Optimal Deployment Model of Key Pre-distribution Protocol for Heterogeneous Wireless Sensor Networks

Qi Yuan[1,2], Chunguang Ma[1] ⋆, Xiaorui Zhong[3], and Peng Wu[1]

[1] College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
[2] College of Communication and Electronic Engineering, Qiqihar University, Qiqihar 161006, China
[3] China Academy of Electronics and Information Technolgy, Beijing 100041, China
machunguang@hrbeu.edu.cn

Abstract. This work develops an equilibrium model which can find the optimal distribution strategy to maximize performance of key pre-distribution protocols in terms of cost, resilience, connectivity and lifetime. As an essential attribute of wireless sensor networks, heterogeneity and its impacts on random key pre-distribution protocols are first discussed. Using supernetworks theory, the optimal node deployment model is proposed and illustrated. In order to find the equilibrium performance of our model, all optimal performance functions are changed into variational inequalities so that this optimization problem can be solved. A small scale example is presented to illustrate the applicability of our model.

Keywords: Optimization,Key pre-distribution,Supernetworks,Variational inequality

1 Introduction

In wireless sensor networks (WSN), a key pre-distribution protocol (KPP) is usually designed or analyzed under the hypothesis that network is ideal. For instance, all sensors are reachable, climate or environment around different nodes are identical and no unexpected incident will happen, or nodes are uniformly deployed in monitoring region [1–4].Under such ideal assumption, plenty of efficient KPPs have been proposed as shown in references [5–10].However, things are different in reality. For example, a node deployed in a hole may never be reached. Research achievements under ideal assumption cant adapt to practical applications very well, and the reference value of relevant analysis stays low. Hence, its of great interest to consider the differences between nodes or their locations, namely heterogeneity. Actually, studying heterogeneity can help us design network models with more practicality, design protocols with better performance, and to present analysis with more accuracy.

⋆ corresponding author

In fact, heterogeneity is an essential attribute of WSN. Since WSNs consist of sensor nodes, node heterogeneity is the most obvious heterogeneity in WSN. For example, if some nodes have higher energy or longer communication range than others, the whole network is heterogeneous. In addition to node itself,environment around node is another source of heterogeneity. Heterogeneous environment or nodes bring many practical problems for protocol designers. For example, nodes with lower energy will die quickly, and nodes with shorter communication range will rise the communication cost. Usually, heterogeneity will keep on affecting the performance of protocol until the network dies.

Although heterogeneity plays a significant role in WSN in terms of raising security or reducing energy consumption, the research on heterogeneity is still in primary stage and the achievements are far from enough. This happens because that the complexity and dynamic changes make it very hard to describe heterogeneity clearly. This drawback blocked and delayed the development of heterogeneity application. Considering the insufficiency of existing researches and the advantages of heterogeneity in terms of bringing more reality into network model, this paper focus on utilizing heterogeneity to optimize performance of random key pre-distribution protocols, and provide optimal network solutions.

Energy heterogeneity and link heterogeneity were used to choose a better route in Ref. [11]. After that,A further classification of link heterogeneity was depicted in Ref. [12], it proposed a heterogeneous link model to increase the throughput of broadcast communication and decrease the communication latency. Katiyar *et al.* improved a clustering algorithm for WSN by taking advantage of energy heterogeneity to prolong life span of networks.Recently, Chen*et al.* [14] improved a complete hierarchical key management scheme which only utilizes symmetric cryptographic algorithms and low cost operations for heterogeneous cluster-based WSN to assure safety and validity of networks.Obviously, existing researches on heterogeneity are focus on energy and link, and aiming at optimize clustering algorithm, route protocol, public key and so on. But that is not enough. Whether there are other heterogeneities affecting protocols? How to describe the state of whole heterogeneous network and utilize heterogeneity to optimize deployment strategy so that random key pre-distribution protocol will achieve its best performance? This work will focus on finding answers to these questions.

The remainder of this paper is organized as follows: Related works and background knowledge are respectively introduced in Sect. 2. In Sect. 3, various heterogeneities are classified, and an optimization model is proposed too. Five optimization goals and their equivalent variational inequalities are given in Sect. 4. Sect. 5 discusses why, when and how the optimal solution of our model can be found. A numerical example is given and analyzed in Sect. 6. Finally, Sect. 7 concludes this paper.

2 Background Knowledge

2.1 Evaluation Metrics

According to Ref. [5], metrics to measure KPPs can be divided into four types:

- *Connectivity*: the probability of establishing secure links among nodes.
- *Validity*: includes energy validity, time validity, storage validity and computing validity.
- *Scalability*: the maximal network size supported by protocol.
- *Security*: includes confidentiality, authentication, resilience, backward-security, forward-security and integrality.

Among above metrics, energy, cost, connectivity, resilience and scalability are five critical metrics. Since scalability depends on nothing but management strategy (e.g. EG scheme) or key materials (e.g. EBS scheme), it has nothing to do with network. In following research, only the first four metrics are taken into account. Based on that, global optimization goal can be further broken down into four specific goals: minimum cost, minimum energy consumption, maximum connectivity and maximum resilience. Though these optimization goals only cover a part of metrics mentioned above, they could still help us to find a global approximate optimal solution, because that they are four critical factors affecting protocol performance.

2.2 Variational Inequality

Definition 2.1 *A finite-dimensional variational inequality problem VI(F,K) is to find a vector* $\boldsymbol{X}^* \in K$ *satisfying*

$$\langle F(\boldsymbol{X}^*), \boldsymbol{X} - \boldsymbol{X}^* \rangle \geq 0, \forall \boldsymbol{X} \in K$$

where F is a continuous function from K to N dimensional Euclidean space R^N*; K is a closed convex set;* $\langle \cdot, \cdot \rangle$ *represents inner product on* R^N *[15–17].*

The relationship between variational inequality and minimum object function are shown as follows:

Relationship 2.1 *If vector* $\boldsymbol{X}^* \in K$ *is a solution to function* $\min f(\boldsymbol{X})$*, then* $\boldsymbol{X}^*$ *satisfies variational inequality*

$$\langle \bigtriangledown f(\boldsymbol{X}^*), \boldsymbol{X} - \boldsymbol{X}^* \rangle \geq 0, \forall \boldsymbol{X} \in K$$

where K is the feasible solution space, $\bigtriangledown f(\boldsymbol{X}^*)$ *is the gradient of object function* $f(\boldsymbol{X})$*.*

