Tsinghua Science and Technology

Volume 21 | Issue 3 Article 9

2016

Optimization of Key Predistribution Protocol Based on Supernetworks Theory in Heterogeneous WSN

Qi Yuan
College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China.

Chunguang Ma
College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China.

Xiaorui Zhong
China Academy of Electronics and Information Technology, Beijing 100041, China.

Gang Du
College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China.

Jiansheng Yao
College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China.

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 09/11 pp333–343
Volume 21, Number 3, June 2016

Optimization of Key Predistribution Protocol Based on Supernetworks Theory in Heterogeneous WSN

Qi Yuan, Chunguang Ma*, Xiaorui Zhong, Gang Du, and Jiansheng Yao

Abstract: This work develops an equilibrium model for finding the optimal distribution strategy to maximize performance of key predistribution protocols in terms of cost, resilience, connectivity, and lifetime. As an essential attribute of wireless sensor networks, heterogeneity and its impacts on random key predistribution 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.

Key words: optimization; key predistribution protocol; supernetworks; variational inequality; wireless sensor networks

1 Introduction

In Wireless Sensor Networks (WSNs), a Key Predistribution Protocol (KPP) is usually designed or analyzed under the hypothesis that the network is ideal. For instance, all sensors are reachable, the climates or environments around different nodes are identical, and no unexpected incident will happen; nodes are uniformly deployed in the monitoring region[1–4]. Under such ideal assumptions, plenty of efficient KPPs have been proposed as shown in Refs. [5–10]. However, things are different in reality. For example, a node deployed in a hole may never be reached. Research achievements under ideal assumptions do not apply to practical applications very well, and their reference value is limited. Hence, it is of great interest to consider the differences among nodes or among their locations—their heterogeneity. Studying heterogeneity can help us design network models with more practicality, design protocols with better performance, and analyse with more accuracy.

In fact, heterogeneity is an essential attribute of WSNs. 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 the node itself, the physical environment around a node is another source of heterogeneity. Heterogeneous environments 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 raise the communication cost. Usually, heterogeneity will keep on affecting the performance of a protocol until the network dies.

Although heterogeneity plays a significant role in WSNs in terms of raising security or reducing energy consumption, the research on heterogeneity is still in

• Qi Yuan, Chunguang Ma, Gang Du, and Jiansheng Yao are with College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China. E-mail: {yuanqi,machunguang}@hrbeu.edu.cn; 50320864@qq.com; yaojiansheng@hrbeu.edu.cn.
• Qi Yuan is also with College of Communication and Electronic Engineering, Qiqihar University, Qiqihar 161006, China.
• Chunguang Ma is also with Key Lab of Network Security and Cryptography of Fujian Province.
• Xiaorui Zhong is with China Academy of Electronics and Information Technology, Beijing 100041, China. E-mail: zhongxiaoruibaby@163.com.
∗ To whom correspondence should be addressed.
Manuscript received: 2016-02-02; accepted: 2016-03-10

an early stage and the achievements so far are limited. This is because the complexity of topic and dynamic changes in it make it very hard to describe heterogeneity clearly. This drawback has blocked and delayed the development of heterogeneity research. Considering the insufficiency of existing research studies and the advantages of heterogeneity in terms of bringing more reality into the network model, this paper focuses on utilizing heterogeneity to optimize the performance of random key predistribution 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]. Zeng et al.[12] proposed a heterogeneous link model to increase the throughput of broadcast communication and decrease its communication latency. Katiyar et al.[13] improved a clustering algorithm for WSNs by taking advantage of energy heterogeneity to prolong the lifespan of networks. Recently, Chen et al.[14] improved a complete hierarchical key management scheme that only utilizes symmetric cryptographic algorithms and low-cost operations for heterogeneous cluster-based WSN to assure safety and validity of networks. Existing research on heterogeneity focuses on energy and links, aiming to optimize clustering algorithms, route protocols, public keys, and so on. But that is not enough. Are other heterogeneities affecting protocols? How to describe the state of a whole heterogeneous network and utilize heterogeneity to optimize deployment strategy so that a random key predistribution 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 introduced in Section 2. In Section 3, various heterogeneities are classified, and an optimization model is proposed. Five optimization goals and their equivalent variational inequalities are given in Section 4. Section 5 discusses why, when, and how the optimal solution of our model can be found. A numerical example is given and analyzed in Section 6. Section 7 concludes this paper.

2 Background Knowledge

2.1 Evaluation metrics

According to Ref. [5], metrics to measure KPP 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 the protocol.
- *Security*: Includes confidentiality, authentication, resilience, backward-security, forward-security, and integrality.

Among these metrics, energy, cost, connectivity, resilience, and scalability are five critical ones. Since scalability depends on nothing but management strategy (e.g., an EG scheme) or key materials (e.g., an EBS scheme), it has nothing to do with the network per se. In the published research, only the first four metrics are taken into account. Based on that, global optimization goals 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 the metrics mentioned above, they may still help us find an approximate optimal global solution, because they are four critical factors affecting protocol performance.

2.2 Variational inequality

Definition 1[15–17] A finite-dimensional variational inequality problem VI(f, K) is to find a vector $\boldsymbol{X}^* \in K$ satisfying

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

where f is a continuous function from K to N-dimensional Euclidean space $\mathbb{R}^N$; K is a closed convex set on $\mathbb{R}^N$; and $\langle \cdot, \cdot \rangle$ represents an inner product on $\mathbb{R}^N$.

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

Relationship 1[15] If vector $\boldsymbol{X}^* \in K$ is a solution to function $\min f(\boldsymbol{X})$, then $\boldsymbol{X}^*$ satisfies variational inequality

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

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

Relationship 2[15] To solve an optimization problem with a constraint set in the form of Formula (1), is equivalent to finding a vector $\boldsymbol{X}_i^* \in K_i$ and $u_j^* \geqslant 0$ satisfying Formula (2), where $f_i : \mathbb{R}^{N_i} \to \mathbb{R}$ is a differentiable convex function; K_i is a closed convex set on $\mathbb{R}^{N_i}$; $\boldsymbol{\psi}_{i,j}^{\mathrm{T}}$ is a vector which consists of coefficients of the j-th constraint condition, and this constraint

condition is used to restraint $\boldsymbol{X}_i$.

$$\begin{cases} \min \sum_{i}^{m} f_i(\boldsymbol{X}_i), \\ \boldsymbol{\psi}_{i,j}^{\mathrm{T}} \boldsymbol{X}_i \leqslant b_j, \ \ b_j \in \mathbb{R}, i \in \{1, \ldots, m\}, j = 1, \ldots, r, \\ \boldsymbol{X}_i \in K_i, i = 1, \ldots, m \end{cases} \tag{1}$$

$$\sum_{i=1}^{m} \langle (\bigtriangledown f_i(\boldsymbol{X}_i^*) + \sum_{j=1}^{r} u_j^* \boldsymbol{\psi}_{i,j})^{\mathrm{T}}, (\boldsymbol{X}_i - \boldsymbol{X}_i^*) \rangle + \sum_{j=1}^{r} ((b_j - \boldsymbol{\psi}_{i,j}^{\mathrm{T}} \boldsymbol{X}_i^*) \times (u_j - u_j^*)) \geqslant 0, \tag{2}$$

$$\boldsymbol{X}_i \in K_i, u_j \geqslant 0, \forall i, j$$

3 Heterogeneity and Model

3.1 Heterogeneity

No completely homogeneous network exists in reality. Heterogeneity can always be found in WSNs. For the purpose of simplifying the description, sensor devices and environment factors around nodes are called "element". One specific node and the environment around it are all called an "element object".

