ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.9, September 2009, pp.2531−2541
doi: 10.3724/SP.J.1001.2009.03366

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于 EBS 的动态密钥管理方法共谋问题*

孔繁瑞[1+], 李春文[1], 丁青青[2], 焦 飞[2], 谷琦彬[2]

[1](清华大学 自动化系,北京 100084)

[2](清华大学 电机工程与应用电子技术系 电力系统及发电设备安全控制和仿真国家重点实验室,北京 100084)

Collusion Problem of the EBS-Based Dynamic Key Management Scheme

KONG Fan-Rui[1+], LI Chun-Wen[1], DING Qing-Qing[2], JIAO Fei[2], GU Qi-Bin[2]

[1](Department of Automation, Tsinghua University, Beijing 100084, China)

[2](State Key Laboratory of Control and Simulation of Power System and Generation Equipment, Department of Electrical Engineering, Tsinghua University, Beijing 100084, China)

+ Corresponding author: E-mail: kongfr@mails.thu.edu.cn

Kong FR, Li CW, Ding QQ, Jiao F, Gu QB. Collusion problem of the EBS-based dynamic key management scheme. *Journal of Software*, 2009,20(9):2531−2541. http://www.jos.org.cn/1000-9825/3366.htm

Abstract: The security of wireless sensor networks has attracted much attention in recent years and the key management is the focus. EBS-based dynamic key management scheme is a new approach for wireless sensor networks. Its major advantages are its enhanced network survivability, high dynamic performance and better support for network expansion. But it suffers from the collusion problem, which means it is prone to the cooperative attack of the compromised nodes. In this paper, the feature of the collusion problem is analyzed and an optimization model is proposed, maximizing the length of the shortest collusion chain, which is the key issue of the problem. A discrete particle swarm optimization algorithm for the collusion problem is also presented based on the optimization model proposed. Simulation results show that compared with the former works, the resilience of the network and the difficulty to compromise the whole network are both greatly improved.

Key words: wireless sensor networks; security; EBS-based dynamic key management; collusion problem; DPSO

摘 要: 设计安全、合理的密钥管理方法是解决无线传感器网络安全性问题的核心内容.基于 exclusion basis system(EBS)的动态密钥管理方法由于安全性高,动态性能和可扩展性好,受到了广泛关注.但在这种方法中存在共谋问题,即对于被捕获节点通过共享各自信息实施的联合攻击抵抗性较差.针对这一问题,分析了传感器节点形成共谋过程中的特点,以最短共谋链的长度为目标提出了共谋问题的优化模型.在此基础上,提出了基于离散粒子群算法的无线传感器网络共谋问题优化方法.仿真实验结果表明,与前人的工作相比,采用此优化模型和方法不仅提高了捕获网络难度,而且显著增强了网络对捕获节点的抵抗性.

关键词: 无线传感器网络;安全性;基于 EBS 的动态密钥管理;共谋问题;离散粒子群算法

中图法分类号: TP393 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant Nos.69774011, 60433050 (国家自然科学基金)
Received 2007-12-27; Accepted 2008-04-30

无线传感器网络(wireless sensor networks,简称 WSNs)是一种由大量密集部署的智能传感器节点构成的网络应用系统[1−4].它集成了传感器技术、微机电系统技术、无线通信技术和分布式信息处理技术等,被广泛应用在军事、民事领域,包括战场监测、国土安全、反恐防爆、环境监测、医疗保健等[1,2,5],能够完成传统系统无法完成的任务.

在许多军事领域的应用中,WSNs 往往工作在作战区域,面临着恶意的信号干扰或是对传感器节点的捕获、篡改和破坏.在这种情况下,保证数据的完整性、准确性显得尤为重要.而在一些民事领域的应用中,例如智能大厦,网络数据包含的用户个人信息应受到保护,避免被监听、泄露.这需要对数据的私密性进行保护.因此,近年来 WSNs 的网络安全问题得到了广泛的重视[6−8].由于 WSNs 具有网络拓扑结构不可预知、传感器节点能量有限、资源(包括计算资源、存储资源和通信资源)有限等特点,传统的具有 Internet 特色的安全体系——基于第三方的公共密钥安全体系并不适合 WSNs,甚至是根本无法使用的[9,10].2002 年,Eschenauer 和 Gligor 提出的密钥预分配(key pre-distribution)方法[11]被认为是一种合理的无线传感器网络密钥管理方式,并得到了很多重要的推广及应用[12−15],但这些方法都是在一个固定的密钥池中,分配给各个节点一些固定的组合,是一种静态的密钥管理方法(static key management).2006 年,Eltoweissy 在 exclusion basis systems(EBS)[16]和传感器网络的分簇结构的基础上提出了动态密钥管理的概念(dynamic key management)[17],它与静态密钥管理相比,主要优点在于:

(1) 可在全网范围内动态且高效地取消任意节点所拥有的全部密钥,从而驱逐被敌人捕获的节点,提高了网络的安全性能.