Relationship 2.2 *To solve a optimization problem with constraint set in the form of (1), equals to find vector* $\boldsymbol{X}_i^* \in K_i$ *and* $u_i \geq 0$ *satisfying expression (2) where* $f_i : R^{n_i} \to R$ *is a differentiable convex function;* a_j^T *is a vector which consists of coefficients of the jth constraint condition and* $\boldsymbol{X} = \{\boldsymbol{X}_1, \ldots, \boldsymbol{X}_m\}$ *[15–17].*

$$\begin{cases} \min \sum_{i}^{m} f_i(\boldsymbol{X}_i) \\ a_j^T \boldsymbol{X} \leq b_j, j = 1, \ldots, r \\ \boldsymbol{X}_i \in K_i, i = 1, \ldots, m \end{cases} \tag{1}$$

$$\sum_{i=1}^{m}\langle(\bigtriangledown f_i(\boldsymbol{X}_i^*)+\sum_{j=1}^{r}u_j^*a_{ji})^T,(\boldsymbol{X}_i-\boldsymbol{X}_i^*)\rangle+\sum_{j=1}^{r}(b_j-a_j^T\boldsymbol{X}^*)\times(u_j-u_j^*)\geq 0,$$
$$\forall X_i\in K_i,u_j\geq 0,\forall i,j \tag{2}$$

3 Heterogeneity and Model

3.1 Heterogeneity

There is no exactly homogeneous network exist in reality. Heterogeneity can always be found in WSN. For the purpose of simplifying description, sensor device and environment factors around nodes are named element. One specific node and environment around it are all called element object.

For example, a WSN consists of two MICAz mote nodes, n_1 and n_2, n_1 is deployed on hill, n_2 is deployed underwater, then elements of this WSN include MICAz devices and nodes deployment location, n_1 and n_2 are MICAz device objects, both of hill and underwater are location objects.

Definition 3.1 *Assume that element e has attributes* $(\cdots,a_i,\cdots,a_j,\cdots)$ *and element objects* $(\cdots,b_p,\cdots,b_q,\cdots)$. *The value of attribute* a_i *of element object* b_p *is denoted by* v_i^p. *If* $v_i^p\neq v_i^q$, *attribute* a_i *is called heterogeneous attribute (HA).*

An example is given in Fig. 1. Node objects n_1 and n_2 have different energy, here energy is a heterogeneous attribute of element Node. Such heterogeneity is called energy heterogeneity.

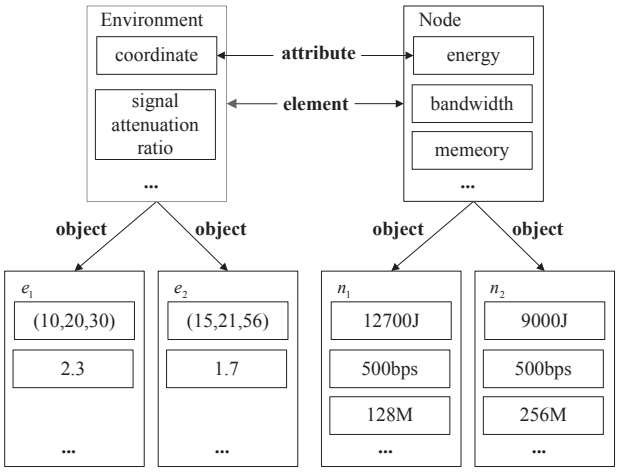

Fig. 1. Relationship among element, attribute and object

Definition 3.2 *Heterogeneity, which is controllable and introduced into networks by human on purpose, is called subjective heterogeneity (SH).*

For example, advanced nodes are introduced for processing and forwarding information while the other normal nodes are used to sense.

Definition 3.3 *Heterogeneity, which is random and uncontrollable, is called objective heterogeneity (OH).*

For example, external geographical environment, location, climate etc. belong to OH. Without manual intervention and control, these heterogeneities still change with time. SH exists in deployment phase, aiming at satisfying special application requirement. As time goes on, SH will finally evolve to OH. Besides, different heterogeneities can be combined together to form several compound heterogeneities which are not mutually exclusive.

Compound heterogeneities affecting KPPs can be conclude into two kinds: node heterogeneity and environment heterogeneity. Node heterogeneity contains all HAs of sensor devices such as energy, communication radius, storage capability, computing capability, bandwidth, etc. Environment heterogeneity contains all heterogeneous environment factors. For example, if different geological location results in different signal attenuation, and finally leads to different communication range, location heterogeneity belongs to environment heterogeneity. Besides, other heterogeneities mentioned in existing researches have been already contained in the two heterogeneities mentioned above. Taking link heterogeneity for example, bandwidth and signal attenuation are both its attribute, but bandwidth heterogeneity belongs to node heterogeneity and signal attenuation heterogeneity belongs to environment heterogeneity. Finally, we discuss the impact of heterogeneities on performance of KPPs. Since different heterogeneity may show same impact, there exists some critical heterogeneity which can replace other ones to generate same impact. Critical heterogeneities involved in this paper and their measurements are shown in Table 1, where RR represents realistic communication radius, and MaxR is the maximum communication radius.

Table 1. Critical Heterogeneities and Their measurements

Symbol	Heterogeneity	Measurement
h_1	node heterogeneity	node type
h_2	communication radius heterogeneity	ratio of RR to MaxR
h_3	density heterogeneity	amount of neighbors

3.2 Deployment Model

As mentioned before, researches have proved that making rational use of heterogeneity can improve performance of KPPs. It is rational to state that when various heterogeneities stay in a certain state, a global optimum performance could be reached. Let $O = \{o_1, \ldots, o_n\}$ and $A = \{a_1, \ldots, a_m\}$ be the object set and the attribute set of element e respectively. For the ith attribute $a_i \in A$ (whose corresponding heterogeneity is h_i), if there are k different attribute values $V_i = \{v_{i,1}, \ldots, v_{i,k}\}$ for all objects, we say that the degree of HA a_i is k, denoted by D_i. We also use HA value distribution (HAVD) to describe how many nodes share the same HA value. The HAVD of a homogenous network is simplest in which all degrees of HAs equal 1. A KPP only has two attributes: key materials and key management tasks. Let t and m be the task set and the key material set respectively, a KPP can be expressed as (t, m).