For example, a WSN consists of two MICAz mote nodes, node_1 and node_2; node_1 is deployed on a hill, and node_2 is deployed underwater. Then elements of this WSN include the MICAz devices and the node deployment locations; node_1 and node_2 are MICAz device objects; and both the hill and the underwater sites are location objects.

Definition 2 Assume that element e has attributes $(\ldots, a_i, \ldots, a_j, \ldots)$ and element objects $(\ldots, o_p, \ldots, o_q, \ldots)$. The value of attribute a_i of element object o_p is denoted by v_i^p. if $v_i^p \neq v_i^q$, attribute a_i is called a Heterogeneous Attribute (HA).

An example is given in Fig. 1. Node objects node_1 and node_2 have different energies; here energy is a heterogeneous attribute of element "Node". Such heterogeneity is called energy heterogeneity.

Definition 3 Heterogeneity, which is controllable and introduced into networks by humans 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 for sensing.

Definition 4 Heterogeneity, which is random and uncontrollable, is called Objective Heterogeneity (OH).

For example, the external geographical environment, location, climate, etc., belong to OH. Without manual intervention and control, these heterogeneities change with time. SH exists in the deployment phase, aiming at satisfying special application requirements. As time goes on, SH will eventually become OH. Different heterogeneities can be combined to form compound heterogeneities, which are not mutually exclusive.

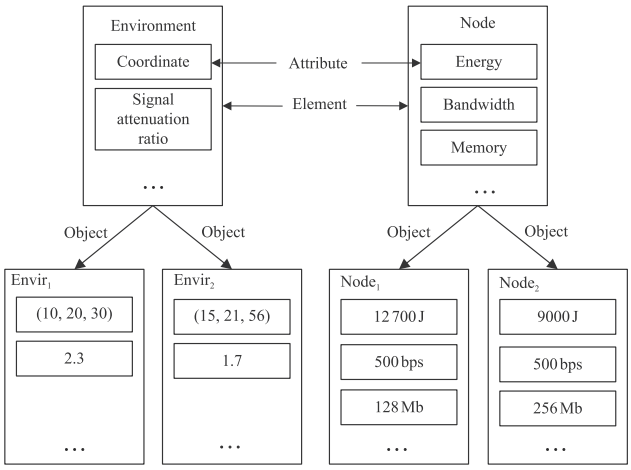

Fig. 1 Relationships among elements, attributes, and objects.

Compound heterogeneities affecting KPP are of 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 locations result in different levels of signal attenuation, and finally lead to different communication ranges, location heterogeneity belongs to environment heterogeneity. Other heterogeneities mentioned in existing studies are included in the two heterogeneities mentioned above. Consider link heterogeneity, for example, bandwidth and signal attenuation are both its attributes, 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 KPP. Since different heterogeneities may have the same impact, there exists some critical heterogeneity that can replace others to generate the 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	Number of neighbors

3.2 Deployment model

As mentioned before, research has proved that making rational use of heterogeneity can improve KPP performance. It is rational to state that when various heterogeneities stay in a certain state, global optimum performance can be reached. Let $O = \{o_1, \ldots, o_n\}$ and $\Delta = \{a_1, \ldots, a_m\}$ be the object set and the attribute set of element e, respectively. For the i-th attribute $a_i \in \Delta$ (whose corresponding heterogeneity is h_i), if there are k different attribute values $v_{i,1}, \ldots, v_{i,k}$ 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 the simplest in which all degrees of HAs are equal to 1. A KPP only has two attributes: key management tasks and key materials. Let KT and KM be the task set and the key material set, respectively; a KPP can be expressed as KPP (KT, KM).

Based on supernetworks theory[15, 18], given a KPP, m heterogeneities existing in KPP-applied networks and corresponding HA values, an 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 (KT, KM).

In Fig. 2, H_i is a value set of the i-th heterogeneity h_i, i.e., $H_i = \{v_{i,1}, \ldots, v_{i,d_i}\}$, $i \neq 1$, and its corresponding attribute is a_i. For simplicity, we define $H_1 = \{n_1, \ldots, n_{d_1}\}$. $h_1 - h_3$ remain consistent with Table 1. Marked circles represent attribute values, tasks or materials. Taking H_1 for example, its degree of HA is d_1, so there are d_1 circles marked from n_1 to n_{d_1}; n_i $(1 \leqslant i \leqslant d_1)$ represents the i-th-level node. The weight of each arrow from circles of H_1 to circles of H_j $(2 \leqslant j \leqslant m)$ represents the number of n_i-th-level $(1 \leqslant i \leqslant d_1)$ nodes, whose value of a_j $(2 \leqslant j \leqslant m)$ equals $v_{j,k}$ $(2 \leqslant j \leqslant m, 1 \leqslant k \leqslant d_j)$ when the best protocol performance is achieved. Let A1 $\mapsto$ B1 be the arrow from circle A1 to B1. If A1 $= n_i$, B1 $= v_{j,k}$ $(j \neq 1)$, the edge weight of A1 $\mapsto$ B1, which represents the number of nodes, is also called the contribution of n_i-th-level nodes to HA value $v_{j,k}$. More precisely, the contribution of $n_1 \mapsto v_{2,1}$ is equal to the number of first-level nodes whose communication radius are $v_{2,1}$.

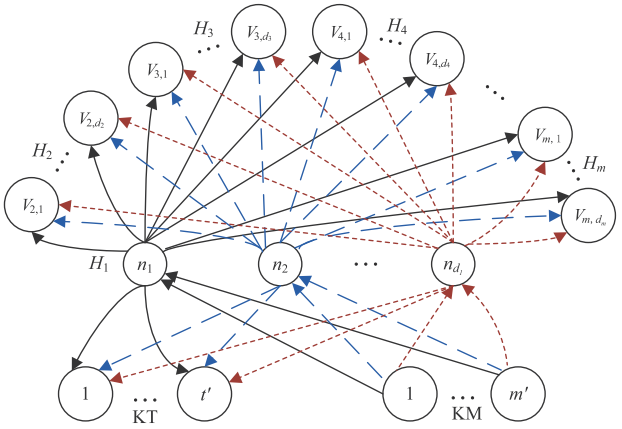

Fig. 2 OVDM of KPP (KT, KM).

