang, Sheng and Li Model** (2006)

  Wang *et al.* [47] proposed an access control model based on ECC. The main objective of the proposed model is to use an ECC scheme for granting user access rights to the collected data. Different users may have different levels of data access due to restriction of access implicated by the data confidentiality and privacy. ECC is used in key distribution and sharing information between the users and a key distribution centre (KDC). In this approach, KDC is responsible for generating all security primitives, such as random numbers, access lists and hash functions, and maintains a user list with associated user identifications. The users have to request access permission from KDC. Access lists, which comprise user identity, group identity and user privilege mask, define the user's access privileges. User access privilege mask is a number of binary bits, and each bit represents a specific information or service. Therefore, users who possess the same mask and access privileges are put in the same group.

- **Zhou, Zhang and Fang Model** (2007)

  Zhou *et al.* [36] proposed an access control protocol based on ECC for node authentication and key establishment. The main idea of their approach is to accomplish node authentication and key establishment for new nodes, whenever they join the sensor network. The proposed access control model uses node identity and node bootstrapping time for the node authentication procedure. They introduced the node bootstrapping time into authentication procedures to differentiate malicious nodes from legitimate new nodes. In this model, the authors are mostly looking at the node deployment to prevent malicious nodes from joining the network. A certification authority (CA) is used to generate a certificate, which includes ID information and bootstrapping time, to authenticate the identity of a new node. Furthermore, the node certificate is signed with CA's private key. Therefore, the adversaries cannot alter ID and bootstrapping time. When the new node is deployed in WSNs, it shows its certificate to the neighbour nodes in order to verify its identity with CA's public key. This access control protocol enforces control sensor node deployment and prevents malicious nodes from joining sensor networks.

- **Al-Mahmud and Morogan Model** (2012)

  Al-Mahmud and Morogan [48] proposed an identity-based authentication and access control model in WSNs. The main idea of the proposed model is to use an identity-based signature (IBS) [49] for providing both user authentication and data access control in WSNs. This protocol is based on the IBS scheme, where an ECC-based digital signature algorithm (DSA) [50] is used to sign and verify a message. A base station (BS) is responsible for generating the private keys of both users and sensor nodes in the network. For the key distribution, a one pass key establishment protocol [51] is used to share session keys between sensor nodes and users. Users are required to register with BS. Based on the access request from the users, BS generates private key and access structure for each user. The sensor nodes are preloaded with hash value of user identities and the private key, which will be used for the authentication process. After the authentication process, the sensor node will check whether the user is authorized to access the data.

3.3. Users' Privacy-Preserving Access Control (UPPAC)

Most of the access control models in WSNs are to provide data privacy and data confidentiality. The privacy of users and sensor nodes in WSNs is different from data privacy and has received less attention in the literature. In user privacy, users aim to hide their ID and other information. Therefore, no one in the network knows the real ID of a user, except the network authority and the user himself. Recently, there are two schemes proposed for the privacy-preservation of users' information in WSNs, namely distributed privacy-preserving access control (DP2AC) [52] and distributed privacy-preserving access control (PRICCESS) [53]. The PRICCESS model is related to the RBAC model. The main reason why the PRICCESS model is presented under UPPAC is that it provides user privacy preserving distributed access control in WSNs.

- **Distributed Privacy-Preserving Access Control (DP2AC)** (2009)

  Zhang *et al.* [52] proposed distributed privacy-preserving access control (DP2AC). The owner of the sensor network generates the token by using a blind signature [54]. 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 unauthorised access to sensed data, while users can protect their data access privacy.

  However, a recent study [55] 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 a 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. A 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.

- **Distributed Privacy-Preserving Access Control (PRICCESS)** (2011)

  He *et al.* [53] 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 [56] 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 PRICCESS model used an ACL matrix to store the access list of the group for data access control in the network controller. Any user from the group can use a group key when he signs the message for data access request. Therefore, the network controller verifies that the message has been signed by one of the group members without knowing who the actual signer is. One of the 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.

We have categorized and briefly discussed the access control models for WSNs in this section; next we compare these access control models.

4. Comparison of Access Control Models in WSNs

This section compares current access control models as have been discussed above based on network model, key management, data encryption, policy specification, the decision-making process, user revocation and user privacy preservation. An outline of the comparison is presented in Table 2.

4.1. Network Model

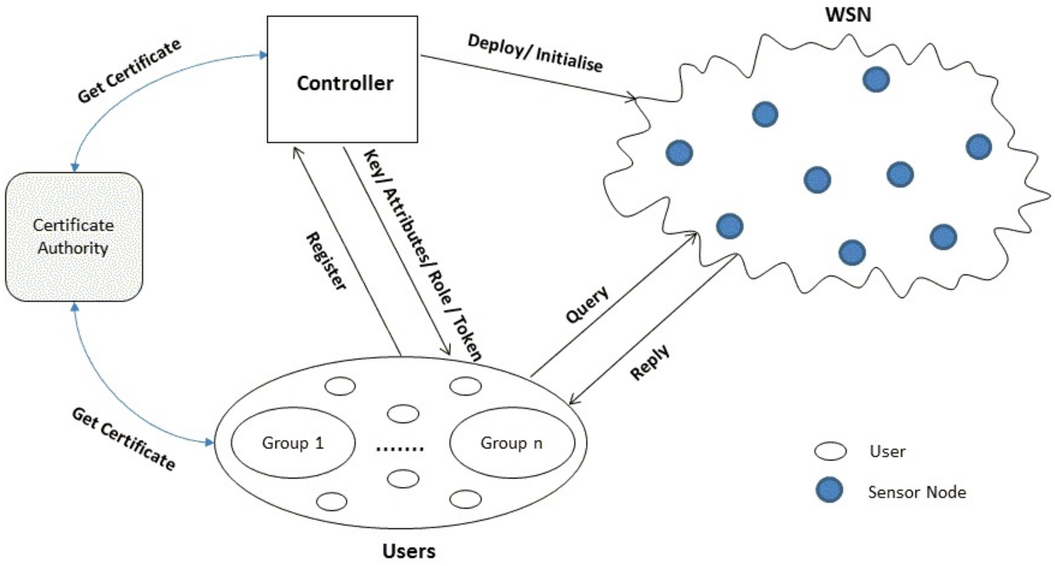
Access control models can be different based on their network architecture model when the cryptographic keys, roles, policies and attributes are distributed to users from the trusted authority or controller. Based on the above discussion about current access control models in WSNs, we separated them into two different network architecture models, namely the centralised network model and the distributed network model.

