A Cluster-Based Multilevel Security Model for Wireless Sensor Networks

Chao Lee, Lihua Yin, Yunchuan Guo

A Cluster-based Multilevel Security Model for Wireless Sensor Networks

Chao Lee[1,2] and Lihua Yin[2] Yunchuan Guo[3]

[1] Institute of Computing Technology,Chinese Academy of Sciences
Beijing, China
lichao@software.ict.ac.cn
[2] Graduate University of Chinese Academy of Sciences
Beijing, China
[3] Institute of Information Engineering,Chinese Academy of Sciences
Beijing, China

Abstract. Wireless sensor network is one of the fundamental components of the Internet of Things. With the growing use of wireless sensor networks in commercial and military, data security is a critical problem in these applications. Considerable security works have been studied. However, the majority of these works based on the scenarios that the sensitivities of data in the networks are in the same. In this paper, we present a cluster-based multilevel security model that enforces information flow from low security level to high security level. The design of the model is motivated by the observation that sensor nodes in numerous applications have different security clearances. In these scenarios, it is not enough for just protecting the data at a single level. The multilevel security mechanism is needed to prevent the information flow from high level nodes to low level nodes. We give the formal description of the model and present a scheme to achieve it. In our model, sensor nodes are grouped into different clusters. In each cluster, the security clearance of sensor nodes must not be higher than the security clearance of the cluster head. We use cryptography techniques to enforce the information flow policy of this model. The higher level nodes can derive the keys of lower level nodes and use the derived key to get the information from lower-level nodes. *abstract* environment.

Keywords: wireless sensor network, multilevel security, information flow control

1 Introduction

The Internet of Things has trended to growing use in commercial and military areas. It has been paid more and more attentions[1, 2]. Wireless sensor network (WSN) is one of the fundamental components of the Internet of Things, which has attractive many researchers[3]. A typical wireless sensor network is composed of a large number of sensor nodes and one or several base stations, which

are used to collect data from the sensor nodes. The base station broadcasts control messages to engage sensor nodes to do some specific tasks. In response, the sensor nodes send back the collected data to the base station. They use radio frequency channels to broadcast messages for communication. Since the communication among sensors is via radio, which is exposed in the air, wireless sensor networks are highly vulnerable to security attacks. Security requirements for sensor networks have attractive many attentions[4–6]. However, the majority of these works are designed to provide uniform security across the network, which means that all the sensor nodes and information have the same security clearance and sensitivity. There are various scenarios that sensor nodes in WSNs play different security levels. For example, in a wireless sensor network operating in a battlefield, the data collected by platoon leader node can be read by battalion commander node but cannot be read by soldiers. The command broadcasted to all battalion commander nodes can be received by the nodes whose security clearances are higher than battalion commander, but can never be received by the nodes whose clearances are lower than it. Take metropolitan surveillance application as another example, the police can see all data, but citizens can only see a subset of the data. This type of applications with multiple priority groups demands different layers of sensed data and multilevel security model in sensor networks. This motivation is the main reason to develop multilevel security in WSNs.

In this paper, we propose a cluster-based multilevel security model to address the problem, in which all sensor nodes and cluster heads have different security clearances. The WSN is modeled as a tree, in which the base station is the root, and each cluster is the subtree. In each cluster, the security clearances of all nodes are lower than the clearance of the cluster head, and the clearances of nodes are decreased from the root to leaf. In our model, each information has a classification, and only the nodes whose clearance is higher than the classification can read and relay the information. We give the formal description of the model and achieve the prototype of it.

To achieve this model, we present a scheme to build the multilevel topology in each cluster, and a multilevel key computation scheme to enforce the information flow control. In this model, each node belongs to different security level. The cluster head election algorithm is used to elect cluster heads with different security levels. The key computation process is initialized by the base station. It computes the keys of all cluster heads according to the clearance of each cluster head. And the key of a sensor node in a cluster is based on the cluster head key and the sensor node's clearances. In other words, the keys are clearance-related. If an upper-level node S_H wants to read an information which flows from a lower-level node S_L and the information is encrypted by the key of S_L, then S_H must have the ability to derive the key of S_L from its own key to decrypt the information.