Based on supernetworks theory [15, 18], given a KPP, n heterogeneities existing in KPP-applied network and corresponding HA values, a optimal HA value distribution model (OVDM) can be designed as shown in Fig. 2. It illustrates what kind of HAVD is needed to achieve optimal performance of the chosen KPP (t, m).

In Fig. 2, h_i denotes the ith heterogeneity affecting KPP, and its corresponding attribute is a_i. $h_1 \sim h_3$ remain consistent with Table 1. Marked circles represent specific attribute value, task or material. Taking h_1 for example, its degree of HA is D_1, so there are D_1 circles marked from 1 to D_1, $v_{1,i}(1 \leq i \leq D_1)$ represents ith-level and illustrated by circle i. The weight of each arrow from circles of h_1 to circles of $h_j(1 < j \leq n)$ represents the number of $v_{1,i}$th-level $(1 \leq i \leq D_1)$ node, whose value of $a_j(1 < j \leq n)$ equals $v_{j,k}(1 \leq k \leq D_j, 1 < j \leq n)$ when the best protocol performance is achieved. Let $A \mapsto B$ be the arrow from circle A to B. If $B = v_{i,p}(i \neq 1)$, $A = v_{1,q}$, the edge weight of $A \mapsto B$, which represents the number of nodes, is also called the contribution of $v_{1,q}$th-level nodes to HA value $v_{i,p}$. More precisely, the contribution of $v_{1,1} \mapsto v_{2,1}$ is equal to the number of 1-level nodes whose communication radius is $v_{2,1}$.

4 Equilibrium Optimization Model

In this section, we give five objective functions of KPP optimization. In order to solve multi-objective equilibrium optimization problemthese objective functions are all converted into equivalent variational inequalities.

4.1 Optimal Cost

The cost of a KPP contains two parts: device cost and deployment cost. The former one can be further divided into software cost and hardware cost. Let f_i be the device cost function. Given the unit price of nodes and the number of the ith kind of nodes n_i, f_i is a function of n_i, namely

$$f_i = f_i(n_i), 0 \leq n_i \tag{3}$$

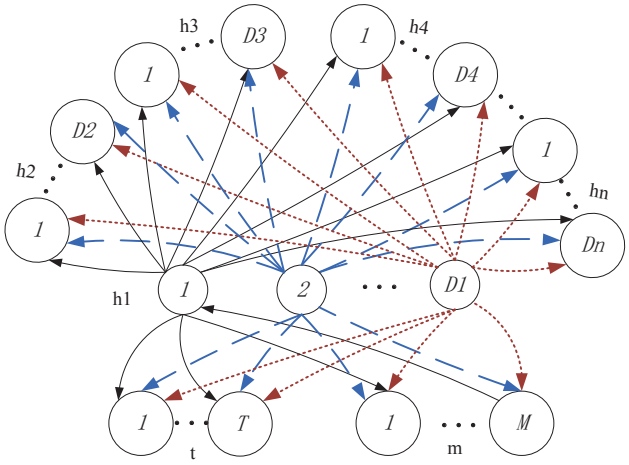

Fig. 2. OVDM of KPP (t, m)

Similarly, when the deployment area is given, the deployment cost is a function of node number too, denoted by d. Thus, the optimal cost function is:

$$\min \sum_{i=1}^{D_1} f_i(n_i) + d(n_i), 0 \leq n_i \tag{4}$$

If both function f and d are continuous differentiable convex functions, according to Relationship 2.2, objective function (4) could be converted into following variational inequality

$$y_1 = \sum_{i=1}^{D_1} (\frac{\partial f_i(n_i^*)}{\partial n_i} + \frac{\partial d(n_i^*)}{\partial n_i}) \times (n_i - n_i^*) \geq 0, (\forall n_i \in K_1) \tag{5}$$

where $K_1 \equiv \{n_i | n_i \geq 0, \forall i\}$,the variables with $'*'$ represents the optimal solution to this function.

4.2 Optimal Connectivity

There are two kinds of connectivity for a protocol: protocol connectivity and network connectivity. The former one is the probability of establishing a secure link between any two nodes which depends on protocol strategy. Since the physical environment, such as node location, link quality etc., could affect the establishment of secure link by decreasing the node communication radius, or even isolating a node from the others, two node sharing many keys may never have a chance to establish a secure link. Hence, we introduced the concept of network connectivity by taking the environment factors into account. In fact, some key management protocols [19–21] based on location need to consider the

network density at the right beginning of design. Therefore that whether two nodes can establish a secure link will depend on two conditions:

(1)Two nodes can establish shared keys according to protocol strategy. This condition is decided by the protocol parameter $r$key ring m and the key pool P;

(2) One of the two node can reach the other one. This is related to the link quality and location.

Let $\boldsymbol{n} =< n_1, \ldots, n_{D_1} >$ and $\boldsymbol{\rho}$ be a vector whose element $\rho_{i,k}(i = 1, \cdots, D_1; k = 1, \cdots, D_3)$ is the contribution of the ith class node to the kth class value of density heterogeneity. Similarly, element $w_{i,v}(i = 1, \cdot, D_1; v = 1, \cdots, D_4)$ of vector $\boldsymbol{w}$ denotes the contribution of the ith class node to the vth class value of Location Heterogeneity. The element $l_{i,z}(i = 1, \cdots, D_1); z = 1, \cdots, D_2$ of vector $\boldsymbol{l}$ shows the contribution of the ith class node to the zth class value of Link Heterogeneity. The element $m_{i,q}(i = 1, \cdots, D_1; q = 1, \cdots, M)$ of vector m represents the contribution of the ith class node to the qth class key material. Therefore, protocol connectivity function of ith class node which has the mth key material can be expressed as:

$$lc_{i,q} = lc_{i,q}(\boldsymbol{m}, \boldsymbol{n}), \forall i \tag{6}$$

where $m_{i,q} \geq 0$. Given the environment parameters $\rho_{i,k}, w_{i,v}, l_{i,z}$, the network connectivity function of ith class node is

$$gc_{i,v,k,z,q} = gc_{i,v,k,z,q}(\boldsymbol{n}, \boldsymbol{w}, \boldsymbol{\rho}, \boldsymbol{l}, \boldsymbol{m}),\ \forall i, v, k, z, q \tag{7}$$

where $m_{i,q} \geq 0, \rho_{i,k} \geq 0, w_{i,v} \geq 0, l_{i,z} \geq 0, n_i \geq 0$. Suppose the importance of this two connectivity are α and β respectively, and $0 < \alpha, \beta < 1, \alpha + \beta = 1$, then the function of optimal connectivity is