4 Equilibrium Optimization Model

In this section, we give five objective functions of KPP optimization. In order to solve the multi-objective equilibrium optimization problem, these 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 can be further divided into software cost and hardware cost. Let $f_{\text{devCost\_}i}$ be the device cost function. When the unit prices of nodes are given and the number of the nodes n_i is expressed as num_i, $f_{\text{devCost\_}i}$ is a function of num_i, namely

$$f_{\text{devCost\_}i} = f_{\text{devCost\_}i}(\text{num}_i), \text{num}_i \geqslant 0 \tag{3}$$

Similarly, when the deployment area is given, the deployment cost is a function of node number too, denoted by $f_{\text{depCost\_}i}$. Thus, the optimal cost function is

$$\min \sum_{i=1}^{d_1} (f_{\text{devCost\_}i}(\text{num}_i) + f_{\text{depCost\_}i}(\text{num}_i)), \quad \text{num}_i \geqslant 0 \tag{4}$$

If both functions $f_{\text{devCost\_}i}$ and $f_{\text{depCost\_}i}$ are continuous differentiable convex functions, according to Relationship 2, objective function (4) can be converted into the following variational inequality,

$$y_1 = \sum_{i=1}^{d_1} \left(\left(\frac{\partial f_{\text{devCost\_}i}(\text{num}_i^*)}{\partial \text{num}_i} + \frac{\partial f_{\text{depCost\_}i}(\text{num}_i^*)}{\partial \text{num}_i} \right) \times (\text{num}_i - \text{num}_i^*) \right) \geqslant 0,$$
$$\text{num}_i^*, \text{num}_i \in K_1, \forall i \tag{5}$$

where $K_1 \equiv \{\text{num}_i | \text{num}_i \geqslant 0, \forall i\}$, the variables num_i^* represent 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 is the probability of establishing a secure link between any two nodes that depend on protocol strategy. Since the physical environment, such as node location, link quality, etc., can affect the establishment of a secure link by decreasing the node communication radius, or even isolating a node from the others, two nodes sharing many keys may never have a chance to establish a secure link. Hence, we introduce 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 beginning of design. Therefore 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 σ, the size of key ring kr, and the size of key pool kp.

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

Let $\boldsymbol{\lambda}_i$ be a vector whose element $\lambda_{i,z}$ ($i = 1, \ldots, d_1$, $z = 1, \ldots, d_2$) is the contribution of the i-th-class node to z-th-class value of link heterogeneity. Similarly, element $\rho_{i,x}$ ($i = 1, \ldots, d_1, x = 1, \ldots, d_3$) of vector $\boldsymbol{\rho}_i$ denotes the contribution of the i-th-class node to the x-th-class value of density heterogeneity. The element $\omega_{i,v}$ ($i = 1, \ldots, d_1, v = 1, \ldots, d_4$) of vector $\boldsymbol{\omega}_i$ shows the contribution of the i-th-class node to the v-th-class value of location heterogeneity. The element $\mu_{i,q} \geqslant 0$ ($i = 1, \ldots, d_1, q = 1, \ldots, m'$) of vector $\boldsymbol{\mu}_i$ represents the contribution of the i-th-class node to q-th-class key material. Therefore, protocol connectivity function of i-th-class node which has the q-th-class key material can be expressed as

$$f_{\text{proConn}} = f_{\text{proConn}}(i, q), \quad i \in \{1, \ldots, d_1\}, q \in \{1, \ldots, m'\} \tag{6}$$

Given the environment parameters $\lambda_{i,z}, \rho_{i,x}$, and $\omega_{i,v}$, the network connectivity function of the i-th-class node is

$$f_{\text{netConn}} = f_{\text{netConn}}(i, z, x, v, q), \quad i \in \{1, \ldots, d_1\}, z \in \{1, \ldots, d_2\}, x \in \{1, \ldots, d_3\}, v \in \{1, \ldots, d_4\}, q \in \{1, \ldots, m'\} \tag{7}$$

where $\lambda_{i,z} \geqslant 0$, $\rho_{i,x} \geqslant 0$, $\omega_{i,v} \geqslant 0$, $\mu_{i,q} \geqslant 0$, and $\text{num}_i \geqslant 0$. Suppose the importance of these two connectivities are α and β, and $0 < \alpha, \beta < 1, \alpha + \beta = 1$, then the function of optimal connectivity is

$$\begin{aligned} &\max \left(\alpha \sum_{i=1}^{d_1} \sum_{q=1}^{m'} f_{\text{proConn}}(i, q) + \beta \sum_{i=1}^{d_1} \sum_{z=1}^{d_2} \sum_{x=1}^{d_3} \sum_{v=1}^{d_4} \sum_{q=1}^{m'} f_{\text{netConn}}(i, z, x, v, q) \right) \Longrightarrow \\ &\min \left(\alpha \sum_{i=1}^{d_1} \sum_{q=1}^{m'} (-f_{\text{proConn}}(i, q)) + \beta \sum_{i=1}^{d_1} \sum_{z=1}^{d_2} \sum_{x=1}^{d_3} \sum_{v=1}^{d_4} \sum_{q=1}^{m'} (-f_{\text{netConn}}(i, z, x, v, q)) \right), \end{aligned} \tag{8}$$

subject to

$$\sum_{z=1}^{d_2} \lambda_{i,z} \leqslant \text{num}_i, \sum_{x=1}^{d_3} \rho_{i,x} \leqslant \text{num}_i, \sum_{v=1}^{d_4} \omega_{i,v} \leqslant \text{num}_i, \sum_{q=1}^{m'} \mu_{i,q} \leqslant \text{num}_i, \forall i$$

When f_{proConn} and f_{netConn} are continuous differentiable concave functions, then $-f_{\text{proConn}}$ and $-f_{\text{netConn}}$ are continuous differentiable convex functions. Thus the equivalent variational inequality of connectivity can be expressed as Eq. (9), where $K_2 \equiv \{(i, z, x, v, q, \eta_{1i}, \eta_{2i}, \eta_{3i}, \eta_{4i}) | \text{num}_i \geqslant 0, \lambda_{i,z} \geqslant 0, \rho_{i,x} \geqslant 0, \omega_{i,v} \geqslant 0, \mu_{i,q} \geqslant 0, \forall i, z, x, v, q\}$, and $\eta_{1i}, \eta_{2i}, \eta_{3i}$, and η_{4i} are the Lagrange multipliers corresponding to the constrains above.