The rest of this paper is organized as follows: Section 2 presents the related work. In section 3, we describe the systems containing multiple sensitive data and users with different access privilege. Our proposed multilevel security model is

described in Section 4. Section 5 provides the achievement scheme of the model. Section 6 discusses our proposed scheme. Finally, the conclusion can be found in Section 7.

2 Related Work

In the past, the research of multilevel security (MLS) has mainly focused on operating systems, programs, and wired computer networks. For example, In [7], Bell and La Padula proposed the classical BLP model for operating system multilevel access control. In [8], Lu and Sundareshan proposed a model to describe the mechanism that enforces the security policy and requirements for computer network. In [9], Winjum and Berg described a MLS scheme for computer network routing information. Very recently, however, multilevel security communication in wireless sensor networks have begun to attract the attentions. In [10], Teng proposed a multi-layer encryption(MLE) scheme for multilevel access control in wireless sensor networks. In this work, users with different security clearance are assigned different group keys. Lower level users' key are computed by an one-way hash function from the keys of higher level users. However, the scheme doesn't enforce the information flow from low-security to high-security in networks. In [11], Panja proposed a scheme called role-based access in sensor networks which provides role-based multilevel security in sensor networks. Each group is organized in such a way that they can have different roles based on the context and thus can provide different levels of accesses. They organized the network using Hasse diagram then compute the key for each individual node and extend it further to construct the key for a group. In [12], Lee and Singhal introduced the concept of multiple security levels (MSL), which segregates different security levels by using a different computing infrastructure. They proposed an architecture to achieve the MLS property based on MSL concept. They divided the network to several domains and guards. A security domain is a discrete network consisting of a set of nodes having the same security level. The guards monitor and control the information flows among different security domains. However, their scheme assumes that all the same security level nodes can join the same group without the consideration of the communication range.

3 System Description

Before we describe the WSN with different access privilege, let us give the definitions of some terms.

- *Security Class*: Security class is a sensitivity level of an entity (e.g. UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET). Let SC denote the set of security classes, which corresponds to a set of disjoint classes of sensitivity level.$SC = \{L_1, L_2, \ldots L_n\}$,where n is a finite integer.
- *Dominate Relation*: We denote $L_i \succeq L_j$ to say that the security class L_i dominates(or covers) L_j. $L_i \preceq L_j$ holds whenever $L_j \succeq L_i$. We then define the relation $\succ$ by $L_i \succ L_j \Leftrightarrow L_i \succeq L_j \wedge \nexists L_k \in SC. L_i \succeq L_k \succeq L_j$.

- *Clearance*: Clearance is the degree of trust associated with a subject. We define the clearance of a subject s is $CL(s) = [L_i, L_j] \in SC \times SC$, where $L_j \succeq L_i$, which means that s can read information at class L_j or lower, and write information at class L_i or higher. We denote $CL_{\perp}(s) = L_i$ and $CL_{\top}(s) = L_j$.
- *Classification*: Classification is a security class assigned to an object which specifies the sensitivity of the object. We denote $CF(o) = L_i \in SC$ as the classification of o.

In our model, we assume the WSNs consisting of sensor nodes, cluster heads and base station. Sensor nodes, which are grouped into clusters, probe the environment to track the target, and then send the collected data to the cluster heads. Each sensor has limited resources and short radio transmission range. If some of them have more than one hop from the cluster, they send their data to relaying nodes in the cluster and finally communicate with the cluster head. Cluster heads have more resources than sensors. They can execute relatively complicated numerical operations than sensors and have much larger radio transmission range than sensor nodes. Each cluster head is assumed to be reachable to all sensors in its cluster. Cluster heads can communicate each other directly and relay data between its cluster members and the base station.