$$\begin{aligned} &\max \alpha \sum_{i=1}^{D_1} \sum_{q=1}^{M} lc_{i,q}(\boldsymbol{n}, \boldsymbol{m}) + \beta \sum_{i=1}^{D_1} \sum_{v=1}^{D_2} \sum_{k=1}^{D_3} \sum_{z=1}^{D_4} \sum_{q=1}^{M} gc_{i,v,k,z,q}(\boldsymbol{n}, \boldsymbol{w}, \boldsymbol{\rho}, \boldsymbol{l}, \boldsymbol{m}) \\ &\Longrightarrow \min \alpha \sum_{i=1}^{D_1} \sum_{q=1}^{M} (-lc_{i,q}(\boldsymbol{n}, \boldsymbol{m})) + \beta \sum_{i=1}^{D_1} \sum_{v=1}^{D_2} \sum_{k=1}^{D_3} \sum_{z=1}^{D_4} (-gc_{i,v,k,z,q}(\boldsymbol{n}, \boldsymbol{w}, \boldsymbol{\rho}, \boldsymbol{l}, \boldsymbol{m})) \end{aligned} \tag{8}$$

subject to

$$\textstyle\sum_{q=1}^{M} m_{i,q} \leq n_i,\ \ \sum_{k=1}^{D_3} \rho_{i,k} \leq n_i,\ \ \sum_{v=1}^{D_4} w_{i,v} \leq n_i,\ \ \sum_{z=1}^{D_2} l_{i,z} \leq n_i$$

When lc, gc are continuous differentiable concave functions, then $-lc$, $-gc$ are continuous differentiable convex functions. Thus the equivalent variational inequality of connectivity can be got as *eq.*(9) where $K_2 \equiv \{(n, w, \rho, l, m, \eta_1, \eta_2, \eta_3, \eta_4) | m_{i,q} \geq 0, \rho_{i,k} \geq 0, w_{i,v} \geq 0, l_{i,z} \geq 0, n_i \geq 0, \forall i, q, k, v, z\}$, and $\eta_{xi}(x = 1, 2, 3, 4)$ is the

lagrange multipliers corresponding to the constrains above.

$$
\begin{aligned}
&y_2 = \\
&\sum_{i=1}^{D_1}\left(\eta_{1i}^* - \frac{\alpha\partial lc_{i,q}(m^*,n^*)}{\partial n_i} - \beta\sum_{z=1}^{D_2}\sum_{k=1}^{D_3}\sum_{v=1}^{D_4}\sum_{q=1}^{M}\frac{\partial gc_{i,v,k,z,q}(n^*,w^*,\rho^*,l^*,m^*)}{\partial n_i}\right)\times(n_i - n_i^*) \\
&+\sum_{i=1}^{D_1}\sum_{q=1}^{M}\left(\eta_{1i}^* - \frac{\alpha\partial lc_{i,q}(m^*,n^*)}{\partial m_{i,q}} - \beta\sum_{z=1}^{D_2}\sum_{k=1}^{D_3}\sum_{v=1}^{D_4}\frac{\partial gc_{i,v,k,z,q}(n^*,w^*,\rho^*,l^*,m^*)}{\partial m_{i,q}}\right)\times(m_{i,q} - m_{i,q}^*) \\
&+\sum_{i=1}^{D_1}\sum_{k=1}^{D_3}\left(\eta_{2i}^* - \beta\sum_{z=1}^{D_2}\sum_{v=1}^{D_4}\sum_{q=1}^{M}\frac{\partial gc_{i,v,k,z,q}(n^*,w^*,\rho^*,l^*,m^*)}{\partial \rho_{i,k}}\right)\times(\rho_{i,k} - \rho_{i,k}^*) \\
&+\sum_{i=1}^{D_1}\sum_{v=1}^{D_4}\left(\eta_{3i}^* - \beta\sum_{z=1}^{D_2}\sum_{k=1}^{D_3}\sum_{q=1}^{M}\frac{\partial gc_{i,v,k,z,q}(n^*,w^*,\rho^*,l^*,m^*)}{\partial w_{i,v}}\right)\times(w_{i,v} - w_{i,v}^*) \\
&+\sum_{i=1}^{D_1}\sum_{z=1}^{D_2}\left(\eta_{4i}^* - \beta\sum_{k=1}^{D_3}\sum_{v=1}^{D_4}\sum_{q=1}^{M}\frac{\partial gc_{i,v,k,z,q}(n^*,w^*,\rho^*,l^*,m^*)}{\partial l_{i,z}}\right)\times(l_{i,z} - l_{i,z}^*) \\
&+\sum_{i=1}^{D_1}(n_i^* - \sum_{q=1}^{M} m_{i,q}^*)\times(\eta_{1i} - \eta_{1i}^*) + \sum_{i=1}^{D_1}(n_i^* - \sum_{k=1}^{D_3}\rho_{i,k}^*)\times(\eta_{2i} - \eta_{2i}^*) \\
&+\sum_{i=1}^{D_1}(n_i^* - \sum_{v=1}^{D_4} w_{i,v}^*)\times(\eta_{3i} - \eta_{3i}^*) + \sum_{i=1}^{D_1}(n_i^* - \sum_{k=1}^{D_2} l_{i,k}^*)\times(\eta_{4i} - \eta_{4i}^*) \geq 0, \\
&\forall(m,\rho,w,l,n,\eta_1,\eta_2,\eta_3,\eta_4) \in K_2
\end{aligned}
\tag{9}
$$

4.3 Optimal Energy Consumption

The majority of node energy is consumed on information processing, transmission and reception. According to Ref. [22], energy consumption can be subdivided into two parts: circuit consumption and transmit amplifier consumption. Given energy consumption for sending and receiving one bit data respectivelythe energy spent on finishing task i is a function of sending/receiving time and the amount of receivers. Since the time is decided by task while the amount of receivers is determined by the node density, the consumption of each task carried out by the ith class node which has kth class density can be defined as

$$
eng_{i,k} = eng_{i,k}(\boldsymbol{n},\boldsymbol{\rho}),\ \forall i,k \tag{10}
$$