(2) 在提供同等安全性保证的前提下,相比静态密钥管理既节约了存储空间,又提高了能量效率[17−19].

因此,基于 EBS 的动态密钥管理方法也成为了无线传感器网络动态密钥分配研究的基础[20−23].本文针对基于 EBS 的无线传感器网络动态密钥分配方法中的共谋问题(collusion problem),提出了 p 跳矩阵的概念,利用 p 跳矩阵求出密钥分配与共谋跳数(hops to collude)之间的关系,进而建立了共谋问题的优化模型,并在此基础上采用离散粒子群优化算法(discrete particle swarm optimization algorithm)进行了密钥分配的优化设计.仿真结果表明,相比于随机分配和 Shell[19],采用本文的分配方式,网络的安全性能得到了显著的提高.

1 基于 EBS 的无线传感器网络动态密钥管理中共谋问题的描述

1.1 EBS和基于EBS的无线传感器网络动态密钥管理方法

EBS 是由 Eltoweissy 等人于 2004 年提出来的一种基于组合原理的组通信密钥管理方法[16].

定义 1(EBS(n,k,m)). 设 n,k,m 均为正整数,且 $1<k,m<n$. EBS(n,k,m)是以集合 $\{1,2,...,n\}$ 的子集为元素构成的集合 Γ,并且对于 $\forall t\in\{1,2,...,n\}$ 满足以下两个条件:

(1) t 最多出现在 Γ 的 k 个元素中.

(2) Γ 中恰好有 m 个元素, $A_1,A_2,...,A_m$,它们的并集 $\bigcup_{i=1}^{m}A_i=\{1,2,...,n\}-\{t\}$ (意味着任何一个用户 t 都可以由恰好 m 个集合排斥掉).

在 EBS(n,k,m)中, n 表示节点数目,k 表示分配给每个节点的密钥个数,$k+m$ 表示密钥总数.可以证明[16]:

1. 当 $\binom{k+m}{k}\geq n$ 时, $\binom{k+m}{k}$ 中的任意 n 个组合方式均可构成 EBS(n,k,m),进而形成一个密钥的分配方案.
2. 通过广播最多 m 个数据包可以取消并更新任意节点拥有的全部密钥,从而驱逐该节点.

例如当 n=8,k=3,m=2 时,密钥分配方案见表 1 中的 EBS 矩阵 M 所示,$M(i,j)$为 1 表示密钥 K_i 分配给节点 N_j. 若要取消并更新 N_1 所具有的密钥 K_3,K_4,K_5,只需广播以下 2 个数据包:

(a) $E_{K_1}(S',E_{K_3}(K_3'),E_{K_4}(K_4'),E_{K_5}(K_5'))$;

(b) $E_{K_2}(S',E_{K_3}(K_3'),E_{K_4}(K_4'),E_{K_5}(K_5'))$.

$E_{K_i}(x)$ 表示以密钥 K_i 对数据 x 进行加密, K_i' 表示密钥 K_i 的更新,S'为新的会话密钥.

Table 1 Matrix of EBS
表 1 EBS 矩阵

	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8
K_1	0	0	0	0	1	1	1	1
K_2	0	1	1	1	0	0	0	1
K_3	1	0	1	1	0	1	1	0
K_4	1	1	0	1	1	0	1	0
K_5	1	1	1	0	1	1	0	1

1.2 基于EBS的无线传感器网络动态密钥管理中的共谋问题描述

文献[16–23]均指出,基于 EBS 的无线传感器网络动态密钥系统中存在共谋问题(collusion problem),而且是影响其安全性的主要因素.敌人可以通过捕获节点的方式来获得节点所拥有的密钥,攻击密钥体系,当捕获的节点处于各自的通信半径之内时,即互为邻居节点时,这些节点便会形成共谋(collusion),共享并扩大它们对系统密钥的捕获,进而破坏整个密钥系统,使网络失去安全保障.