In the system, we consider two modes. One is data collection, and the other is command distribution. A login user gets the collected data or distributes command via the base station. Each node and user have security clearances $[L_i, L_j]$. Any information transmitted over the WSN must be designated a security classification L_k where $L_i \preceq L_k \preceq L_j$ according to the sensor's task. For example, a sensor whose clearance is $[soldier, soldier]$ can just generate information of *soldier* classification, while a sensor whose clearance is $[soldier, platoon\_commander]$ can generate information of *soldier* or *platoon_commander* according to the task or the collected data sensitivity. In the data collection mode, if the information collected by a sensor node is designated the classification *platoon_commander*, only the nodes whose clearances dominant the classification *platoon_commander* can get and relay the information, the login user on the base station whose clearance cover *platoon_commander* can read the data. In the distribution mode, a battalion commander whose clearance is $[soldier, battalion\_commander]$ wants to distribute a command to all platoon commanders, the command is designated the classification of *platoon_commander*, only the sensor whose clearance dominant *platoon_commander* can receive the command, but all the *soldier* nodes cannot get the information. In the system, the information transmitted over the network can only be allowed to send to the node whose security level is equal or higher than with information classification. We assume appropriate network communication protocols designed to ensure reliable information transmission across the network.

4 A Multilevel Security Model for WSN

We first give the definition of *information flow relation*.

Definition 1 (Information Flow Relation) *For subjects $S', S'' \in S$, and information $i \in O$. $S' \overset{i}{\rightsquigarrow} S''$ defines information i can flow from S' to S''. The information flow relation $\rightsquigarrow$ is defined as follows:*

$$S' \overset{i}{\rightsquigarrow} S'' \Leftrightarrow CL_{\perp}(S') \preceq CF(i) \preceq CL_{\top}(S'')$$

For example, in a cluster, there are two sensors S' and S''. The clearance of S' is $[soldier, soldier]$. Similarly, the clearance of S'' is $[soldier, commander]$. S' can send information with *soldier* classification to S''.

To build the multilevel security cluster, we present *completely dominate relation.*

Definition 2 (Completely Dominate Relation) *For two sensors $S', S'' \in S$, we say $CL(S'')$* completely dominate *$CL(S')$ if and only if $CL_{\top}(S') \preceq CL_{\top}(S'') \wedge CL_{\perp}(S') \preceq CL_{\perp}(S'')$. We denote it $CL(S') \trianglelefteq CL(S'')$.*

Proposition 1 *$\trianglelefteq$ is a partial ordering relation.*

Proof. It easy to see that $\trianglelefteq$ is reflexive and antisymmetric. Below we just proof that $\trianglelefteq$ is transitive. Assume $[L_i, L_j] \trianglelefteq [L_m, L_n]$ and $[L_m, L_n] \trianglelefteq [L_r, L_s]$, according to Definition 2, we have $L_i \preceq L_m$, $L_j \preceq L_n$, $L_m \preceq L_r$ and $L_n \preceq L_s$. Since $\preceq$ is transitive, we can get $L_i \preceq L_r$ and $L_j \preceq L_s$. So $[L_i, L_j] \trianglelefteq [L_r, L_s]$, $\trianglelefteq$ is transitive. Therefore $\trianglelefteq$ is a partial ordering relation.

In our model, we represent each cluster by a tree $T(V, E)$, where V represents a set of sensors and E represents a set of communication links. Each node is denoted by $(ID, CL(ID))$.

Definition 3 (Multilevel Security Cluster) *We define a multilevel security cluster as tuples*

$$MLSC = (CH, S, CL, \trianglelefteq)$$

where CH is the cluster head. S is the set of sensor nodes (members) contained in the cluster. CL is clearance of subjects. $\trianglelefteq$ is the completely dominate relation. A cluster is a multilevel security cluster if and only if:

(1) For $\forall S', S'' \in S$, $S'.parentID = x, S'.parentID = y \Rightarrow x = y$.
(2) $S'.parentID = S''.ID \Rightarrow CL(S') \trianglelefteq CL(S'')$.

We denote the set of multilevel security cluster by MSLCs.