In a centralised network model, WSN is deployed and initialized with key, role, attributes, *etc.*, by the controller. Whenever the users want to access data from the network, they have to register with the controller to obtain the keys, access structure, token, role, *etc.* Some schemes involve cooperation with a certificate authority (CA) before the users register with the controller. The users can send a query message with keys, access structure, token, *etc.*, which have to be matched the keys, attributes, role, *etc.*, from the sensor nodes. If the users have the right access privilege, the sensor nodes will allow the users to access data based on their access privileges.

Table 2. Comparison of access control models in WSNs.

Access Control Model	Network Architecture and Component	Key Management	Encryption and Decryption	Policy Specification and Decision-Making Process	User Revocation	User Privacy Preservation
Zhu's Model [23]	Authentication Manager (AM)	DH	-	Role, Purpose, Operation	-	-
CA-RBAC [1]	System Administrator (SA)	-	-	Role, Context Information	-	-
BTG-RBAC [26]	System Administrator (SA)	-	-	Role, Purpose, Operation, Obligation	-	-
FDAC [29]	Network Controller (NC)	DB-DH	ABE	Attributes-Based Key	CP-ABE	-
DFAC [41]	Distribution Centre (DC)	B-DH	ABE	Attributes-Based Key	ABE	-
DFG-AC [43]	System Controller (SC) and Data Aggregator	B-DH	ABE	Attributes-Based Key	Attribute Level User Revocation	-
A2C [45]	System Administrator (SA)	-	ABE	Attributes-Based Key, Context Information, Behaviour Trust Value	-	-
Wang, Sheng and Li Model [47]	Key Distribution Centre (KDC)	EC-DH	ECC	Key	-	-
Zhou, Zhang and Fang Model [36]	Certificate Authority (CA)	DH	ECC	Key	-	-
Al-Mahmud and Morogan Model [48]	Base Station (BS)	One-Pass Key Establishment Protocol	ECC-Based IBE	Key (Built on ID)	-	-
DP2AC [52]	Network Owner	RSA-DH	RSA	Role, Token	-	Blind Signature
PRICCESS [53]	Certificate Authority (CA)	DH	ECC	Role, Group Key	-	Ring Signature

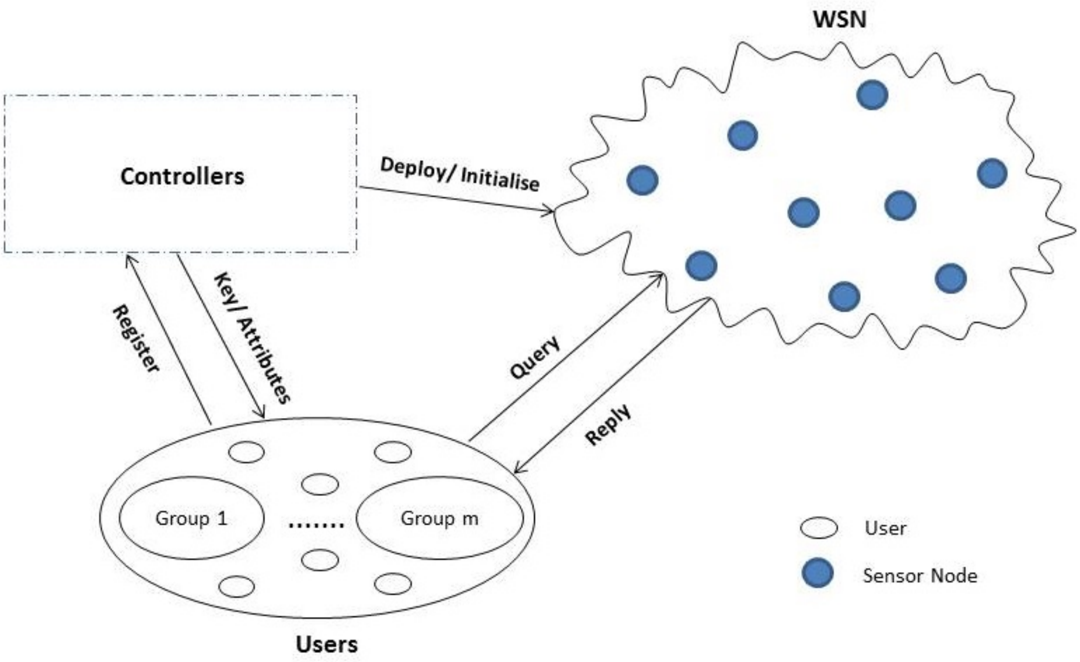
Figure 5. Centralized network model.



An overview diagram of the centralised network model is shown in Figure 5. The current access control models, such as Zhu's model [23], CA-RBAC [1], BTG-RBAC [26], the FDAC model [29], DFG-AC [43], Wang, Sheng and Li's model [47], Zhou, Zhang and Fang's model [36], Al-Mahmud and Morogan's model [48], DP2AC [52] and PRICCESS [53], used the centralised network model. The controller shown in Figure 5 might be identified as the authentication manager (AM) [23], system administrator (SA) [1,26], network controller (NC) [29], system controller (SC) [43], key distribution center (KDC) [47], base station (BS) [48], certificate authority (CA) [36,53] or network owner [52]. Users have to register with the controller to obtain the access privileges for data access. The disadvantage of the centralised network management model is that a single point of failure can occur at anytime, because the controller manages all of the key generation, distribution, *etc*. If the controller is compromised, there is no security provision in the network.

In the distributed network model, multiple controllers manage the WSN instead of it being handled by just one controller, as in the centralized network model. A user has to register with several distribution centres (DCs) to obtain the data access according to his/her access privileges. In the distributed approach, the controllers are not cooperating with each other. The public key of the network is derived from the attributes. A sensor node is preloaded with some attributes from each DC and the public key parameter set based on the possession of attributes. Each user needs to present his/her identity to each DC to get a set of attributes and a set of access structures. An access structure consists of subtrees, which contain attributes at the leaf nodes. Even at the leaf nodes of subtrees, there are AND, OR and t-out-of-n threshold operations. Each DC gives only one access subtree to the user. All of the subtrees from each DC are ANDed together to build a complete access structure for a single user. The user who matches a set of attributes with a sensor is able to access data from that sensor. If one controller is compromised by an attacker, he can only get certain types of data, which are managed by that controller. The disadvantage of the distributed approach is that the sensor nodes need to interact with more than one controller and store multiple keys when the network is initialised and deployed by the controllers. The overview diagram of the distributed network model can be seen in Figure 6.