图 1 为共谋问题的示意图,节点之间的连线表示它们之间的邻居关系.如图 1(a)所示,虽然节点 1 和 3 均被捕获,但由于他们并不能直接通信,所以他们之间无法形成共谋.但当节点 2 也被捕获时,如图 1(b)所示,3 个节点之间形成了一条捕获通道,他们可以交换各自捕获的密钥信息,对密钥系统的危害相当于 3 个单独节点的综合.

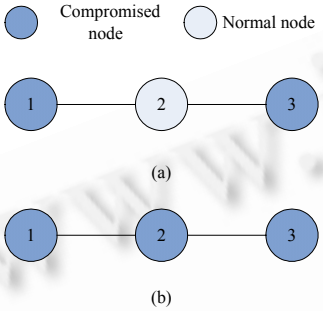

Fig.1 Illusion of the collusion problem
图 1 共谋问题示意图

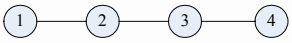

Fig.2 A simplified network
图 2 简单的网络示意图

在进一步讨论共谋问题及其特性之前,我们给出以下定义:

定义 2(连通链). 网络中的一个节点集,其中任意两个节点都可以通过单跳或多跳互相到达.

定义 3(共谋链). 网络中的一条连通链,其上节点所拥有的密钥总和为全部密钥空间.

定义 4(共谋链长度). 共谋链上的节点个数.

显然,当被捕获的节点构成一条共谋链时,网络的密钥体系会被完全破坏,网络中的所有通信都将面临着被阻塞、篡改,丢弃的危险.在一个具有复杂拓扑结构的无线传感器网络中,可能会存在多条共谋链.而节点被捕获可以认为是独立同分布的事件[19],因此在所有共谋链中,长度最短的共谋链是网络安全的最薄弱环节.而共谋链的长度与节点的密钥分配方案是直接相关的,针对同一个网络,不同的密钥分配方案会带来不同的共谋链分布,其最短共谋链长度也是不同的.因此优化密钥的分配方案,最大化最短共谋链长度,是解决共谋问题的根本途径.

2 最短共谋链长度的计算与共谋问题的优化模型

2.1 符号表

在给出最短共谋链长度的计算方法和优化模型之前,先将使用到的符号及其含义表述如下:

Table 2 Notations and their meanings
表 2 符号及其含义

Notation	Implication	Notation	Implication
N	Set of nodes	N_c	Number of nodes
n_i	$n_i \in N$, node i	d	Communication radius, two nodes are neighbors if their distance is less than
V	$V \subseteq N \times N, (n_i,n_j) \in V$ if the distance between n_i,n_j is less than d	$k+m$	Number of all keys
k	The number of keys every nodes has	m	Number of packets needed to evacuate a node
x_i	Node n_i's key distribution scheme, $k+m$ bit binary number, 1 in bit j represents having the key, 0 otherwise	$\dim(\bullet)$	Dimension of a node serial.
A	Initial state matrix	C	Single matrix
D_p	P matrix	$D_p(i,j,\mu)$	Element μ of $D_p(i,j)$,which is a node serial
$\lvert\bullet\rvert$	Number of keys of a node serial		

2.2 节点序列和p跳状态矩阵

共谋链是由互相连通的节点构成,可以把它看作是从起始节点通过多跳遍历链上的所有节点,从而逐跳扩大捕获密钥范围的动态过程,因此,共谋链及其长度与网络中任意两个节点之间的连通路径有着密切的关系.本文采用 p 跳状态矩阵来表达这种动态跳跃过程和任意两个节点之间的连通路径.

定义 5(节点序列). $n_{t_1}n_{t_2}...n_{t_l}$ 被称作一个从节点 n_{t_1} 到 n_{t_l} 长度为 l 的节点序列,若 $\forall i,1<i\le l$ 都有 $(n_{t_{i-1}},n_{t_i})\in V$.

定义 6(节点序列的维度). 节点序列 $n_{t_1}n_{t_2}...n_{t_l}$ 的维度记作 $\dim(n_{t_1}n_{t_2}...n_{t_l})$,表示节点序列中包含节点的个数.