So the minimal energy consumption of each task is

$$
\min\sum_{i=1}^{D_1}\sum_{k=1}^{D_3} eng_{i,k}(\boldsymbol{n},\boldsymbol{\rho}),\ \rho_{i,k} \geq 0, \sum_{k=1}^{D_3} \leq n_i \tag{11}
$$

When *eng* is a continuous differentiable convex function, its equivalent variational inequality is

$$\begin{aligned} y_3 = &\sum_{i=1}^{D_1}\sum_{k=1}^{D_3}\left(\eta_{2i}^* + \frac{\partial eng_{k,i}(\boldsymbol{n}^*,\boldsymbol{\rho}^*)}{\partial \rho_{i,k}}\right) \times (\rho_{i,k} - \rho_{i,k}^*) + \sum_{i=1}^{D_1}\left(\sum_{k=1}^{D_3}\frac{\partial eng_{k,i}(\boldsymbol{n}^*,\boldsymbol{\rho}^*)}{\partial n_i} - \eta_{2i}^*\right) \\ &\times (n_i - n_i^*) + \sum_{i=1}^{D_1}(n_i^* - \sum_{k=1}^{D_3}\rho_{i,k}^*) \times (\eta_{2i} - \eta_{2i}^*) \geq 0, \\ &(\forall(\boldsymbol{n},\boldsymbol{\rho},\boldsymbol{\eta_2}) \in K_3) \end{aligned} \tag{12}$$

where $K_3 \equiv \{(\boldsymbol{n},\boldsymbol{\rho},\boldsymbol{\eta}_2)|\rho_{i,k} \geq 0, n_i \geq 0, \forall i,k\}$.

4.4 Optimal Resilience

Resilience of the ith class node which has the qth class key material depends on the size of key pool and key ring. Therefore, global resilience can be calculated as

$$r_{i,q} = r_{i,q}(\boldsymbol{m},\boldsymbol{n}),\ \forall q \tag{13}$$

then the maximal global resilience is

$$\max \sum_{i=1}^{D_1}\sum_{q=1}^{M} r_{i,q}(\boldsymbol{m}^*,\boldsymbol{n}^*) \tag{14}$$

subject to $m_{1,q} \geq 0, n_i \geq 0, \sum_{q=0}^{M} m_{i,q} \leq n_i$. When r is a continuous differentiable convex functionits equivalent variational inequality:

$$\begin{aligned} y_4 = &\sum_{i=1}^{D_1}\sum_{q=1}^{M}\left(\eta_{1i}^* - \frac{\partial r_{i,q}(\boldsymbol{m}^*,\boldsymbol{n}^*)}{\partial m_{i,q}}\right) \times (m_{i,q} - m_{i,q}^*) \\ &+ \sum_{i=1}^{D_1}\sum_{q=1}^{M}\left(-\frac{\partial r_{i,q}(\boldsymbol{m}^*,\boldsymbol{n}^*)}{\partial n_i} - \eta_{1i}^*\right) \times (n_i - n_i^*) \\ &+ \sum_{i=1}^{D_1}(n_i^* - \sum_{q=1}^{M} m_{i,q}^*) \times (\eta_{1i} - \eta_{1i}^*) \geq 0, \\ &(\forall(\boldsymbol{n},\boldsymbol{m},\boldsymbol{\eta_1}) \in K_4) \end{aligned} \tag{15}$$

where $K_4 = \{(\boldsymbol{n},\boldsymbol{m},\boldsymbol{\eta_1})|n_i \geq 0,\ m_{i,q} \geq 0,\ \forall i,q\}$.

4.5 Equilibrium Expression

Global optimal performance, called equilibrium performance, is a tradeoff among the 4 performances mentioned in section 4.1 $\sim$ 4.4. These performances

are usually interdependent and interactive. For addressing the equilibrium constraint problem of KMP, we need to find a feasible solution $(\boldsymbol{n}, \boldsymbol{m}, \boldsymbol{l}, \boldsymbol{\rho}, \boldsymbol{w}) \in R_+^{D_1+D_1\times M+D_1\times D_2+D_1\times D_3+D_1\times D_4}$ of the following inequality:

$$y_1 + y_2 + y_3 + y_4 \geq 0 \tag{16}$$

Our models can be easily extended to describe more complicated or special application-oriented network by adding more constraint conditions. For example, if limit $\sum_{i=1}^{D_1} n_i \leq N$, the discussed network will change from a infinite scalable one to a finite one.

5 Theoretical Analysis

Before solving the equilibrium model, we need to ensure that the solution exists.

Theorem 5.1 *Solution of variational inequality (16) exists when all functions are continuous.*

Proof. In a sensor networkthe amount of nodes $N = \sum_{i=1}^{D_1} n_i$ is always finite. Considering each element of vector $\boldsymbol{l}, \boldsymbol{\rho}, \boldsymbol{w}, \boldsymbol{m}, \boldsymbol{t}$ must be no more than its corresponding n_i, a vector $\boldsymbol{O}$ consisting of $o_i (1 \leq i \leq 6)$ can be found which will give a true statement to the feasible solution shown as (17). K is a closed convex subset. Since functions in (16) are all continuous, satisfying the necessary and sufficient conditions for the existence of the solution of a variational inequality problem $VI(F, K)$, this proposition is true. □

$$\begin{aligned}\boldsymbol{K} \equiv\{&(\boldsymbol{n}, \boldsymbol{l}, \boldsymbol{\rho}, \boldsymbol{w}, \boldsymbol{m}) | o \leq \boldsymbol{n} \leq o_1, 0 \leq \boldsymbol{l} \leq o_2,\ 0 \leq \boldsymbol{\rho} \leq o_3,\ 0 \leq \boldsymbol{w} \leq o_4,\ 0 \leq \boldsymbol{m} \leq o_5 \\ &\forall i, k, z, q, v\}\end{aligned} \tag{17}$$

Theorem 5.2 *the solution of variational inequality (16) is unique when all functions are continuous, differentiable and convex.*

Proof. Functions $(f, d, eng, -gc, -r, -lc)$ in (16) are continuous, differentiable and convex, and because the derivative of a convex function is monotonic, $F = y_1 + y_2 + y_3 + y_4$ is monotonic too. When one of these derivatives is strictly monotonic, F is a strictly convex function, namely $\langle F(X_1) - F(X_2), X_1 - X_2 \rangle > 0$.