Figure 6. Distributed network model.



Based on the above discussion, most of the access control models in WSNs use the centralised approach apart from DFAC [41] and A2C [45], which use the distributed approach. However, the network models are quite similar for all the access control models. In each model, different controllers are used for network management and for key distribution. All of the controllers have similar functionality, such as CA or trusted authority. Overall, AM, CA, SA, NC, DC, KDC and the network owner, which have much the same functionality, are used in the current models to handle network management and key distribution.

4.2. Key Management

The Diffie–Hellman (DH) key exchange protocol and ECC are widely used for key distribution and key management in access control models in WSNs. Simple DH key exchange is used in Zhu's scheme [23] to provide sensor level access control and to protect from malicious nodes joining the network. DH key exchange protocol is simple and fully distributed, and ECC has smaller-sized cryptographic keys than other public key schemes. Therefore, the combination of DH and ECC is suitable to use in resource and memory limited small devices, like sensor nodes. The ECC-based DH key management scheme is used in Zhou, Zhang and Fang's model [36], PRICCESS [53] and Wang, Sheng and Li's model [47]. ECC-based decisional bilinear Diffie–Hellman (DB-DH) is used in FDAC [29]. However, bilinear Diffie-Hellman (B-DH) is used in both DFG-AC [43] and DFAC [41]. RSA-based public and private keys are used for key management in DP2AC [52], but the key management scheme is based on the DH approach. In addition, the uTESLA[57] protocol is used by the network owner to update keys of the sensor nodes. In Al-Mahmud and Morogan's model [48], a one-pass key establishment protocol is used for the key distribution and shared session keys between sensor nodes, users and the base station. There is no explanation about the key management scheme in BTG-RBAC [26] and CA-RBAC [1].

4.3. Data Encryption

A popular encryption method for data storage in WSNs is using ABE at the sensor nodes. ABE-based encryption is popular relative to other public key encryption methods because of its highly promising approach to realize scalability and fine-grained access control. The ABE method is used in the FDAC [29], DFAC [41], DFG-AC [43] and A2C [45] models for data encryption, as well as for data access control. Data in the sensor nodes are encrypted using attributes and keys from the trusted authorities. Data access is given only to users who have both keys and access structures to match the attributes and keys from the sensor nodes. Other public key encryption methods are based on ECC and RSA. ECC is a popular choice for data encryption, because of its characteristics, such as small sized key and low overhead. ECC-based encryption is used in Zhou, Zhang and Fang's model [36], PRICCESS [53] and Wang, Sheng and Li's model [47]. Simple data encryption based on RSA is used in DP2AC [52] for data encryption.

4.4. Policy Specification and Decision-Making Process

Policy specification and decision-making processes depend on the network architecture and policy; and the role specifications in the access control model. The decision-making process is based on predefined roles and policies in RBAC-based models, such as Zhu's model [23], CA-RBAC [1] and BTG-RBAC [26], but in CB-RBAC, contextual information and roles are considered. BTG-RBAC used authorization and obligation roles to make access decisions based on users' requests in an emergency. The main disadvantage of using the RBAC model is that the data access roles and policies need to be defined in advance. Sometimes, it is hard to predict and predefine all the possibility of roles and policies for policy specification and the decision-making process.

In ABE-based access control models, such as FDAC [29], DFAC [41], DFG-AC [43] and A2C [45], attributes, such as location, role, *etc.*, are used to define policies and make access decisions on users' requests. The access policies are different based on the attributes and the unique key from each user. In the A2C model, not only an attributes-based key is used, but also contextual information and a behaviour trust value are used to make a flexible access decision in any situation. Therefore, to override a denial access policy in the A2C model, the key, behaviour trust value and contextual information are considered in order to make an effective access decision. In Wang, Sheng and Li's model [47], the private key and access list of the user are used to make an access decision at the sensor nodes, but for Zhou, Zhang and Fang's model [36], the private key and certificate are used for node deployment. In Al-Mahmud and Morogan's model [48], hash values of the user identity and the private key of the user are used to specify policy. DP2AC [52] used a blind signature to generate a token, which contains access privileges for the data. For PRICCESS [53], the ACL matrix is used to store roles and policies. These policies and roles are stored based on a group of users and their access privileges. Therefore, each group of users has different access privileges based on their group's policy.

4.5. User Revocation

User revocation means that the users' service subscription is expired, the key of the user is compromised or the user changes to a different group intentionally. It has received less attention in WSNs. Only FDAC [29], DFAC [41] and DFG-AC [43] discussed user revocation in WSNs. In FDAC and DFAC, the life time of a sensor node is divided into many phases. In each phase, the master key of the network is updated by using a CP-ABE-based broadcast encryption scheme to prevent unauthorized access from the old users who leave the sensor network. Only users who still have access to the sensed data will receive the key update messages from the trusted authority. In DFG-AC [43], the system controller notifies and sends the updated membership list to a data aggregator, as well as to the network users that are listed on the membership list. When the data aggregator receives the notification message, it changes the attribute group key and re-encrypts the stored data with that key. Therefore, only the network users, who receive the update message, are able to access data from the sensor nodes.

4.6. Users' Privacy Preservation

DP2AC [52] and PRICCESS [53] provide privacy preservation for users who access data from the network. In DP2AC, the network owner generates the token by using a blind signature. No one will know the true identity of that user, including the network owner himself, because user information is not needed to generate the tokens. The ring signature is used in the PRICCESS protocol to provide the privacy of user information in WSNs. Anyone in a group can access data by using the group ring key instead of using his own identity and key. An alternative way to provide privacy preserving in WSNs is to use pseudo-random functions (PRF) [58]. In that approach, the user ID is computed with a PRF function to generate a random number. Therefore, no one in the network will know who the actual signer of the access request is.

Table 2 shows the comparison of access control models in WSNs based on the above discussion. The next section evaluates current access control models based on features and performance.