$$\begin{aligned} y_2 = &\sum_{i=1}^{d_1} \left(\eta_{1i}^* - \frac{\alpha \partial f_{\text{proConn}}(i^*, q^*)}{\partial \text{num}_i} \right) \times (\text{num}_i - \text{num}_i^*) - \\ &\sum_{i=1}^{d_1} \left(\beta \sum_{z=1}^{d_2} \sum_{x=1}^{d_3} \sum_{v=1}^{d_4} \sum_{q=1}^{m'} \frac{\partial f_{\text{netConn}}(i^*, z^*, x^*, v^*, q^*)}{\partial \text{num}_i} \right) \times \\ &(\text{num}_i - \text{num}_i^*) + \sum_{i=1}^{d_1} \sum_{z=1}^{d_2} \eta_{2i}^* \times (\lambda_{i,z} - \lambda_{i,z}^*) - \end{aligned}$$

$$\sum_{i=1}^{d_1}\sum_{z=1}^{d_2}\left(\beta\sum_{x=1}^{d_3}\sum_{v=1}^{d_4}\sum_{q=1}^{m'}\frac{\partial f_{\text{netConn}}(i^*,z^*,x^*,v^*,q^*)}{\partial\lambda_{i,z}}\right)\times$$
$$(\lambda_{i,z}-\lambda^*_{i,z})+\sum_{i=1}^{d_1}\sum_{x=1}^{d_3}\eta^*_{3i}\times(\rho_{i,x}-\rho^*_{i,x})-$$
$$\sum_{i=1}^{d_1}\sum_{x=1}^{d_3}\left(\beta\sum_{z=1}^{d_2}\sum_{v=1}^{d_4}\sum_{q=1}^{m'}\frac{\partial f_{\text{netConn}}(i^*,z^*,x^*,v^*,q^*)}{\partial\rho_{i,x}}\right)\times$$
$$(\rho_{i,x}-\rho^*_{i,x})+\sum_{i=1}^{d_1}\sum_{v=1}^{d_4}\eta^*_{4i}\times(\omega_{i,v}-\omega^*_{i,v})-$$
$$\sum_{i=1}^{d_1}\sum_{v=1}^{d_4}\left(\beta\sum_{z=1}^{d_2}\sum_{x=1}^{d_3}\sum_{q=1}^{m'}\frac{\partial f_{\text{netConn}}(i^*,z^*,x^*,v^*,q^*)}{\partial\omega_{i,v}}\right)\times$$
$$(\omega_{i,v}-\omega^*_{i,v})+$$
$$\sum_{i=1}^{d_1}\sum_{q=1}^{m'}\left(\eta^*_{1i}-\frac{\alpha\partial f_{\text{proConn}}(i^*,q^*)}{\partial\mu_{i,q}}\right)\times(\mu_{i,q}-\mu^*_{i,q})-$$
$$\sum_{i=1}^{d_1}\sum_{q=1}^{m'}\left(\beta\sum_{z=1}^{d_2}\sum_{x=1}^{d_3}\sum_{v=1}^{d_4}\frac{\partial f_{\text{netConn}}(i^*,z^*,x^*,v^*,q^*)}{\partial\mu_{i,q}}\right)\times$$
$$(\mu_{i,q}-\mu^*_{i,q})+$$
$$\sum_{i=1}^{d_1}(n^*_i-\sum_{z=1}^{d_2}\lambda^*_{i,z})\times(\eta_{2i}-\eta^*_{2i})+$$
$$\sum_{i=1}^{d_1}(n^*_i-\sum_{x=1}^{d_3}\rho^*_{i,x})\times(\eta_{3i}-\eta^*_{3i})+$$
$$\sum_{i=1}^{d_1}(n^*_i-\sum_{v=1}^{d_4}\omega^*_{i,v})\times(\eta_{4i}-\eta^*_{4i})+$$
$$\sum_{i=1}^{d_1}(n^*_i-\sum_{q=1}^{m'}\mu^*_{i,q})\times(\eta_{1i}-\eta^*_{1i})\geqslant 0,$$
$$\forall i,z,x,v,q,\eta_{1i},\eta_{2i},\eta_{3i},\eta_{4i}\in K_2 \tag{9}$$

4.3 Optimal energy consumption

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

$$f_{\text{eng}}=f_{\text{eng}}(i,x),\ i\in\{1,\dots,d_1\},x\in\{1,\dots,d_3\} \tag{10}$$

So the minimal energy consumption of each task is

$$\min\sum_{i=1}^{d_1}\sum_{x=1}^{d_3}f_{\text{eng}}(i,x),\ \rho_{i,x}\geqslant 0,\sum_{x=1}^{d_3}\rho_{i,x}\leqslant\text{num}_i \tag{11}$$

When $f_{\text{eng}}(i,x)$ is a continuous differentiable convex function, its equivalent variational inequality is

$$y_3=\sum_{i=1}^{d_1}\sum_{x=1}^{d_3}\left(\eta^*_{3i}+\frac{\partial f_{\text{eng}}(i,x)}{\partial\rho_{i,x}}\right)\times(\rho_{i,x}-\rho^*_{i,x})+$$
$$\sum_{i=1}^{d_1}\left(\sum_{x=1}^{d_3}\frac{\partial f_{\text{eng}}(i,x)}{\partial\text{num}_i}-\eta^*_{3i}\right)\times(\text{num}_i-\text{num}^*_i)+$$
$$\sum_{i=1}^{d_1}(\text{num}^*_i-\sum_{x=1}^{d_3}\rho^*_{i,x})\times(\eta_{3i}-\eta^*_{3i})\geqslant 0,$$
$$\forall i,x,\eta_{3i}\in K_3 \tag{12}$$

where $K_3\equiv\{(i,x,\eta_{3i})|\rho_{i,x}\geqslant 0,\text{num}_i\geqslant 0,\forall i,x\}$.

4.4 Optimal resilience

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

$$f_{\text{res}}=f_{\text{res}}(i,q),\ i\in\{1,\dots,d_1\},q\in\{1,\dots,m'\} \tag{13}$$

then the maximal global resilience is

$$\max\sum_{i=1}^{d_1}\sum_{q=1}^{m'}f_{\text{res}}(i^*,q^*) \tag{14}$$

subject to $\text{num}_i\geqslant 0$, $\mu_{i,q}\geqslant 0$, and $\sum_{q=1}^{m'}\mu_{i,q}\leqslant\text{num}_i$.