According to the judgment condition for unique solution of a variational inequality, if F's solution exists, it's unique. □

Theorem 5.3 *Variational inequality (16) is Lipschiz continuous.*

Proof. According to lagrange mean value theorem, there must be a value $\xi \in [X_2, X_1]$ satisfying $F'(\xi)(X_1 - X_2) = F(X_1) - F(X_2)$. So $|F'(\xi)|\|X_1 - X_2\| = \|F(X_1) - F(X_2)\|$and exist $L > 0$ makes $L\|X_1 - X_2\| \geq \|F(X_1) - F(X_2)\|$ true.

Hence, variational inequality (16) is Lipschiz continuousand L is its Lipschiz constant. □

Theorem 5.1, 5.2 and 5.3 proved that the equilibrium constraint expression is monotonic, Lipschiz continuous and has a unique solution. Therefore, the improved Korpelevich method [15], as shown in Table 2, can be used to solve our variational inequality and return its unique optimal solution.

Table 2. Algorithm 1

algorithm: solve the variational inequality
input:
$X^0 = (n_0, l_0, \rho_0, w_0, m_\rangle \in K; //initialize$
$\tau = 1; //round\ number$
$0 \le \theta \le \frac{1}{L}; //L - Lipschiz\ constant, \theta - step\ length$
$0 \le \varepsilon \le 1; //a\ numbe\ small\ enough\ for\ convergence$
$//x_1 = n; x_2 = l; x_3 = \rho; x_4 = w; x_5 = m;$
$for(l = 1; l < 6; l++)\{$
$\quad while(\max\lvert x_l^\tau - x_l^{\tau-1}\rvert \ge \varepsilon) do\{$
$\quad\quad if\ require\ x_l^\tau \ge c$
$\quad\quad\quad \bar{x_l}^{\tau-1} = \max(c, x_l^{\tau-1} - \theta F(x_l^{\tau-1}));$
$\quad\quad\quad x_l^\tau = \max(c, x_l^{\tau-1} - \theta F(\bar{x_l}^{\tau-1}));$
$\quad\quad else$
$\quad\quad\quad \bar{x}^{\tau-1} = \min(c, x^{\tau-1} - \theta F(x^{\tau-1}));$
$\quad\quad\quad x^\tau = \min(c, x^{\tau-1} - \theta F(\bar{x}^{\tau-1}));$
$\quad\quad endif$
$\quad\quad \tau = \tau + 1; X^\tau = (x_1^\tau, x_2^\tau, x_3^\tau, x_4^\tau, x_5^\tau)$
$\}\}$
output X^τ

6 Numerial Example

According to Ref. [22] and Ref. [24], some parameters are picked as follows-Four kinds of heterogeneities are considered as listed in Table. 1. The HA value of link heterogeneity, location heterogeneity and density heterogeneity are $(0.9, 0.7)$, $(1, 0.2)$, $(0.2, 0.3)$ respectively. The unit price and communication radius of normal nodes ($h_{1,1}$) and advanced nodes ($h_{1,2}$) are (10, 20m) and (40, 40m) respectively. In addition, all of sensor nodes are omnidirectional antenna

nodes which can receive messages from any direction. The circuit consumption $e_{ek} = 0.533\mu J/bit$, the pass loss exponent $\alpha = 2.5$, the amplifier consumption $e_a = 10\mu J/(bit \cdot m)$. The area of monitoring region $A = 10^5 m^2$. The size of key pool $|P| = 10^4$. Step length $\theta = 0.05$, end condition $\varepsilon = 1$. EG scheme is adopted as an protocol example.

Without considering time factor, an OVDM model for EG scheme is established as shown in Fig. 3. The HA values of each heterogeneity are depicted in the figure directly. Weight of $h_{1,i} \to t$ equals to the number of the ith class nodes, meaning that all nodes have a fair chance to execute each task. The weight of $h_{1,i} \to m$ represents the optimal size of key ring.

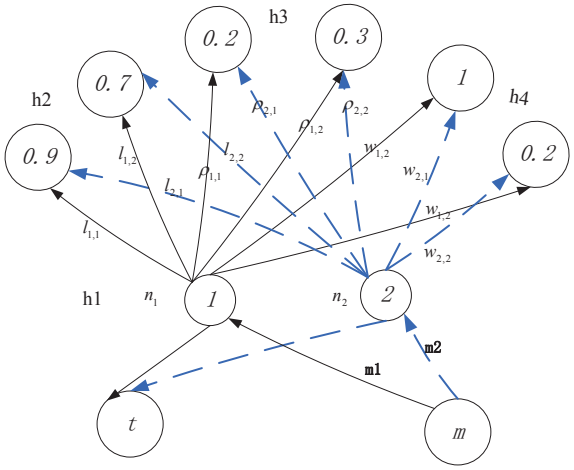

Fig. 3. OVDM for EG

The network cost function is

$$nc(n) = 10 \times n_1 + 40 \times n_2 + 0.3 \times (n_1 + n_2) + 0.02 \times 10^6$$

Let m_1 and m_2 be the size of key ring of $h_{1,1}$ node and $h_{1,2}$ node respectively, the average connectivity functions are shown in eq. (18).

Take nodes whose HA value of Node Heterogeneity $h_{1,2} = 2$ for example, the amount of them is equal to n_2, when the HA values of Location Heterogeneity , Density Heterogeneity , Link heterogeneity are w, ρ *and* l respectivelytheir probability of establishing a secure link with another $h_{1,2}$ node could be calculated as $\frac{n_2}{A} \times \pi(wlr^2)/[\pi(wlr)^2\rho] = n_2/\rho A$. Hence, the network connectivity

functions are as shown as eq. (19).Similarly, we can get$gc_{1,1,1,2},\ gc_{2,2,2,2}$.