5. Evaluation of Access Control Model in WSNs

In this section, the criteria used for the comparison and evaluation of access control models are studied and a novel set of evaluation criteria is proposed. The current access control models in WSNs will be evaluated based on two aspects: features and performance evaluation.

5.1. Evaluation Based on Features

To make meaningful comparisons of the current access control models in WSNs, the evaluation framework is defined to compare and contrast current access control models by using the following features [27,59,60].

1. *Support Data Privacy*

   The need for data privacy is growing among all of the real-world applications in WSNs. Data privacy becomes more and more important in WSNs, when data are to be released to only authorized and legitimate users. The more data being disclosed, the more the owner of that data loses his own privacy.

2. *Support User Privacy*

   The need for user privacy is important in some applications. Sometimes, a user, who tries to access data from the network, does not want to share his detailed information with other users in the network. This means that the users' privacy preservation is needed to protect the privacy of user information in the network.

3. *Flexibility*

   No matter how perfect an access control system is, if it does not support accommodation to changes, such as insertion and deletion of the application systems, the access control model is not feasible to use in real-world applications. In WSNs, the user characteristics and the access context are changing continuously. Therefore, the access control decisions must be synchronised with continuously changing security conditions. It is desirable for the access control model to handle the dynamism of users and environments. Therefore, the access control model needs to be flexible enough to support changes and synchronise with the access control decisions.

4. *Support for Emergency Data Access*

   An ideal access control model needs to support data access, not only in normal situations, but also in an emergency situation. Many applications will benefit from such a provision.

5. *Context Sensitivity*

   An access control model is context sensitive when context information plays a role in making the appropriate access decision. This means that the contextual information is used in defining policies for making an access control decision dynamically.

6. *Granularity*

   There are two different types of granularity in access control, which are fine-grained and coarse-grained. Fine-grained means that the access control models should allow different roles for specific data accesses and provide a fine-grained reference to the subjects and objects. Coarse-grained means that groups of users and collections of objects often share the same access control requirements. The access control system should then offer support for authorization specific to the groups of users, objects and possibly actions.

These six supporting features listed above are used to evaluate the current access control models in WSNs. Table 3 shows a comparison of current access control models based on these features and qualities. The first row of the table describes evaluation criteria, and the first column lists access control models. Each cell in the table shows whether the model of that row has the feature of that column.

All of the access control models in WSNs provide data confidentiality and data privacy in normal conditions, but the users' privacy preservation is only supported in DP2AC and PRICCESS. The access control models that used ABE and contextual information to make access decisions provide flexibility in the system. Based on Table 3, all of the access control models in WSNs support authorization decisions and allow for changes, like roles, users, policy, *etc*. Among them, CA-RBAC, BTG-RBAC and A2C support emergency and immediate data access, but data privacy has not been discussed, apart from the adaptive access control model. There are few access control models that make authorization decisions based on context information. Approximately equal numbers of access control models support coarse-grained and fine-grained. As a summary, the authorization policy for each scheme is different, which means that all models are proposed to solve different problems and look from different points of view to fill the gaps in WSNs area. In addition, there is no access control model that provides data privacy in emergency and unexpected conditions, apart from A2C model.

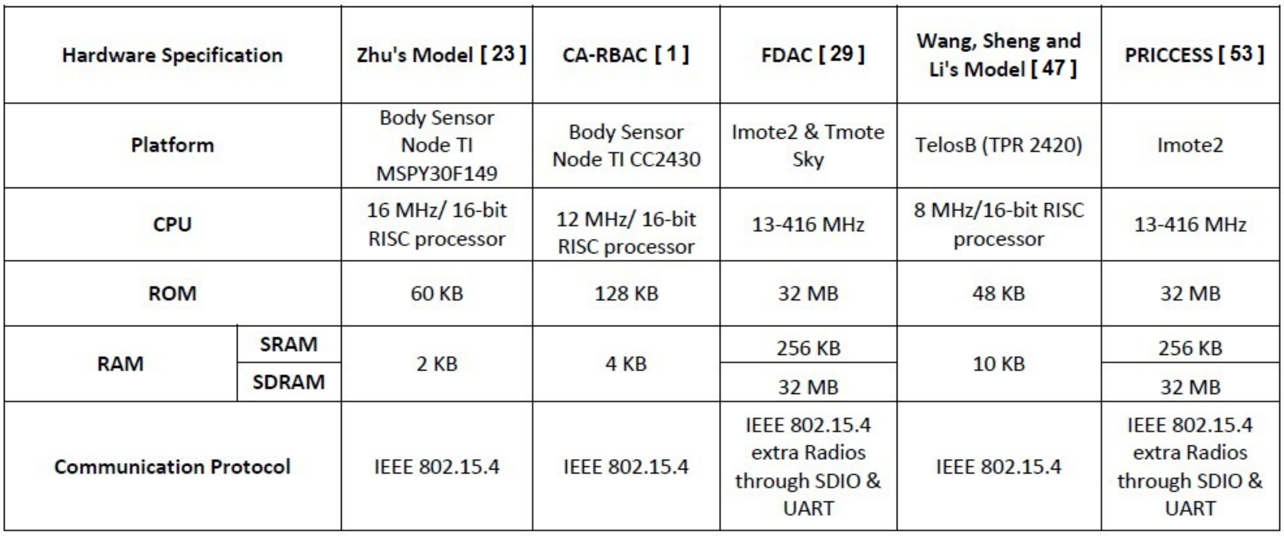
Table 3. Comparison of access control models based on features in WSNs.