When $f_{\text{res}}(i,q)$ is a continuous differentiable convex function, its equivalent variational inequality is

$$y_4=\sum_{i=1}^{d_1}\sum_{q=1}^{m'}\left(\eta^*_{1i}-\frac{\partial f_{\text{res}}(i^*,q^*)}{\partial\mu_{i,q}}\right)\times(\mu_{i,q}-\mu^*_{i,q})+$$
$$\sum_{i=1}^{d_1}\sum_{q=1}^{m'}\left(-\frac{\partial f_{\text{res}}(i^*,q^*)}{\partial\text{num}_i}-\eta^*_{1i}\right)\times$$
$$(\text{num}_i-\text{num}^*_i)+$$
$$\sum_{i=1}^{d_1}\left(\text{num}^*_i-\sum_{q=1}^{m'}\mu^*_{i,q}\right)\times(\eta_{1i}-\eta^*_{1i})\geqslant 0,$$
$$\forall i,q,\eta_{1i}\in K_4 \tag{15}$$

where $K_4 = \{(i, q, \eta_{1i}) | \text{num}_i \geqslant 0,\ \mu_{i,q} \geqslant 0,\ \forall i, q\}$.

4.5 Equilibrium expression

Global optimal performance, called equilibrium performance, is a trade-off among the four performances mentioned in Sections 4.1 – 4.4. These performances are usually interdependent and interactive. For addressing the equilibrium constraint problem of KMP, we need to find a feasible solution ($\lambda_{i,z}, \rho_{i,x}, \omega_{i,v}, \mu_{i,q} \in \mathbb{R}^+$) of the following inequality:

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

Our models can be easily extended to describe more complicated or special application-oriented networks by adding more constraint conditions. For example, if limit $\sum_{i=1}^{d_1} \text{num}_i \leqslant \text{Number}$, Number $\in \mathbb{N}$, the discussed network will change from an infinite scalable one to a finite one.

5 Theoretical Analysis

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

Lemma 1 A solution of variational inequality Eq. (16) exists when all functions are continuous.

Proof In a sensor network, the number of nodes $\sum_{i=1}^{d_1} \text{num}_i$ is always finite. Considering that each element of vectors $\boldsymbol{\lambda}_i, \boldsymbol{\rho}_i, \boldsymbol{\omega}_i, \boldsymbol{\mu}_i$, and $\boldsymbol{\zeta}_i$ must be no more than its corresponding num_i, let $\boldsymbol{\zeta}_i$ be a vector whose element $\zeta_{i,c}\ (i = 1, \ldots, d_1, c = 1, \ldots, t')$ is the contribution of the i-th-class node to c-th key management task. A vector $\boldsymbol{u}$ consisting of $u_i\ (1 \leqslant i \leqslant 6)$ can be found which will make the feasible solution shown as Eq. (17) true. K is a closed convex subset. Since functions in Eq. (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. ■

$$\begin{aligned} K \equiv &\{(i, z, x, v, q) | 0 \leqslant i \leqslant u_1, 0 \leqslant z \leqslant u_2, \\ &0 \leqslant x \leqslant u_3,\ 0 \leqslant v \leqslant u_4,\ 0 \leqslant q \leqslant u_5, \\ &\forall i, z, x, v, q\} \end{aligned} \tag{17}$$

Lemma 2 The solution of variational inequality Eq. (16) is unique when all functions are continuous, differentiable, and convex.

Proof Functions f_{devCost}, f_{depCost}, $-f_{\text{proConn}}$, $-f_{\text{netConn}}$, f_{eng}, and f_{res} in Eq. (16) are continuous, differentiable, and convex. 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 the unique solution of a variational inequality, if F's solution exists, it's unique. ■

Lemma 3 Variational inequality Eq. (16) is Lipschiz continuous.

Proof According to the Lagrange mean value theorem, there must be a value $\xi \in [X_1, X_2]$ 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 the existence of $L > 0$ makes $L\|X_1 - X_2\| \geqslant \|f(X_1) - f(X_2)\|$ true. Hence, variational inequality Eq. (16) is Lipschiz continuous and L is its Lipschiz constant. ■

Lemmas 1, 2, and 3 prove that the equilibrium constraint expression is monotonic, Lipschiz continuous, and has a unique solution. Therefore, the improved Korpelevich method[15], as shown in Fig. 3, can be used to solve our variational inequality and return its unique optimal solution.

6 Numerial Example

According to Refs. [22, 23], some parameters are

Algorithm: Solve the variational inequality

Input:

$X^0 = (i_0, z_0, x_0, v_0, q_0) \in K$; //initialize

$\tau = 1$; //round number

$0 \leqslant \theta \leqslant \dfrac{1}{L}$; //$L$ – Lipschiz constant, θ – step length

$0 \leqslant \varepsilon \leqslant 1$; //a number small enough for convergence

Process:

$x_1 = i; x_2 = z; x_3 = x; x_4 = v; x_5 = q;$

for($l = 1; l < 6; l++$){

  while(max $|x_l^\tau - x_l^{\tau-1}| \geqslant \varepsilon$) do{

    if require $x_l^\tau \geqslant C$

      $\bar{x_l}^{\tau-1} = \max(C, x_l^{\tau-1} - \theta F(x_l^{\tau-1}))$;

      $x_l^\tau = \max(C, x_l^{\tau-1} - \theta F(\bar{x_l}^{\tau-1}))$;

    else

      $\bar{x}^{\tau-1} = \min(C, x^{\tau-1} - \theta F(x^{\tau-1}))$;

      $x^\tau = \min(C, x^{\tau-1} - \theta F(\bar{x}^{\tau-1}))$;

    endif

    $\tau = \tau + 1; X^\tau = (x_1^\tau, x_2^\tau, x_3^\tau, x_4^\tau, x_5^\tau)$;

}}

Output: X^τ

Fig. 3 Algorithm of the variational inequality.

picked as follows. Three kinds of heterogeneities are considered as listed in Table 1. The HA value of link heterogeneity, location heterogeneity, and density heterogeneity are $(0.9, 0.7)$, $(1, 0.2)$, and $(0.2, 0.3)$, respectively. The unit price and communication radius of normal nodes and advanced nodes are (10, 20 m) and (40, 40 m), respectively. In addition, all sensor nodes are omnidirectional antenna nodes, which can receive messages from any direction. The circuit consumption $e_{\text{ek}} = 0.533\,\mu\text{J/bit}$, the path loss exponent $\kappa = 2.5$, and the amplifier consumption $e_{\text{a}} = 10\,\mu\text{J}/(\text{bit}\cdot\text{m})$. The area of the monitoring region $A = 1\times10^5\,\text{m}^2$. The size of the key pool $\text{kp} = 1\times10^4$. The step length $\theta = 0.05$, and the end condition $\varepsilon = 1$. The EG scheme is adopted as a protocol example.

Without considering the time factor, an OVDM model for an EG scheme is established, as shown in Fig. 4. The HA values of each heterogeneity are depicted in the figure directly. The weight of $n_i \rightarrow \text{t1}$ equals to number of the i-th-class nodes, meaning that all nodes have a fair chance to execute each task. The weight of $n_i \rightarrow \text{m1}$ represents the optimal size of the key ring.

