# Poster: A Multilevel Security Model for Wireless Sensor Networks

Chao Lee(Student)
*Institute of Computing Technology*
*Chinese Academy of Sciences*
*Graduate University of Chinese Academy of Sciences*
*Beijing, China*
*lichao@software.ict.ac.cn*

Li-Hua Yin(Faculty), Yun-Chuan Guo(Faculty)
*Institute of Information Engineering*
*Chinese Academy of Sciences*
*Beijing, China*
{*yinlihua,guoyunchuan*}*@software.ict.ac.cn*

***Abstract*—In wireless sensor networks, 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. In this paper, we present a cluster-based multilevel security model that enforces information flow from low-security level nodes to high-security level nodes to prevent information leakage. 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, and if a sensor node has a relay node, the sensor node clearance must be lower than the relay node clearance. 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 get the information using the derived keys.**

***Keywords*-wireless sensor network; multi-level security; access control;**

## I. Introduction

Wireless sensor networks (WSNs) are becoming more widely adopted and implemented to manage data acquisition and communication in wireless areas, which form the basis for a broad spectrum of commercial and military applications. Security requirements for sensor networks have attractive many attentions. 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 (WSN) 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.

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, 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 cluster head election algorithm and a cluster routing algorithm to build the multilevel security topology of WSN, and give a hierarchical key computation scheme to enforce the information flow control.

## II. A Multilevel Security Model for WSN

**Definition 1.** Let $SC$ denote the set of security classes, which corresponds to a set of disjoint classes of sensitivity level.$SC = \{L_1, L_2, \dots L_n\}$,where $n$ is a finite integer.

**Definition 2.** We denote $L_i \succeq L_j$ to say that the security class $L_i$ covers(or dominates) $L_j$. $L_i \preceq L_j$ holds whenever $L_j \succeq L_i$.

For a sensor node $S_i \in S$, $int(S_i) = [L_i, L_j] \in SC \times SC$, where $L_j \succeq L_i$ means that sensor node $S_i$ may sink information at class $L_j$ or lower, and may source information at class $L_i$ or higher. For information $x \in O$, $int(x) = [L, L] \in SC \times SC$, which means that a given information has a unique classification. We write $int(x) = L$ briefly if there's no ambiguous.

**Definition 3.** The WSN cluster-based multilevel security model is defined by $WSN\_CMLSM = (C, I, SC, P)$, where $C$ is the set of clusters, each cluster $C_r$ contains several sensor nodes. For $S_i, S_j, S_k \in C_r, C_r \in C$, $S_i.parent = S_j \wedge S_i.parent = S_k \Rightarrow S_j = S_k$. $I$ is the set of information, $SC$ is the security classes, and $P$ is the information flow policy that

$$S_i.parent = S_j \Leftrightarrow int_\perp(S_i) \preceq int_\perp(S_j) \wedge int_\top(S_i) \preceq int_\top(S_j) \wedge int_\perp(S_i) \preceq int(x) \preceq int_\top(S_j)$$

If an information flow satisfies the policy, we say the information flow is valid.For example, in a cluster, there are two sensors $S_i$ and $S_j$. Sensor $S_i$ is configured to manage *unclass* and *secret* information, and it can be denoted by $int(S_i) = [u, s]$. Similarly, Sensor $S_j$ is set to manage *secret* and *top secret* information, and $int(S_j) = [s, t]$. $S_i$ and $S_j$ communicate with *secret* information. According to the policy, the information flow $S_{is} \to S_{js}$ is valid.

## III. 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.

### A. Cluster-based Multilevel Security Topology

**Step 1: Cluster Head Election**.To build the clusters, we need to choose the cluster heads first. We assume that the approximate percentages of nodes with different security clearances are known. Let $P_{L_i}$ denotes the percentage of nodes with $L_i$ security class. We propose an election algorithm **CHE**$(P_{L_i}, L_i, r)$ adapted from the cluster head election of leach protocol [1], where $r$ is the current round of election. It computes a threshold and a random number ranged in [0,1], if the random number is larger than the threshold, the sensor is marked as cluster head.

$$T(n) = \begin{cases} \frac{P_{L_i} \times p}{1 - P_{L_i} \times p \times (r \ mod \frac{1}{P_{L_i} \times p})}, & \forall n \in G; \\ 0, & \text{otherwise.} \end{cases} \quad \text{(III.1)}$$

**Step 2: Multilevel Security Cluster Building**. After the cluster heads election, each senor node performs the following algorithm, **MSCB**$(Range(S_i, CHs), Range(S_i, S))$. It takes as input $Range(CHs)$ and $Range(S)$, which means the cluster heads and sensor nodes in the communication range of $S_i$ respectively. It outputs the routing information of $S_i$.

If $Range(S_i, CHs) \neq \emptyset$, for each $CH \in Range(S_i, CHs)$,if $int_\perp(S_i) \preceq int_\perp(CH) \wedge int_\top(S_i) \preceq int_\top(CH)$. $Set_{CH} \leftarrow CH$.If $Set_{CH} \neq \emptyset, Chosen\_CH = Nearest(Set_{CH})$, and $S_i.parentID = Chosen\_CH.ID$.

If $Range(S_i, CHs) = \emptyset$, for each $S' \in Range(S_i, S)$, if $int_\perp(S_i) \preceq int_\perp(S') \wedge int_\top(S_i) \preceq int_\top(S')$, $Set_{Node} \leftarrow S'$, $Chosen\_Node = Nearest(Set_{Node})$, and $S.parentID = Chosen\_Node.ID$ ;

### B. Key computation scheme

**Cluster head key computation.** The hierarchical relations of security classifications are organized as a lattice logically. We use 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 $k$th child of $L_i$, then $K_j = H_k(K_i)$. Moreover, if $L_j$ has more than one direct parents $L_j^1, L_j^2, \ldots, L_j^m$, and $L_j$ is the $c_1$th,..., $c_m$th child of the parent $L_j^1, L_j^2, \ldots, L_j^m$ respectively, 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 $K_{L_i}$.

**Sensor node key computation.** In each cluster, the sensor nodes are organized as a tree. In a cluster, the node can only communicate with its successors and predecessors. We compute the sensor node key as follows:

1) Each node $S_i$ computes the hierarchical key through a one-way hash function $K_{S_i}^h = H(K_{S_i.parent}^h, S_i.ID)$
2) The sensor node computes the communication key by $K_{S_i}^c = K_{S_i}^h \oplus f(S.ID, y)$, where $y$ is the IDs of the nodes that connected to $S$, where $f(x, y) = \sum_{i,j=0}^{t} a_{ij} x^i y^j$ is a bivariate t-degree polynomial to establish pair-wise keys [2].

When sensor node $S_i$ sends the collected data to the base station. It encrypts the data by $K_{S_i}^c$, and sends to its parent $S_j$. $S_j$ can compute the $K_{S_i}^c$ through $f(S_j, S_i)$ and $K_{S_i}^h = H(K_{S_j}^h, S_i.ID)$. $S_j$ can get the information of $S_i$, and it forwards the message to its parent.

## IV. Conclusions

We propose a multilevel security model for WSN and implement a prototype of it. The model enforces the information flow from low level to high level, which 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)

## References

[1] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on*, jan. 2000, p. 10 pp. vol.2.

[2] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*. London, UK, UK: Springer-Verlag, 1993, pp. 471–486.