Access Control Models	Support Data Privacy	Support User Privacy	Flexibility	Support For Emergency Access	Context Sensitivity	Granularity
Zhu's Model [23]	Yes	No	No	No	No	Coarse-Grained
CA-RBAC [1]	Yes	No	Yes	Yes	Yes	Fine-Grained
BTG-RBAC [26]	Yes	No	Yes	Yes	No	Coarse-Grained
FDAC [29]	Yes	No	Yes	No	Yes	Fine-Grained
DFAC [41]	Yes	No	Yes	No	Yes	Fine-Grained
DFG-AC [43]	Yes	No	No	No	Yes	Fine-Grained
A2C [45]	Yes	No	Yes	Yes	Yes	Fine-Grained
Wang, Sheng and Li Model [47]	Yes	No	No	No	No	Coarse-Grained
Zhou, Zhang and Fang Model [36]	Yes	No	No	No	No	Coarse-Grained
Al-Mahmud and Morogan Model [48]	Yes	No	No	No	No	Coarse-Grained
DP2AC [52]	Yes	Yes	No	No	No	Coarse-Grained
PRICCESS [53]	Yes	Yes	No	No	No	Coarse-Grained

5.2. Evaluation Based on Performance

The performance evaluation is discussed based on computation cost, communication cost, memory usage and processing or execution time. Before we discuss the performance evaluation, we describe the hardware specifications and products that are used to deploy the access control engines and models for WSNs. Figure 7 shows the comparison of hardware specifications that are used in the proposed access control models. Based on Figure 7, the various platforms of sensor nodes are used. The CPU speed and size of the memory are also varied based on the sensor node's platform. However, all of the sensor nodes are chosen to use IEEE 802.15.4 as the communication protocol. Some of the proposed access control models in WSNs are not developed in practice, yet, but some of them are implemented in experiments.

Figure 7. A comparison of hardware specification.

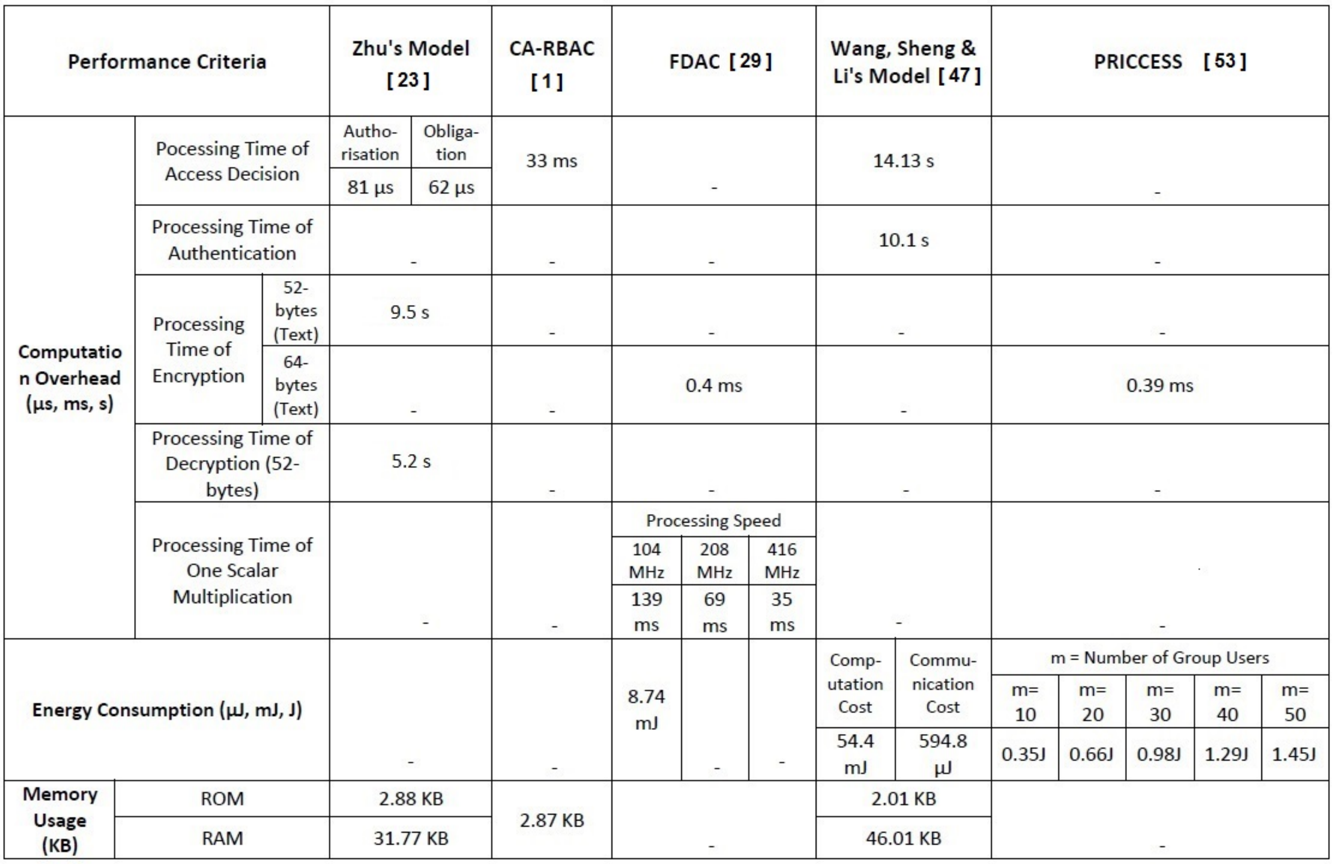


Hardware Specification		Zhu's Model [23]	CA-RBAC [1]	FDAC [29]	Wang, Sheng and Li's Model [47]	PRICCESS [53]
Platform		Body Sensor Node TI MSPY30F149	Body Sensor Node TI CC2430	Imote2 & Tmote Sky	TelosB (TPR 2420)	Imote2
CPU		16 MHz/ 16-bit RISC processor	12 MHz/ 16-bit RISC processor	13-416 MHz	8 MHz/16-bit RISC processor	13-416 MHz
ROM		60 KB	128 KB	32 MB	48 KB	32 MB
RAM	SRAM	2 KB	4 KB	256 KB	10 KB	256 KB
	SDRAM			32 MB		32 MB
Communication Protocol		IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4 extra Radios through SDIO & UART	IEEE 802.15.4	IEEE 802.15.4 extra Radios through SDIO & UART

Differently, A2C [45] has been designed and implemented in the simulation environment of Ponder2 [61] for wireless body sensor networks in medical applications. The simulation results show that fine-grained data access control is provided in this model, but there is no performance evaluation based on memory, CPU speed, *etc.* Therefore, we cannot make a fully comparative performance evaluation, but the performance evaluation of the developed access control models will be discussed briefly. The comparison has been made based on the results obtained from the implementation and evaluation outcomes of the proposed WSN access control models. In Figure 8, there are many blanks cells in the table. This means that the performance measurement of each model is varied and measured differently based on the design and what kind of security services are provided. It would be very useful for future research if some kind of benchmark could be produced to compare the performance of different WSN access control models.