The network cost function is

$$\sum_{i=1}^{2}\left(f_{\text{devCost}\_i}(\text{num}_i)) + f_{\text{depCost}\_i}(\text{num}_i)\right) = 10\times\text{num}_1 + 40\times\text{num}_2 + 0.3\times(\text{num}_1+\text{num}_2) + 0.05\times10^4.$$

Let kr_1 and kr_2 be the size of the key rings of nodes n_1 and n_2, so the value of kr_1 and the value of kr_2 are m1_1 and m1_2, respectively; Let kp be the size of the key pool; the protocol connectivity functions are shown in Eq. (18).

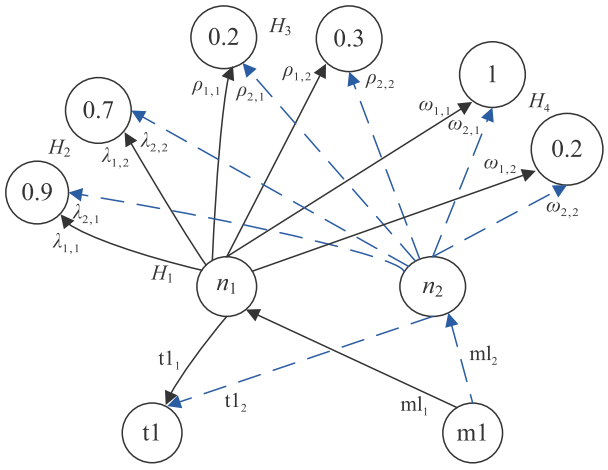

Fig. 4 OVDM for EG.

$$f_{\text{proConn}}(\text{num}_1,\text{kr}_1) = \left[1-\frac{C_{\text{kp}}^{\text{kr}_2}C_{\text{kp}-\text{kr}_2}^{\text{kr}_2}}{C_{\text{kp}}^{\text{kr}_2}C_{\text{kp}}^{\text{kr}_1}}\right]\times\frac{C_{\text{num}_2}^1C_{\text{num}_1}^1}{C_{\text{num}_2+\text{num}_1}^2} + \left[1-\frac{C_{\text{kp}}^{\text{kr}_1}C_{\text{kp}-\text{kr}_1}^{\text{kr}_1}}{(C_{\text{kp}}^{\text{kr}_1})^2}\right]\times\frac{C_{\text{num}_1}^2}{C_{\text{num}_2+\text{num}_1}^2}\approx \left[1-\frac{\left(1-\frac{\text{kr}_2}{\text{kp}}\right)^{\text{kp}-\text{kr}_2+0.5}\left(1-\frac{\text{kr}_1}{\text{kp}}\right)^{\text{kp}-\text{kr}_1+0.5}}{\left(1-\frac{\text{kr}_2}{\text{kp}}-\frac{\text{kr}_1}{\text{kp}}\right)^{\text{kp}-\text{kr}_2-\text{kr}_1+0.5}}\right]\times\frac{2\text{num}_2\text{num}_1}{(\text{num}_2+\text{num}_1)(\text{num}_2+\text{num}_1-1)} + \left[1-\frac{\left(1-\frac{\text{kr}_1}{\text{kp}}\right)^{2(\text{kp}-\text{kr}_1+0.5)}}{\left(1-\frac{2\text{kr}_1}{\text{kp}}\right)^{\text{kp}-2\text{kr}_1+0.5}}\right]\times\frac{\text{num}_1\times(\text{num}_1-1)}{(\text{num}_2+\text{num}_1)(\text{num}_2+\text{num}_1-1)} \tag{18}$$

Take second-level nodes for example; their number is equal to num_2, when the HA values of location heterogeneity, density heterogeneity, and link heterogeneity are ω, ρ, and λ, respectively, their probability of establishing a secure link with another n_2 node could be calculated as $\frac{\text{num}_2}{A}\times\pi(\omega\lambda\sigma)^2/[\pi(\omega\lambda\sigma)^2\rho] = \text{num}_2/\rho A$. Hence, the protocol connectivity functions are as shown as Eq. (19).

$$f_{\text{proConn}}(\text{num}_2,\text{kr}_2) = \left[1-\frac{C_{\text{kp}}^{\text{kr}_2}C_{\text{kp}-\text{kr}_2}^{\text{kr}_2}}{(C_{\text{kp}}^{\text{kr}_2})^2}\right]\times\frac{C_{\text{num}_2}^2}{C_{\text{num}_2+\text{num}_1}^2} + \left[1-\frac{C_{\text{kp}}^{kr_2}C_{\text{kp}-\text{kr}_2}^{\text{kr}_1}}{C_{\text{kp}}^{\text{kr}_2}C_{\text{kp}}\text{kr}_1}\right]\times\frac{C_{\text{num}_2}^1C_{\text{num}_1}^1}{C_{\text{num}_2+\text{num}_1}^2}\approx \left[1-\frac{\left(1-\frac{\text{kr}_2}{\text{kp}}\right)^{2(\text{kp}-\text{kr}_2+0.5)}}{\left(1-\frac{2\text{kr}_2}{\text{kp}}\right)^{\text{kp}-2\text{kr}_2+0.5}}\right]\times\frac{\text{num}_2\times(\text{num}_2-1)}{(\text{num}_2+\text{num}_1)(\text{num}_2+\text{num}_1-1)} + \left[1-\frac{\left(1-\frac{\text{kr}_2}{\text{kp}}\right)^{\text{kp}-\text{kr}_2+0.5}\left(1-\frac{\text{kr}_1}{\text{kp}}\right)^{\text{kp}-\text{kr}_1+0.5}}{\left(1-\frac{\text{kr}_2}{\text{kp}}-\frac{\text{kr}_1}{\text{kp}}\right)^{\text{kp}-\text{kr}_1-\text{kr}_2+0.5}}\right]\times\frac{2\text{num}_1\text{num}_2}{(\text{num}_2+\text{num}_1)(\text{num}_2+\text{num}_1-1)},$$
$$f_{\text{proConn}}(\text{num}_2,\text{kr}_1) = f_{\text{proConn}}(\text{num}_1,\text{kr}_2) = 0 \tag{19}$$