The Condition (1) points out that a sensor node only has a unique parent node, as only one next-hop node to be allowed from lower level to upper level. When a node S' joining a cluster, if there are more than one nodes S_i, S_j,...,S_m, and $S' \trianglelefteq S_i$, $S' \trianglelefteq S_j$, ..., $S' \trianglelefteq S_m$, then S' chooses the closest one to be its parent. The Condition (2) can ensure the secure information flow.

Lemma 1 *In a multilevel security cluster, $S', S'' \in S$ are two sensors, and S'' is the parent of S':*

(1) In the data collection mode, information i can flow from S' to S'' all the time.
(2) In the command distribution mode, information i can flow from S'' to S' only when $CF(i) \preceq CL_{\top}(S')$.

Proof. In a multilevel security cluster, there must be $CL(S') \trianglelefteq CL(S'')$. That is $CL_{\perp}(S') \preceq CL_{\perp}(S'') \wedge CL_{\top}(S') \preceq CL_{\top}(S'')$. In the data collecting mode, information i is generated by S', so $CL_{\perp}(S') \preceq CF(i) \preceq CL_{\top}(S')$. We can easily get $CL_{\perp}(S') \preceq CF(i) \preceq CL_{\top}(S'')$. According to Defintion 1, i can flow S' to S'' all the time. In the command distribution mode, we can get $CL_{\perp}(S'') \preceq CF(i) \preceq CL_{\top}(S'')$. If $CF(i) \preceq CL_{\top}(S')$, and $CL(S') \trianglelefteq CL(S'')$, then $CL_{\perp}(S'') \preceq CF(i) \preceq CL_{\top}(S'')$, i can flow S'' to S'. Otherwise, the flow is prevented.

Definition 4 (Cluster-based Multilevel Security Model for WSN) *The WSN cluster-based multilevel security model is defined by*

$$\text{WSN-CMLSM} = (MSLCs, BS, U, P, I, \rightsquigarrow)$$

where

- *$MSLCs$ is the set of multilevel security clusters.*
- *BS is the base station. All the $C \in MSLCs$ connect to BS.*
- *U is the set of users. Each login user whose clearance is $[L_i, L_j]$ can read collected data whose classification is not higher than L_j, and write distribution command with classification not lower than L_i.*
- *P is the security policy $(SC, \preceq)$, which is defined by a lattice.*
- *I is the information transmitted over the WSN.*
- *$\rightsquigarrow$ is the information flow relation.*

In Figure 1, we illustrate an example of our scheme. The topology of the network is generated by the method in Section 5.

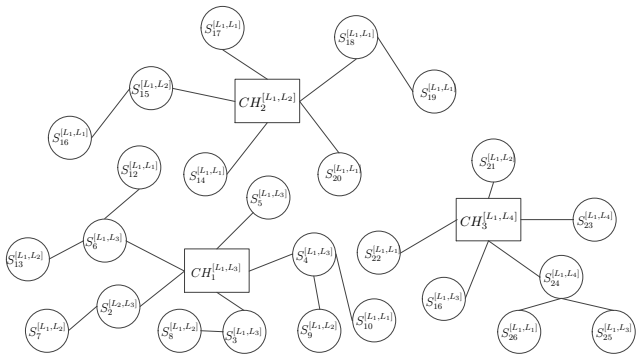


Fig. 1. Cluster-based multilevel security model exmamle

Let $S_i^{[L_i,L_j]}$ denote a sensor node i with the clearance $[L_i, L_j]$. For example, $S_1^{[L_1,L_2]}$ denotes sensor node 1 whose clearance is $[L_1, L_2]$, and $S_2^{[L_1,L_3]}$ presents a node whose identity is 2 and clearance is $[L_1, L_3]$.

If the node $S_8^{[L_1,L_2]}$ sends the data d_1 to the cluster head $CH_1^{[L_1,L_3]}$, it transmits the data through the path $S_8^{[L_1,L_2]} \rightarrow S_3^{[L_1,L_3]} \rightarrow CH_1^{[L_1,L_3]}$.(We will give the scheme of generating it in section 5).