Without such a benchmark, the performance evaluation for each model is quite different and is measured differently. The computation overhead for each access control model is different based on how the access control model has been designed and what was the purpose of the proposed model. The processing time of access decisions and authentication processes are different based on what kinds of method and approach are used in the proposed models. For example, in Zhu's model, the processing of authorization and obligation decisions takes about 81 μs and 62 μs, respectively. The processing time of access control decisions in CA-RBAC is 33 ms, which excludes delays due to the communication overhead, length of the message, message collisions and verification of digital certificates. In Wang, Sheng and Li's model, the total access decision time is 14.13 s, which is relatively long, when compared with CA-RBAC. It includes the users perceived delay from sending out the access request to the sensor node, as well as the amount of time for the sensor node to make an access decision and to approve the users. Ten-point-one seconds is required for the authentication processing time in Wang, Sheng and Li's model. This seems to indicate that the proposed WSN models are not measuring the same thing.

Figure 8. A comparison of access control models based on performance Evaluation.



Performance Criteria			Zhu's Model [23]	CA-RBAC [1]	FDAC [29]	Wang, Sheng & Li's Model [47]	PRICCESS [53]
Computation Overhead (μs, ms, s)	Pocessing Time of Access Decision		Autho-risation 81 μs Obliga-tion 62 μs	33 ms	-	14.13 s	-
	Processing Time of Authentication		-	-	-	10.1 s	-
	Processing Time of Encryption	52-bytes (Text)	9.5 s	-	-	-	-
		64-bytes (Text)	-	-	0.4 ms	-	0.39 ms
	Processing Time of Decryption (52-bytes)		5.2 s	-	-	-	-
	Processing Time of One Scalar Multiplication		-	-	Processing Speed 104 MHz: 139 ms 208 MHz: 69 ms 416 MHz: 35 ms	-	-
Energy Consumption (μJ, mJ, J)			-	-	8.74 mJ - -	Comp-utation Cost 54.4 mJ Commu-nication Cost 594.8 μJ	m = Number of Group Users m=10: 0.35J m=20: 0.66J m=30: 0.98J m=40: 1.29J m=50: 1.45J
Memory Usage (KB)	ROM		2.88 KB	2.87 KB	-	2.01 KB	-
	RAM		31.77 KB			46.01 KB	

It is also important to measure the processing time of encryption and decryption under the computation overhead. The processing delay of both TinyECC [62] -based encryption and decryption for 52-bytes message is 9.5 s and 5.2 s in Zhu's model. If a symmetric Skipjack cryptography [63] is used instead of TinyECC, the processing delay will be decreased dramatically from 9.5 s to 150 μs for encryption and from 5.2 s to 90 μs for decryption. The processing time of encryption for 64-bytes text message in the PRICCESS model is 0.39 ms, but there is no information about the processing time of decryption in this model. In FDAC, the computation overhead of one scalar multiplication (the sensor nodes need to execute one scalar multiplication on elliptic curves, one-way hash and one symmetric key data encryption for 64-bytes text message) on Imote2 is 139 ms when working with 104 MHz. For 208 MHz and 416 MHz, it took 69 ms and 35 ms for one scalar multiplication. The computation overhead of one scalar multiplication will be much lower, if the RSA-based algorithm is used instead of the ECC-based algorithm. The processing time of encryption is 0.4 ms for the RSA-based algorithm to encrypt 64 bytes of random text.

Some access control models are mostly concerned with the energy consumption in WSNs, because battery power is used. Therefore, it is important to measure the energy consumption based on computation and communication cost. In Wang, Sheng and Li's model, the power consumption for communication is calculated based on the maximum current draw. The total computation and communication cost for one access control decision in this model is 55.1 mJ, which is 54.4 mJ for computation cost and 594.8 μJ for communication cost. In FDAC, the energy consumption cost for one scalar multiplication process in 104 MHz is 8.74 mJ. In PRICCESS, the energy consumption cost will be different based on the number of users in a group. The node verification cost for 10, 20, 30, 40 and 50 members in the group is 0.35 J, 0.66 J, 0.98 J, 1.29 J and 1.45 J.

Based on the hardware specification of the sensor node in Figure 5, there is a limited memory storage for each sensor node, but it will be different on the platforms. Therefore, the usage of memory for each sensor node has to be measured correctly and carefully. Comparing Zhu's model with Wang, Sheng and Li's model, the memory usage for authentication executable occupies 31.77 Kb and 46.01 Kb of ROM, respectively, but for RAM, 2.88 Kb and 2.01 Kb are occupied. The total memory requirement for the CA-RBAC model is 2.87 Kb.

Based on the above discussion, the comparison of the proposed WSN access control models is hard to clarify, especially in performance measurement, because these models are proposed and designed based on different requirements and different security services to fill the gaps of active application areas in WSNs. It also shows and indicates that various access control models are measuring different things. Further studies are needed to clarify and evaluate the performance measurement of WSN access control models. This means that the authors, or other researchers in the WSN community, should study and measure the performance of all of the proposed WSN access control models in a similar way. The next section will explain some potential research issues for the access control models based on the above comparison and evaluation results.

6. Potential Research Issues

The development of access control in WSNs is challenging, because memory and other resources are limited, but access control is an essential security service, which is necessary to prevent unauthorized access by malicious users in a WSN. Especially in medical and military applications, data access controls for legitimate users are important to provide in any situation, because it is hard to assume and predefine all of the possibilities of what will happen in the future and what kind of unexpected situations will occur in the system. Based on the above literature review of the current access control models in WSNs and WMSNs, key open research issues are identified as follows:

- Various access control models have been proposed; however, no systematic comparisons have been conducted on these models. Further evaluation and comparison is desirable to learn the security services, performance, reliability and efficiency of these access control models.

- Most of the proposed access control models for WSNs are focused on node authentication and query authentication, but users' data access control has received little attention. The control of the user to the sensed data at the sensor nodes merits more investigation.
- Current access control models need to be made much more flexible to make access decisions on the unexpected events, because it is hard to predefine all of the possibilities in a WSN. A new access control model is needed to address higher reliability, scalability, availability and accountability to prevent unauthorized user access and allow authorized users data access in unexpected and unpredictable cases.
- The performance of WSN access control models should be studied and measured carefully in the future. It would be useful to produce an appropriate benchmark for the WSN research community.
- It is also likely that more powerful sensor nodes will need to be designed in order to support the increasing requirements for computation and communication in the sensor nodes. This means that a powerful encryption and decryption method should be able to apply in the future.