节点序列 $n_{t_1}n_{t_2}...n_{t_l}$ 实际上表达了从节点 n_{t_1} 通过 l–1 跳到达节点 n_{t_l} 的一种方式.但要注意,这里的结点序列是一种松弛的表达形式,节点可以重复,所以节点的维度与其长度是不一样的,维度通常不大于长度.

定义 7(初始状态矩阵和单跳矩阵).

初始状态矩阵 A 和单跳矩阵 C 均为 $N\times N$ 的方阵,元素为节点序列的集合:

$$A(i,j)=\begin{cases}\{n_i\}, i=j\\ \varnothing, \text{否则}\end{cases}\quad C(i,j)=\begin{cases}\{n_i\},(n_i,n_j)\in V\\ \varnothing, \text{否则}\end{cases}.$$

初始状态矩阵 A 表达了网络的初始状态,单跳矩阵 C 表示了网络的邻居节点关系和从任意节点通过一跳达到另一节点的过程中,节点序列的变化情况.

为了描述初始状态矩阵和单跳矩阵之间的运算,我们同时定义:

定义 8(运算⊕和⊗).

节点序列集合 $A=\{a_i\mid 0<i\le n_a\}$ 和 $B=\{b_j\mid 0<j\le n_b\}$ 作 $\oplus$ 运算, $A\oplus B=\{a_ib_j\mid 0<i\le n_a,0<j\le n_b\}$.空集与任何集合作⊕运算仍是空集, $\forall A, A\oplus\varnothing=\varnothing\oplus A=\varnothing$.

元素为节点序列集合的矩阵 P,Q.P 为 $p\times g$ 的矩阵,Q 为 $p\times g$ 的矩阵,$P\otimes Q$ 为 $p\times q$ 的矩阵, $(P\otimes Q)(i,j)=\bigcup_t P(i,t)\oplus Q(t,j)$.

两个节点序列集合作⊕运算,表示两个集合中的节点序列做连接所构成的节点序列集合,⊕运算与数的乘法运算类似,只是将两个数相乘变为了两个节点序列集合的连接.而⊗运算与矩阵的乘法运算类似,只是用⊕取代了数的乘法,用集合的并运算取代了数的加法.定义这两种运算为进一步简化求取共谋链长度提供了便利.下面我们将给出 p 跳状态矩阵的概念及其重要特性.

定义 9(p 跳状态矩阵). p 跳状态矩阵 $D_p=A\otimes\underbrace{C\otimes C...\otimes C}_{p\text{个}}$.

定理 1. $D_p(i,j)$是所有从节点 n_i 到 n_j 长度为 p+1 的节点序列构成的集合.

证明:采用数学归纳法来证明.当 p=1 时,$D_1 = A \otimes C$,$(AC)(i,j) = n_i \oplus C(i,j) = \begin{cases} \{n_i n_j\}, (ni,nj) \in V \\ \varnothing, \quad \text{否则} \end{cases}$,显然结论在 p=1 时是成立的.

假设当 p=s 时也成立.即 $D_s(i,j)$是所有从节点 n_i 到 n_j 长度为 s+1 的节点序列的集合.

当 p=s+1 时,$D_{s+1} = D_s \otimes C$,$D_{s+1}(i,j) = \left[\bigcup_t D_s(i,t) \oplus C(t,j)\right] = \left[\bigcup_{(t,j)\in V}^{t} D_s(i,t) \oplus n_j\right]$,因为 $D_s(i,t)$表示所有从节点 n_i 到 n_t 长度为 s+1 节点序列的集合,而$(t,j)\in V$,所以 $\left[\bigcup_{(t,j)\in V}^{t} D_s(i,t) \oplus n_j\right]$ 表示所有从节点 n_i 到 n_j 长度为 s+2 的节点序列的集合,即 p=s+1 时结论也成立. □