$$
\begin{aligned}
lc_{n_1,m_1} &= \left[1-\frac{C_P^{m_2}C_{P-m_2}^{m_2}}{C_P^{m_2}C_P^{m_1}}\right]\times\frac{C_{n_2}^1C_{n_1}^1}{C_{n_2+n_1}^2}+\left[1-\frac{C_P^{m_1}C_{P-m_1}^{m_1}}{(C_P^{m_1})^2}\right]\times\frac{C_{n_1}^2}{C_{n_2+n_1}^2}\\
&\overset{n!=\sqrt{2\pi}n^{n+\frac{1}{2}}e^{-n}}{\approx}\left[1-\frac{(1-\frac{m_2}{P})^{P-m_2+0.5}(1-\frac{m_1}{P})^{P-m_1+0.5})}{(1-\frac{m_2}{P}-\frac{m_1}{P})^{P-m_2-m_1+0.5}}\right]\times\frac{2n_2n_1}{(n_2+n_1)(n_2+n_1-1)}\\
&+\left[1-\frac{(1-\frac{m_1}{P})^{2(P-m_1+0.5)}}{(1-\frac{2m_1}{P})^{P-2m_1+0.5}}\right]\times\frac{n_1\times(n_1-1)}{(n_2+n_1)(n_2+n_1-1)}\\
lc_{n_2,m_2} &= \left[1-\frac{C_P^{m_2}C_{P-m_2}^{m_2}}{(C_P^{m_2})^2}\right]\times\frac{C_{n_2}^2}{C_{n_2+n_1}^2}+\left[1-\frac{C_P^{m_2}C_{P-m_2}^{m_1}}{C_P^{m_2}C_P^{m_1}}\right]\times\frac{C_{n_2}^1C_{n_1}^1}{C_{n_2+n_1}^2}\\
&\overset{n!=\sqrt{2\pi}n^{n+\frac{1}{2}}e^{-n}}{\approx}\left[1-\frac{(1-\frac{m_2}{P})^{2(P-m_2+0.5)}}{(1-\frac{2m_2}{P})^{P-2m_2+0.5}}\right]\times\frac{n_2\times(n_2-1)}{(n_2+n_1)(n_2+n_1-1)}\\
&+\left[1-\frac{(1-\frac{m_2}{P})^{P-m_2+0.5}(1-\frac{m_1}{P})^{P-m_1+0.5}}{(1-\frac{m_2}{P}-\frac{m_1}{P})^{P-m_1-m_2+0.5}}\right]\times\frac{2n_1n_2}{(n_2+n_1)(n_2+n_1-1)}\\
lc_{n_2,m_1} &= lc_{n_1,m_2}=0
\end{aligned}
\tag{18}
$$

$$
gc_{1,1,1,1}=\frac{w_{1,1}}{w_{1,1}+w_{1,2}}\times\frac{l_{1,1}}{l_{1,1}+l_{1,2}}\times\frac{\rho_{1,1}}{\rho_{1,1}+\rho_{1,2}}\times\left[\begin{array}{l}\left(1-\frac{C_P^{m_1}C_{P-m_1}^{m_1}}{(C_P^{m_1})^2}\right)\times\frac{n_1}{0.2A}\\+\left(1-\frac{C_P^{m_2}C_{P-m_2}^{m_1}}{C_P^{m_1}C_P^{m_2}}\right)\times\frac{n_2}{0.2A}\end{array}\right]
$$

$$
\begin{aligned}
gc_{2,2,1,1}&=\frac{w_{2,1}}{w_{2,1}+w_{2,2}}\times\frac{l_{2,1}}{l_{2,1}+l2,2}\times\frac{\rho_{2,2}}{\rho_{2,1}+\rho_{2,2}}\\
&\times\left[\begin{array}{l}\left(1-\frac{C_P^{m_2}C_{P-m_2}^{m_1}}{C_P^{m_2}C_P^{m_1}}\right)\times\frac{n_1}{0.3A}\\+\left(1-\frac{C_P^{m_2}C_{P-m_2}^{m_2}}{(C_P^{m_2})^2}\right)\times\frac{n_2}{0.3A}\end{array}\right]
\end{aligned}
$$

In EG schema, there are two kinds of task: direct key establishment and indirect key establishment. In order to finish the former process, nodes will broadcast their key ID list. If nodes who received this message find a match in its own key ID listthey randomly choose a common key as shared key. Every node needs to establish direct shared key first, then two nodes in the communication range of each other but no common key established will start the indirect key establishment. Source node broadcasts target ID, when a middle node sharing keys with both of the source node and the target node receives this message, it will generate a shared key and transmit it to both of them. Because of using omnidirectional antenna, every message sending by a node will be received by all nodes in its communication range, just like broadcast. When a node going to send l bit data and its communication range is r, the sending consumption $e_s = l(e_{ek} + e_a r^\alpha)$, the receiving consumption is $e_r = le_{ek}$, so the broadcast consumption for establishing a direct shared key should be $e_1 = e_s + \rho re_r$, and

the consumption for establishing a indirect key is $e_2 = 2e_s + (\rho_{source} r_{source} + \rho_{middle} r_{middle}) e_r$. Since nodes usually use signal intensity to measure the distance from their neighbor, it is reasonable to choose the nearest neighbor as the middle node, and that may make the energy consumed on middle node is approximate to that of source node. Thereforeenergy consumption function is

$$e_{1,1} = \frac{3n_1}{n_1 + n_2} \times \frac{\rho_{1,1}}{\rho_{1,1} + \rho_{1,2}} \times (e_s + 0.2 \times 20 e_r)$$

Functions $e_{1,2}, e_{2,1}, e_{2,2}$ can be got in the same way. When one node is compromised, the resilience of a uncompromised node is equal to

$$r = \frac{n_1}{n_1 + n_2} \times \frac{m_1}{P} + \frac{n_2}{n_1 + n_2} \times \frac{m_2}{P}$$

The solution to our model is found by using algorithm 1, as shown in Table 5. Keeping $n_1 + n_2$ constantreducing the value of variables in column n_1 and n_2 by 30% respectively to generate two groups of data, *result_n*$_1$ and *result_n*$_2$. Expand the value in 6 to 1.5 times, new data *result_au* is got. Calculating the performance of each data group, the result is shown in Fig. 4.

Table 3. Result

param	n_1	n_2
n	1910.76	104.53
m	164.93	199.15
l_1	1900	69.8
l_2	30.1	30
w_1	887.7	57.4
w_2	1002.4	42.4
ρ_1	1050	50
ρ_2	900	50
η_1	−1089	−3
η_2	−382	1981
η_3	−330	16929
η_4	2	4

It can be seen from Fig. 4, though the resilience of data *result* is worse than *result_n*$_2$, the performances in terms of connectivity, energy consumption and cost are obviously better than the other three groups. And the other three performances of *result_n*$_2$ is badly worse than *result*. Comparing with *result*, when the number of n_1 decrease 30%, the number of n_2 increase 30%, the cost and energy consumption of protocol will increasewhile the resilience is reducing. When all values are replaced by bigger numbers, connectivity and resilience obviously decrease, and the cost raises higher than *result*, lower than *result_n*$_1$. Generally speakingthe model proposed in this paper solved the optimization problem of key management protocol, and returned a global optimization performance.