7. Conclusion

In this paper, we present the security vulnerabilities, security requirements and a literature review of current access control models, and also, we discuss the performance evaluation and comparison of the proposed models in WSNs. Although research efforts have been made on cryptography, key distribution and management and access control models in WSNs, there are still some challenges to be addressed, like the selection of appropriate cryptographic methods. Furthermore, the design of access control models in WSNs must satisfy constraints, such as energy, computation capacity and memory. Access control is a critical security service in sensor networks and is essential to ensure that network services are offered only to legitimate users in WSNs. The comparison of current access control models showed that there is still lots of work to be done on access control models in WSNs, especially for emergency and immediate data access.

Author Contributions

HM drafted the initial manuscript. HX, BC and JAM amended and refined the structure, content, and language of the manuscript. All authors read and approved the final manuscript.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments.

Conflict of Interest

The authors declare no conflict of interest.

References

1. Garcia-Morchon, O.; Wehrle, K. Modular context-aware access control for medical sensor networks. In Proceedings of the 15th ACM symposium on Access control models and technologies (SACMAT '10), Pittsburgh, PA, USA, 9–11 June 2010; pp. 129–138.
2. Ngo, D.N. Deployment of 802.15.4 Sensor Networks for C4ISR Operations. PhD Thesis, Navy Postgraduate School, Monterey, CA, USA, 2006.
3. Faye, Y.; Niang, I.; Noël, T. A survey of access control schemes in wireless sensor networks. *World Acad. Sci. Eng. Technol.* **2011**, *5*, 814–823.
4. Vella, M.N. *Survey of Wireless Sensor Network Security*; Report; Texas A and M University-Corpus Christi, Computer Science Program, Texas A and M University Press: College Station, TX, USA, 2008.
5. Sen, J. A survey on wireless sensor network security. *Int. J. Commun. Netw. Inf. Secur.* **2009**, *1*, 55–78.
6. Ng, H.S.; Sim, M.L.; Tan, C.M. Security issues of wireless sensor networks in healthcare applications. *BT Technol. J.* **2006**, *24*, 138–144.
7. Wang, W.; Bhargava, B. Visualization of wormholes in sensor networks. In Proceedings of the 3rd ACM Workshop on Wireless Security (WiSe '04), Philadelphia, PA, USA, 26 September 2004; pp. 51–60.
8. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The sybil attack in sensor networks: Analysis & defenses. In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 26–27 April 2004; pp. 259–268.
9. Li, Z.; Gong, G. *A Survey on Security in Wireless Sensor Networks*; Technical Report; University of Waterloo: London, UK, 2008.
10. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: attacks and countermeasures. In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA, 11 May 2003; pp. 113–127.
11. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62.
12. Perrig, A.; Stankovic, J.; Wanger, D. Security in wireless sensor networks. *Commun. ACM* **2004**, *47*, 53–57.
13. Gligor, V.D. Handling new adversaries in wireless ad-hoc networks (transcript of discussion). In *Security Protocols XVI*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6615, pp. 120–125.
14. Wang, Y.; Attebury, G.; Ramamurthy, B. A survey of security issues in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2006**, *8*, 20–23.
15. Alemdar, H.; Ersoy, C. Wireless sensor networks for healthcare: A survey. *Comput. Netw.* **2010**, *54*, 2688–2710.
16. Pathan, A.S.K.; Lee, H.-W.; Hong, C.S. Security in wireless sensor networks: Issues and challenges. In Proceedings of the 8th International Conference on Advanced Communication Technology, Pyeongchang, Korea, 20–22 February 2006; Volume 2.
17. Raymond, D.R.; Midkiff, S.F. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Comput.* **2008**, *7*, 74–81.

18. Ferraiolo, D.F.; Kuhn, D.R. Role-based access controls. In Proceedings of the 15th National Computer Security Conference, Baltimore, MD, USA, 13–16 October 1992.
19. Sandhu, R.; Munawer, Q. How to do discretionary access control using roles. In Proceedings of the 3rd ACM Workshop on Role-Based Access Control, Fairfax, VA, USA, 22–23 October 1998.
20. Lampson, B. Protection. In Proceedings of the 5th Princeton Conference on Information Sciences and Systems, Princeton, NJ, USA, January 1971.
21. Samarati, P.; Vimercati, S. Access control: Policies, models, and mechanisms. In *Foundation of Security Analysis and Design*; Springer: Berlin Heidelberg, Germany, 2001; Volume 2171, pp. 137–196.
22. Zhao, G.; Chadwick, D.W. On the modeling of bell-lapadula security policies using RBAC. In Proceedings of the 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '08), Washington, DC, USA, 23–25 June 2008; pp. 257–262.
23. Zhu, Y.; Keoh, S.L.; Sloman, M.; Lupu, E.C. A lightweight policy system for body sensor network. *IEEE Trans. Netw. Serv. Manag.* **2009**, *6*, 137–148.
24. Zhu, Y.; Keoh, S.L.; Sloman, M.; Lupu, E.; Zhang, Y.; Dulay, N.; Pryce, N. Finger: An efficient policy system for body sensor networks. In Proceedings of 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Atlanta, GA, USA, 29 September–2 October 2008; pp. 428–433.
25. Morchon, O.G.; Wehrle, K. Efficient and context-aware access control for pervasive medical sensor networks. In Proceedings of 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany, 29 March–2 April 2010.
26. Ferreria, A.; Correia, R.; Monterio, H.; Brito, M.; Antunes, L. Usable access control policy and model for healthcare. In Proceedings of 2011 24th International Symposium on Computer-Based Medical Systems (CBMS), Bristol, UK, 27–30 June 2011; pp. 1–6.
27. Ghani, N.A.; Selamat, H.; Sidek, Z.M. Analysis of existing privacy-aware access control for e-commerce application. *Glob. J. Comput. Sci. Technol.* **2012**, *12*, 1–5.
28. Al-Hamdani, W.A. Cryptography based access control in healthcare web systems. In Proceedings of 2010 Information Security Curriculum Development Conference (InfoSecCD '10), Kennesaw, GA, USA, 1–3 October 2010; pp. 66–79.
29. Yu, S.; Ren, K.; Lou, K. Fdac: Toward fine-grained distributed data access control in wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **2011**, *22*, 673–686.
30. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1983**, *26*, 96–99.
31. Malan, D.J.; Welsh, M.; Smith, M.D. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, CA, USA, 4–7 October 2004.
32. Boneh, D.; Gentry, C.; Waters, B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Proceedings of the 25th annual international conference on Advances in Cryptology (CRYPTO'05), Berlin/Heidelberg, Germany, 20–24 August 2005; pp. 258–275.