Similarly, we can get the network connectivities $f_{\text{netConn}}(1,1,1,1,1)$, $f_{\text{netConn}}(2,1,2,1,2)$, $f_{\text{netConn}}(1,1,2,1,1)$, $f_{\text{netConn}}(2,2,2,2,2)$,

$$f_{\text{netConn}}(1,1,1,1,1) = \frac{\lambda_{1,1}}{\lambda_{1,1}+\lambda_{1,2}} \times \frac{\rho_{1,1}}{\rho_{1,1}+\rho_{1,2}} \times \frac{\omega_{1,1}}{\omega_{1,1}+\omega_{1,2}} \times \left[\left(1 - \frac{C_{kp}^{kr_1} C_{kp-kr_1}^{kr_1}}{(C_{kp}^{kr_1})^2} \right) \times \frac{\text{num}_1}{0.2A} + \left(1 - \frac{C_{kp}^{kr_2} C_{kp-kr_2}^{kr_1}}{C_{kp}^{kr_1} C_{kp}^{kr_2}} \right) \times \frac{\text{num}_2}{0.2A} \right],$$

$$f_{\text{netConn}}(2,1,2,1,2) = \frac{\lambda_{2,1}}{\lambda_{2,1}+\lambda_{2,2}} \times \frac{\rho_{2,2}}{\rho_{2,1}+\rho_{2,2}} \times \frac{\omega_{2,1}}{\omega_{2,1}+\omega_{2,2}} \times \left[\left(1 - \frac{C_{kp}^{kr_2} C_{kp-kr_2}^{m_1}}{C_{kp}^{kr_2} C_{kp}^{kr_1}} \right) \times \frac{\text{num}_1}{0.3A} + \left(1 - \frac{C_{kp}^{kr_2} C_{kp-kr_2}^{m_2}}{(C_{kp}^{kr_2})^2} \right) \times \frac{\text{num}_2}{0.3A} \right].$$

In the 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 lists. If nodes that received this message find a match in their own key ID lists, they randomly choose a common key as a shared key. Every node needs to establish a direct shared key first, then two nodes in each other's communication range that have no common key established will start the indirect key establishment. A source node broadcasts a target ID; when a middle node sharing keys with both 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 antennas, every message sent by a node will be received by all nodes in its communication range. When a node is going to send l bits of data and its communication range is λ, the sending consumption $e_{\text{send}} = l(e_{\text{ek}} + e_a \lambda^{\kappa})$, the receiving consumption is $e_{\text{rec}} = l e_{\text{ek}}$[22]. So the broadcast consumption for establishing a direct shared key should be $e_1 = e_{\text{send}} + e_{\text{rec}} \lambda \rho$, and the consumption for establishing an indirect key is $e_2 = 2e_{\text{send}} + (\rho_{\text{source}} \lambda_{\text{source}} + \rho_{\text{middle}} \lambda_{\text{middle}}) e_{\text{rec}}$. 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 by middle node to be approximately the same as that of the source node. Therefore, the energy consumption function is

$$f_{\text{eng}}(1,1) = \frac{3\text{num}_1}{\text{num}_1+\text{num}_2} \times \frac{\rho_{1,1}}{\rho_{1,1}+\rho_{1,2}} \times (e_{\text{send}} + 0.2 \times 20 e_{\text{rec}}).$$

Functions $f_{\text{eng}}(1,2)$, $f_{\text{eng}}(2,1)$, and $f_{\text{eng}}(2,2)$ can be obtained in the same way. When one node is compromised, the resilience of an uncompromised node is equal to

$$f_{\text{res}} = \frac{\text{num}_1}{\text{num}_1+\text{num}_2} \times \frac{\text{kr}_1}{\text{kp}} + \frac{\text{num}_2}{\text{num}_1+\text{num}_2} \times \frac{\text{kr}_2}{\text{kp}}.$$

The solution to our model is found by using algorithm in Fig. 3 and values in Fig. 4, as shown in Table 2. We make values of solution be real numbers for the better accuracy. n represents the numbers of nodes n_1 and n_2; m_1 express the size of key rings of nodes. Keeping $\text{num}_1 + \text{num}_2$ constant reduces the value of variables by 30%, to generate two groups of data: *result_n*1 and *result_n*2. Expand the value in 1.5 times and obtain a new data *result_all_up*. Calculating the performance of each data group yields the result shown in Fig. 5.

It can be seen from Fig. 5, that though the resilience of data *result* is worse than that of *result_n*2, the performances in terms of connectivity, energy

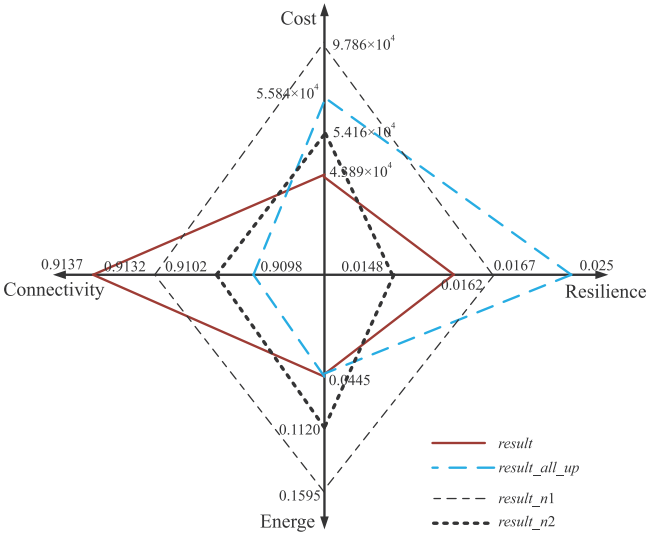

Fig. 5 OVDM for EG.

Table 2 Optimal result of OVDM.

Node	n	m_1	λ_1	λ_2	ρ_1	ρ_2	ω_1	ω_2	η_1	η_2	η_3	η_4
n_1	1910.76	164.93	1900	30.1	1050	900	887.7	1002.4	−1089	−382	−330	2
n_2	104.53	199.15	69.8	30	50	50	57.4	42.4	−3	1981	16 929	4

consumption, and cost are obviously better than those of the other three groups. And the other three performances of *result_n*2 are much worse than that of *result*. Comparing with *result*, when the number of n_1 decreases by 30%, the number of n_2 increases 30%, the cost and energy consumption of the protocol will increase, while the resilience decreases. When all values are replaced by bigger numbers, connectivity and resilience decrease, and the cost rises higher than *result*, while remaining lower than *result_n*1. Generally speaking, the model proposed in this paper solves the optimization problem of the key management protocol, and returns a global optimization of performance.

7 Conclusion

Based on supernetworks and variational inequality theory, we propose an optimal HA value distribution model and provide a method to find the optimal solution. Our model illustrates a simple way to depict the complex relationship between heterogeneities and protocols. The optimal result can help designers reasonably deploy a WSN so that 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 that will attain global optimal performance for key management protocols.

In the future, we will focus on the following two areas: (1) the time factor and its effect on heterogeneities and protocol performance, and (2) performance metrics besides cost, energy consumption, connectivity, and resilience.