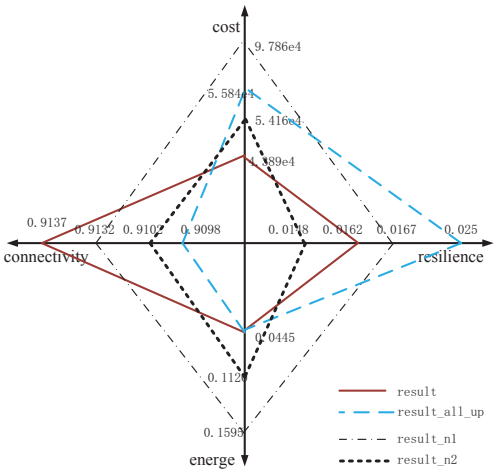

Fig. 4. OVDM for EG

7 Conclusion

Based on supernetworks and variational inequality theory, we proposed a optimal HA value distribution model (OHVM) and provided a method to find the optimal solution. Our model illustrated a simple way to depict the complex relationship between heterogeneities and protocols. The optimal result can help designer to reasonably deploy a WSN so that the optimal protocol performance can be achieved. In addition, the OHVM is scalable and combinable so that it can be easily used to analyze different application-oriented key management protocols. Our experimental result shows that:

1. OHVM is feasible;
2. The result generated by solving our model can provide a node distribution scheme which will bring a global optimal performance for key management protocols.

In the future, we will going to focus on the following two aspects:

1. The time factor and its affect on heterogeneities and protocol performance.
2. The other performance metrics except cost, energy consumption, connectivity and resilience.

acknowledgements

This research was supported by National Natural Science Found of China under Grant No. 61170241 and No.61472097

References

1. Yum D H, Lee P J. Exact formulae for resilience in random key predistribution Schemes: Wireless Communications, IEEE Transactions on, 11(5), 1638-1642(2012)
2. Turkanovic M, Brumen B, Holbl M: A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Networks, 20, 96-112(2014)
3. Suganthi N, Vembu S.: Energy Efficient Key Management Scheme for Wireless Sensor Networks, International Journal of Computers Communications Control, 9(1), 71-78(2014)
4. Novales R L, Mittal N, Sarac K.: SKAIT: A parameterized key assignment scheme for confidential communication in resource constrained ad hoc wireless networks, Ad Hoc Networks, 20, 163-181(2014)
5. Su Z, Lin C, Feng F J, et al: Key management schemes and protocols for wireless sensor networks, Journal of Software, 18(5), 1218-1231 (2007)
6. Alcaraz C, Lopez J, Roman R, et al: Selecting key management schemes for WSN applications. Computers and Security, 31(8), 956-966 (2012)
7. Cheng C, Qian Y, Zhang D: An Approach Based on Chain Key Predistribution against Sybil Attack in Wireless Sensor Networks, International Journal of Distributed Sensor Networks, (2013)
8. Bechkit W, Challal Y, Bouabdallah A, et al:A highly scalable key pre-distribution scheme for wireless sensor networks. IEEE Transactions on Wireless Communications, 12(2),948-959 (2013)
9. Boloorchi A T, Samadzadeh M H, Chen T. Symmetric Threshold Multipath (STM): An online symmetric key management scheme. Information Sciences, 268,489-504 (2014)
10. Maura B.Paterson, Douglas R.Stinson: A unified approach to combinatorial key predistribution scheme for sensor networks, Designs,Codes and Cryptography, 71(3),433-457 (2014)
11. Yarvis, M., Kushalnagar, N., Singh, H., et al.: Exploiting Heterogeneity in Sensor Networks. In: Proc. of INFOCOM'05, pp. 878-890. Miami, USA (2005)
12. Zeng G, Wang B, Mutka M, et al: Efficient multicast for link-heterogeneous wireless mesh networks. In: Proc.of 2009 International Conference on Performance Computing and Communications ,pp. 177-184 (2009)
13. KATIYAR V., CHAND N., SONI S.: Improving Lifetime of Large-Scale Wireless Sensor Networks Through Heterogeneity. In: Proc. of 2011 International Conference on Emerging Trends in Electrical and Computer Technology, pp. 1032-1036. Nagercoil, India (2011).
14. Chen C M, Zheng X, Wu T Y: A complete hierarchical key management scheme for heterogeneous wireless sensor networks, The Scientific World Journal, (2014)
15. WANG Z.P., WANG Z.T.: Supernetworks Theory and Applications. Science Press, New York (2008).
16. WANG Z.P., ZHOU S.B., GUO J.F.: Variational-Inequality-Based Supernetworks Model for Network Advertisement Distribution. Journal of Dalian Maritime University. 33(4), 26-30 (2007).
17. HAN W.M., CHEN X.L.: Introduction to Variational Inequality - the Basic Theory. Numerical Analysis and Applications. Academic Press, New York (2007)
18. KIM J.K., ZHANG B.T.: Evolving Hypernetworks for Pattern Classification. In: Proc. of 2007 IEEE Congress on Evolutionary Computation, pp. 1856-1862. Tokyo, Japan (2007)

19. Erman A T, Dilo A, Hoesel L, et al: On Mobility Management in Multi-Sink Sensor Networks for Geocasting of Queries. Sensors, 11(12),11415-11446 (2011)
20. Chen C L, Tsai Y T, Castiglione A, et al: Using bivariate polynomial to design a dynamic key management scheme for wireless sensor networks. Computer Science and Information Systems, 10(2): 589-609 (2013)
21. Lee J H, Kwon T: GENDEP Location-Aware Key Management for General Deployment of Wireless Sensor Networks. International Journal of Distributed Sensor Networks (2014)
22. HAAPOLA J., SHELBY Z., POMALAZA R.C., et al.: Cross-Layer Energy Analysis of Multi-Hop Wireless Sensor Network. In: Proc. of European Conference on Wireless Sensor Networks, pp. 33-44. Istanbul, Turkey (2005)
23. BERTSEKAS D.P, TSITSIKLIS J.: Parallel and Distriuted Computation. Prentice-Hall, (1989)
24. DU W.L., DENG J., Han Y.S., et al.: A Key Predistribution Scheme for Sensor Networks using Deployment Knowledge. IEEE Transactions on Dependable and Secure Computing. 3(1), pp. 62-77 (2006)