Proposition 2 *The information flow in the WSN-CMLSM is secure.*

Proof. According to Lemma 1, we can easily prove it. Because of space constraint, we omit the details.

5 A Scheme to achieve the multilevel model

We proposed a scheme to provide multilevel security for wireless sensor networks. The scheme consists of two parts. We first organized the sensors as a cluster-based multilevel security topology. And then the hierarchical keys on the topology are computed to enforce the information flow from low to high.

5.1 Multilevel Security Clusters Building

Each sensor node performs Algorithm 1 to build the multilevel security clusters. It takes as input $Range(S_i, CHs)$ and $Range(S_i, S)$, which means the cluster heads and sensor nodes in the communication range of S_i respectively. It outputs the routing information of S_i. In the algorithm, we assume that each sensor can detect the sensors and cluster heads in its communication range. It choose the nearest cluster head which satisfies the $CL(S_i) \preceq CL(CH)$ to the parent node. If it not exists the satisfied cluster head, the sensor node choose the nearest node which meets $CL(S_i) \preceq CL(S')$ to the parent node. The detail is shown in Algorithm 1.

5.2 Key computation scheme

We presente a key computation scheme to enforce the information flow policy discussed in Section 4.

One way of implementing such a policy is to encrypt the data with security classification $L_i \in SC$ with key K_{L_i}. And the easiest way of the key management is to hold all the security classification related keys of its direct or indirect child nodes. However, when the hierarchy is large, it is difficult for node to store all the keys. So we utilize *dependent keys management* approach to achieve the multilevel security policy.

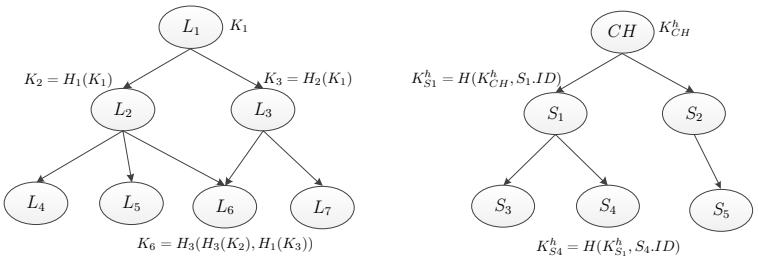
Algorithm 1: Multilevel security clusters building algorithm

Data: $Range(S_i, CHs)$,$Range(S_i, S)$
Result: $S_i.parentID$

```
1  begin
2      if Range(S_i, CHs) ≠ ∅ then
3          foreach CH ∈ Range(S_i, CHs) do
4              if CL(S_i) ⊴ CL(CH) then
5                  Set_Candidate_CH ← CH;
6              end
7          end
8          if Set_Candidate_CH ≠ ∅ then
9              Chosen_CH = Nearest(Set_Candidate_CH);
10             S_i.parentID = Chosen_CH.ID;
11         end
12     end
13     else
14         foreach S' ∈ Range(S_i, S) do
15             if CL(S_i) ⊴ CL(S') then
16                 Set_Candidate_Node ← S';
17                 Chosen_Node = Nearest(Set_Candidate_Node);
18                 S_i.parentID = Chosen_Node.ID;
19             end
20         end
21     end
22 end
```

Cluster head key computation The keys of cluster heads are computed in the base station. Assume the base station has the knowledge of the relation of security class before the WSN deployment is reasonable. $(SC, \preceq)$ are organized as a lattice. Each security class has many direct successors and predecessors. The base station uses one-way functions $H_1, H_2, \ldots H_m$ to compute the dependent keys, where m is the maximum number of children per node. If a security class L_j is directly covered by L_i whose key is K_i; and if L_j is the kth child of L_i, then $K_j = H_k(K_i)$. Moreover, if L_j has more than one direct parents $L_j^1, L_j^2, \ldots, L_j^m$, where L_j is the c_1th,$\ldots$, c_mth child of the parent $L_j^1, L_j^2, \ldots, L_j^m$, then $K_j = H_{c_1}(H_{c_1}(K_{L_j^1}), H_{c_2}(K_{L_j^2}), \ldots, H_{c_m}(K_{L_j^m}))$. According to the scheme, the key belongs to high security class can derived from the key of low security class. The key of L_i is denoted by K_{L_i}.Take Figure 2(a) as an example, let K_i is the key of L_i, where $1 \leq i \leq 7$, then we can compute $K_2 = H_1(K_1)$, $K_3 = H_2(K_1)$, $K_6 = H_3(H_3(K_2), H_1(K_3))$.