33. Gaubatz, G.; Kaps, J.-P.; Sunar, B. Public key cryptography in sensor networks—Revisited. In *Security in Ad-hoc and Sensor Networks*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 2–18.
34. Gura, N.; Patel, A.; Wander, A.; Eberle, H.; Shantz, S.C. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In *Cryptographic Hardware and Embedded Systems—CHES 2004*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 119–132.
35. Wander, A.S.; Gura, N.; Eberle, H.; Gupta, V.; Shantz, S.C. Energy analysis of public-key cryptography for wireless sensor networks. In Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (PERCOM '05), Kauai Island, HI, USA, 8–12 March 2005; pp. 324–328.
36. Zhou, Y.; Zhang, Y.; Fang, Y. Access control in wireless sensor networks. *Ad Hoc Netw.* **2007**, *5*, 3–13.
37. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.
38. Gentry, C. *Handbook of information Security*; John Wiley and Sons: Bakersfield, CA, USA, 2006.
39. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy, Washington, DC, USA, 20–23 May 2007; pp. 321–334.
40. Li, J.; Zhao, G.; Chen, X.; Xie, D.; Rong, C.; Li, W.; Tang, L.; Tang, Y. Fine-grained data access control systems with user accountability in cloud computing. In Proceedings of IEEE 2nd International Conference on Cloud Computing Technology and Science, Indianapolis, IN, USA, 30 November 2010.
41. Ruj, S.; Nayak, A.; Stojmenovic, I. Distributed fine-grained access control in wireless sensor networks. In Proceedings of 2011 IEEE International Parallel and Distributed Processing Symposium (IPDPS), Anchorage, AK, USA, 16–20 May 2011; pp. 352–362.
42. Chase, M.; Chow, S.S.M. Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009.
43. Hur, J. Fine-grained data access control for distributed sensor networks. *Wirel. Netw.* **2011**, *17*, 1235–1249.
44. Ye, F.; Luo, H.; Cheng, J.; Lu, S.; Zhang, L. A two-tier data dissemination model for large-scale wireless sensor networks. In Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02), Atlanta, Georgia, USA, 23–28 September 2002; pp. 148–159.
45. Maw, H.; Xiao, H.; Christianson, B. An adaptive access control model for medical data in wireless sensor networks. In Proceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom) (IEEE Healthcom 2013), Lisbon, Portugal, 9–12 October 2013.

46. Maw, H.A.; Xiao, H.; Christianson, B. An adaptive access control model with privileges overriding and behaviour monitoring in wireless sensor networks. In Proceedings of the 8th ACM International Symposium on QoS and Security for Wireless and Mobile Networks 2012 (ACM Q2SWinet 2012), Paphos, Cyprus, 24–25 October 2012.
47. Wang, H.; Sheng, B.; Li, Q. Elliptic curve cryptography based access control in sensor networks. *Int. J. Secur. Netw.* **2006**, *1*, 127–137.
48. Al-mahmud, A.; Morogan, M.C. Identity-based authentication and access control in wireless sensor networks. *Int. J. Comput. Appl.* **2012**, *41*, 18–24.
49. Shamir, A. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1985; Volume 196, pp. 47–53.
50. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63.
51. Wang, Y.; Wong, D.S.; Huang, L. A one-pass key establishment protocol for anonymous wireless roaming with PFS. In Proceedings of 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–5.
52. Zhang, R.; Zhang, Y.; Ren, K. DP2AC: 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 and Communications Societies (INFOCOM 2009), Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1251–1259.
53. He, D.; Bu, J.; Zhu, S.; Chan, S. Chen, C. Distributed access control with privacy support in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 3472–3481.
54. Radu, C.; Govaerts, R.; Vandewalle, J. A restrictive blind signature scheme with applications to electronic cash. In Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security II, Essen, Germany, 23–24 September 1996; pp. 196–207.
55. Li, M.; Lou, W.; Ren, K. Data security and privacy in wireless body area networks. *Wirel. Commun.* **2010**, *17*, 51–58.
56. Bender, A.; Katz, J.; Morselli, R. Ring signatures: Stronger definitions, and constructions without random oracles. *J. Cryptol.* **2008**, *22*, 114–138.
57. Perrig, A.; Szewczyk, R.; Wen, V.; Culler, D.; Tygar, J.D. Spins: Security protocols for sensor networks. *Wirel. Netw.* **2001**, *8*, 189–199.
58. Boneh, D.; Waters, B. *Constrained Pseudorandom Functions and Their Applications*. Cryptology ePrint Archive; Report 2013/352; Springer: Berlin/Heidelberg, Germany, 2013.
59. Mohammad, A.; Khdour, T.; Kanaan, G.; Kanaan, R. Ahmad, S.B. Analysis of existing access control models from web services applications' perspective. *J. Comput.* **2011**, *3*, 10–16.
60. Sahafizadeh, E.; Parsa, S. Survey on access control models. In Proceedings of 2nd International Conference on Future Computer and Communication, Wuhan, China, 21–24 May 2010.
61. Twidle, K.; Dulay, N.; Lupu, E.; Sloman, M. Ponder2: A Policy System for Autonomous Pervasive Environments. Available online: http://http://pubs.doc.ic.ac.uk/ponder2-policy-pervasive/ponder2-policy-pervasive.pdf. (accessed on 9 May 2012).

62. Liu, A.; Ning, P. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In Proceedings of 2008 International Conference on Information Processing in Sensor Networks, St. Louis, MO, USA, 22–24 April 2008; pp. 245–256.
63. Skipjack and KEA Algorithm Specifications. Available online: http://csrc.nist.gov/encryption/skipjack-kea.htm (accessed on 13 May 2013).