Acknowledgment

This research was supported by the National Natural Science Foundation of China (Nos. 61170241 and 61472097), the Specialized Research Fund for the Doctoral Program of Higher Education (No. 20132304110017), and the Open Fund of the Key Lab of Network Security and Cryptography of Fujian Province (No. 150003).

References

[1] L. Hu, Z. Zhang, and F. Wang, Optimization of the deployment of temperature nodes based on linear programing in the internet of things, *Tsinghua Science and Technology,* vol. 18, no. 3 , pp. 250–258, 2013.

[2] M. Turkanovic, B. Brumen, and M. Holbl, 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,* vol. 20, pp. 96–112, 2014.

[3] N. Suganthi and S. Vembu, Energy efficient key management scheme for wireless sensor networks, *International Journal of Computers Communications Control,* vol. 9, no. 1, pp. 71–78, 2014.

[4] R. L. Novales, N. Mittal, and K. Sarac, KAIT: A parameterized key assignment scheme for confidential communication in resource constrained ad hoc wireless networks, *Ad Hoc Networks,* vol. 20, pp. 163–181, 2014.

[5] Z. Su, C. Lin, and F. J. Feng, Key management schemes and protocols for wireless sensor networks, *Journal of Software,* vol. 18, no. 5, pp. 1218–1231, 2007.

[6] C. Alcaraz, J. Lopez, and R. Roman, Selecting key management schemes for WSN applications, *Computers and Security,* vol. 31, no. 8, pp. 956–966, 2012.

[7] C. Cheng, Y. Qian, and D. Zhang, An approach based on chain key predistribution against sybil attack in wireless sensor networks, *International Journal of Distributed Sensor Networks*, vol. 2013, p. 839320, 2013.

[8] W. Bechkit, Y. Challal, and A. Bouabdallah, A highly scalable key predistribution scheme for wireless sensor networks, *IEEE Transactions on Wireless Communications,* vol. 12, no. 2, pp. 948–959, 2013.

[9] A. T. Boloorchi, M. H. Samadzadeh, and T. Chen, Symmetric Threshold Multipath (STM): An online symmetric key management scheme, *Information Sciences*, vol. 268, pp. 489–504, 2014.

[10] M. B. Paterson and D. R. Stinson, A unified approach to combinatorial key predistribution scheme for sensor networks, *Designs, Codes and Cryptography,* vol. 71, no. 3, pp. 433–457, 2014.

[11] M. Yarvis, N. Kushalnagar, and H. Singh, Exploiting heterogeneity in sensor networks, in *Proc. IEEE INFOCOM 2005*, Miami, USA, 2005, pp. 878–890.

[12] G. Zeng, B. Wang, and M. Mutka, Efficient multicast for link-heterogeneous wireless mesh networks, in *Proc. 28th International Performance Computing and Communications Conf.*, 2009, pp. 177–184.

[13] V. Katiyar, N. Chand, and S. Soni, Improving lifetime of large-scale wireless sensor networks through heterogeneity, in *Proc. 2011 International Conference on Emerging Trends in Electrical and Computer Technology*, Nagercoil, India, 2011, pp. 1032–1036.

[14] C. M. Chen, X. Zheng, and T. Y. Wu, A complete hierarchical key management scheme for heterogeneous wireless sensor networks, *The Scientific World Journal*, vol. 2014, p. 816549, 2014.

[15] Z. P. Wang and Z. T. Wang, *Supernetworks Theory and Applications*. New York, USA: Science Press, 2008.

[16] Z. P. Wang, S. B. Zhou, and J. F. Guo, Variational-inequality-based supernetworks model for network advertisement distribution, *Journal of Dalian Maritime University,* vol. 33, no. 4, pp. 26–30, 2007.

[17] W. M. Han and X. L. Chen. *An Introduction to Variational Inequality: Elecmentary Theory, Numerical Analysis and Applications*, (in Chinese). Beijing, China: Higher Education Press, 2007.

[18] J. K. Kim and B. T. Zhang, Evolving hypernetworks for pattern classification, in *Proc. 2007 IEEE Congress on Evolutionary Computation*, Tokyo, Japan, 2007, pp. 1856–1862.

[19] A. T. Erman, A. Dilo, and L. Hoesel, On mobility management in multi-sink sensor networks for geocasting of queries, *Sensors,* vol. 11, no. 12, pp. 11415–11446, 2011.

[20] C. L. Chen, Y. T. Tsai, and A. Castiglione, Using bivariate polynomial to design a dynamic key management scheme for wireless sensor networks, *Computer Science and Information Systems,* vol. 10, no. 2, pp. 589–609, 2013.

[21] J. H. Lee and T. Kwon, GENDEP location-aware key management for general deployment of wireless sensor networks, *International Journal of Distributed Sensor Networks*, vol. 2014, p. 490202, 2014.

[22] J. Haapola, Z. Shelby, and R. C. Pomalaza, Cross-layer energy analysis of multi-hop wireless sensor network, in *Proc. European Conference on Wireless Sensor Networks*, Istanbul, Turkey, 2005, pp. 33–44.

[23] W. L. Du, J. Deng, and Y. S. Han, A key predistribution scheme for sensor networks using deployment knowledge, *IEEE Transactions on Dependable and Secure Computing,* vol. 3, no. 1, pp. 62–77, 2006.

Qi Yuan received the BS degree from Heilongjiang University, China, in 1995, and the MS degree from Capital Normal University, China, in 2007. She is currently a PhD student at Harbin Engineering University, China, and an associate professor in Qiqihar University, China. Her research interests include wireless sensor network security and game theory.

Xiaorui Zhong is currently an engineer of China Academy of Electronics and Information Technology. She received the BS and PhD degrees from Harbin Engineering University in 2009 and 2014, respectively. Her research interests include big data, information system security, and system integration.

Gang Du received the BS degree from University of New England, Australia, in 1997, and the MS degree from the University of Sydney, Australia, in 2008. He is currently a PhD student at Harbin Engineering University, China, and a lecturer in the New Oriental Education and Technology Group. His research interest is private information retrial.

Jiansheng Yao received the BS degree from Jilin Normal University, China, in 2003, and the MS degree from Harbin Engineering University in 2010. He is currently a PhD student at Harbin Engineering University, and a lecturer in Jilin Normal University. His research interests include wireless sensor network and delay tolerant network.

Chunguang Ma is currently a professor and doctorial supervisor of College of Computer Science and Technology at Harbin Engineering University, China. He got the BS degree in applied mathematics from Heilongjiang University, China, in 1996, and the MS degree in computer applied technology from Qiqihar University, China, in 2002. He received the PhD degree in cryptography from Beijing University of Posts and Telecommunications, China, in 2005. He is a senior member of China Computer Federation (CCF) and a director of Chinese Association for Cryptologic Research (CACR). His research is focused on cyptography, information security, privacy preserving, and mobile Ad hoc networking and computing.