Sensor node key computation Since in each cluster, the sensor nodes are organized as a tree not a lattice, and the above cluster head key computation scheme is too energy consuming for sensor nodes, we compute the sensor node key as follows:



(a) security class key example (b) sensor node key example

Fig. 2. Key computation scheme examples

1. Each node S_i computes the hierarchical key through a one-way hash function $K^h_{S_i} = H(K^h_{S_i.parent}, S_i.ID)$.
   Take Figure 2(b) as an example, $K^h_{S_4}$ can be computed from $K^h_{S_3}$ via $K^h_{S4} = H(K^h_{S_1}, S_4.ID)$.
2. In [13], Blundo et al, establish pair-wise keystone using a bivariate t-degree polynomial $f(x,y) = \sum_{i,j=0}^{t} a_{ij}x^i y^j$, which has the property of $f(x,y) = f(y,x)$.For example, node S' and S'' compute the symmetric key to secure communication. let i and j are the ID of S' and S'' respectively. Node S' have $f(i,y)$, and it computes the key $f(i,j)$ to communicate with node S''. Node S'' can derive $f(j,i)$ through $f(j,y)$.
   The sensor node computes the communication key by $K^c_{S'} = K^h_{S'} \oplus f(S'.ID, y)$, where f is the polynomial in [13], y is the IDs of the nodes that connected to S'.

When sensor node S' sends the data to the cluster head. It encrypts the data by $K^c_{S'}$, and sends to its parent S''. S'' can compute the $K^c_{S'}$ through $f(S''.ID, S'.ID)$ and $K^h_{S'} = H(K^h_{S''}, S'.ID)$. S'' can get the information of S', and it forwards the message to its parent.

6 Theoretical analysis

Theorem 3 *For security class L_i and L_j, if $L_i \preceq L_j$, then K_{L_i} can be derived from K_{L_j}.*

Proof. Assume $L_m, L_n, \cdots, L_r, L_s$ are between L_i and L_j, we can easily get $K_{L_m} = H(K_{L_i}), K_{L_n} = H(K_{L_m}), K_{L_{n+1}} = H(K_{L_n}), \cdots, K_{L_s} = H(K_{L_r})$, so $K_{L_j} = H(H(H(...H(K_i)...)))$. Therefore, if $L_i \preceq L_j$, K_{L_j} can derive K_{L_i}.

Proposition 4 *Information M is transited over the WSN, only the sensor node S' satisfied $CF(M) \preceq CL_{\top}(S')$ can get the information.*

Proof. The information M ($CF(M) = L_m$) is encrypted by K_{L_m}. When the information from the base station to sensors, only the cluster head satisfied

$L_k \preceq CL_\top(CH)$ can get the information, as K_{CH} can derive from K_{L_m} according to Theorem 3. The other cluster heads cannot get the information because of their inability to compute K_{L_m}. The cluster heads satisfied $L_m \preceq CL_\top(CH)$ send the information to their members. Since in MLSC, any sensor node S satisfies $CL(S) \trianglelefteq CL(S.parent)$ and the hierarchical key is computed by the topology, if $CF(M) \preceq CL_\top(S')$,$S'$ can derive K_{L_m} from $K^h_{S'}$. Therefore, S' can get the information of M. When the information is from the sensor to the base station, assume M is generated by a node S. In MLSC, the sensor's next hop must satisfy $CL(S') \trianglelefteq CL(S'.parent)$, so M can only send through the path $CF(M) \preceq CL_\top(S')$, according to Theorem 3, the sensors can derive K_{L_m}. the node $CF(M) \npreceq CL_\top(S')$ is not on the routing path of M, and the K_{L_m} cannot be derived, so only the sensor node S' satisfied $CF(M) \preceq CL_\top(S')$ can get the information.

Because of space constraint, the details of simulation will be presented in a separate paper.

7 Summary

In this paper, we proposed a cluster-based multilevel security model for wireless sensor networks. We divided the sensors in different clusters and modeled each cluster as a tree. In each cluster, the clearance of the cluster head completely dominated its member's clearance. Each sensor node has a unique parent, and the clearance of the node is completely dominated by its parent. The information flow policy is proposed to ensure the information flow low level to high level. We present a scheme to achieve it. In our scheme, cryptographic technologies are employed to enforce the information flow policy. The high level node can derive keys of the low level nodes, while the low-level node cannot derive keys of the high level nodes. Therefore, information can only flow from low to high that satisfies the requirement of the scenarios that the sensor nodes have different sensitivities.

Acknowledgment

This research is supported by the National High Technology Research and Development Program of China (863 Program) (2009AA01Z438), and the National Natural Science Foundation of China (61070186,61100186)

References

1. Atzori, L., Iera, A. and Morabito, G.:The Internet of Things: A survey. Computer Networks.54,2787–2805(2010).
2. Weber, R. H.:Internet of Things C New security and privacy challenges.Computer Law & Security Review.26,23–30(2010).

3. Zhao, F. and Guibas, L.J.:Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann,San Francisco(2004).
4. Wang, Y., Attebury, G and Ramamurthy, B.: A survey of security issues in wireless sensor networks.IEEE Communications Surveys and Tutorials.8,2–23(2006).
5. Xiao, Y., Rayi, V. K.,Sun, B.,Du, X., and Hu, F. and Galloway, M: A survey of key management schemes in wireless sensor networks.Computer Communications.30,2314–2341(2007).
6. Jr, Marcos A. Simplicio , Barreto, Paulo S.L.M., Margi, Cintia B., and Carvalho, Tereza C.M.B.:A Survey on Key Management Mechanisms for Distributed Wireless Sensor Networks.Computer Networks.54(15),2591–2612(2010).
7. Bell, D. E. and LaPadula, Leonard J.: Secure computer systems: mathematical foundations and model.Technical Report M74-244, MTR (1973).
8. Lu, W.-P. and Sundareshan, M.K.:A Model for Multilevel Security in Computer Networks. IEEE Trans. Softw. Eng.16(6),647–659(1990).
9. Winjum, E. and Berg, T.J.:Multilevel security for ip routing. In:Military Communications Conference 2008, pp 1–8.IEEE Press, New York(2008).
10. Teng, Po-Yuan, Huang, Shih-I, and Perrig, Adrian.:Multi-layer Encryption for Multi-level Access Control in Wireless Sensor Networks.In:Proceedings of The IFIP TC 11 23rd International Information Security Conference. pp 705–709(2008).
11. Panja, Biswajit, Madria, Sanjay Kumar, and Bhargava, Bharat:A Role-based Access in a Hierarchical Sensor Network Architecture to Provide Multilevel Security.Comput. Commun, 31:793–806 (2008).
12. Lee, Jongdeog, Son, S.H., and Singhal, M.:Design of an Architecture For Multiple Security Levels in Wireless Sensor Networks.In:7th International Conference on Networked Sensing Systems (INSS), pp 107–114.IEEE Press, New York(2010).
13. Blundo, Carlo, Santis, Alfredo De, Herzberg, Amir, Kutten, Shay, Vaccaro, Ugo, and Yung, Moti.:Perfectly-secure key distribution for dynamic conferences.In: 12th Annual International Cryptology Conference on Advances in Cryptology, pp 471–486, London, UK. Springer-Verlag (1993).