例如图 2 所示的网络拓扑结构,显然 $A = \begin{bmatrix} n_1 & 0 & 0 & 0 \\ 0 & n_2 & 0 & 0 \\ 0 & 0 & n_3 & 0 \\ 0 & 0 & 0 & n_4 \end{bmatrix}$,$C = \begin{bmatrix} n_1 & n_2 & 0 & 0 \\ n_1 & n_2 & n_3 & 0 \\ 0 & n_2 & n_3 & n_4 \\ 0 & 0 & n_3 & n_4 \end{bmatrix}$,将 $A \otimes C \otimes C$ 简记作 AC^2,则:

$$D_2 = AC^2 = \begin{bmatrix} \{n_1n_1n_1, n_1n_2n_1\} & \{n_1n_1n_2, n_1n_2n_2\} & \{n_1n_2n_3\} & \varnothing \\ \{n_2n_1n_1, n_2n_2n_1\} & \{n_2n_1n_2, n_2n_2n_2, n_2n_3n_2\} & \{n_2n_2n_3, n_2n_3n_3\} & \{n_2n_3n_4\} \\ \{n_3n_2n_1\} & \{n_3n_2n_2, n_3n_3n_2\} & \{n_3n_2n_3, n_3n_3n_3, n_3n_4n_3\} & \{n_3n_3n_4, n_3n_4n_4\} \\ \varnothing & \{n_4n_3n_2\} & \{n_4n_3n_3, n_4n_4n_3\} & \{n_4n_3n_4, n_4n_4n_4\} \end{bmatrix}.$$

$D_2(i,j)$ 表示从 n_i 到 n_j 长度为 3 的节点序列的集合,例如: $D_2(1,3) = \{n_1n_2n_3\}$ 表示两跳从 n_1 到 n_3 所经过的节点为 n_1,n_2,n_3. $D_2(2,3) = \{n_2n_2n_3, n_2n_3n_3\}$ 表示两跳从 n_2 到 n_3 所经过的节点为 n_2,n_2,n_3 或 n_2,n_3,n_3.

2.3 最短共谋链长度的计算与共谋问题的优化模型

如上节所述,$D_p(i,j)$是从节点 n_i 到 n_j 所有长度为 p+1 的节点序列的集合,可以证明网络中任意一个共谋链,都与 $D_p(i,j)$中的某一个节点序列存在着对应关系.可以在这些共谋链对应的节点序列中,找到最短共谋链所对应的节点序列,计算出最短共谋链的长度,进而将它作为优化目标建立优化模型.

定理 2. p 跳状态矩阵 D_p,若存在 i,j,μ,使得 $\left|D_p(i,j,\mu)\right| = k+m$,则由节点序列 $D_p(i,j,\mu)$所包含的全部节点构成的集合 $S = \{n_t \mid n_t \in D_p(i,j,\mu)\}$ 为一共谋链.

证明:由定理 1 可知,$D_p(i,j,\mu)$为从节点 n_i 到 n_j 的长度为 p+1 的一个节点序列,故 S 是连通的.又因为 $\left|D_p(i,j,\mu)\right| = k+m$,所以 S 所拥有的密钥个数也为 k+m,即 S 拥有整个密钥空间.所以 S 符合共谋链的定义,它是一个共谋链.证毕. □

定理 3. 对于任意共谋链 L_θ,都可以找到节点序列 $D_p(i,j,\mu)$,使得 $D_p(i,j,\mu)$所包含的节点构成的集合 $S = \{n_q \mid n_q \in D_p(i,j,\mu)\} = L_\theta$.

证明:可以采用构造的办法来证明这个结论.假设共谋链 L_θ由节点 $n_{\theta_1}, n_{\theta_2}, ..., n_{\theta_l}$ 构成.由于共谋链是连通链,所以从节点 n_{θ_1} 到 n_{θ_2} 可以找到一个节点序列 $n_{\theta_1} n_{\theta_{t_1}} n_{\theta_{t_2}} ... n_{\theta_{t_s}} n_{\theta_2}$,起始于 n_{θ_1},终止于 n_{θ_2},且遍历所有节点 $n_{\theta_1}, n_{\theta_2}, ..., n_{\theta_l}$.由定理 1 可知,$D_{s+1}(\theta_1,\theta_2)$ 是所有从节点 n_{θ_1} 到 n_{θ_2} 长度为 s+2 的节点序列的集合,所以 $n_{\theta_1} n_{\theta_{t_1}} n_{\theta_{t_2}} ... n_{\theta_{t_s}} n_{\theta_2} \in D_{s+1}(\theta_1,\theta_2)$,因此存在 $D_{s+1}(\theta_1,\theta_2,\mu) = n_{\theta_1} n_{\theta_{t_1}} n_{\theta_{t_2}} ... n_{\theta_{t_s}} n_{\theta_2}$.又因为 $n_{\theta_1} n_{\theta_{t_1}} n_{\theta_{t_2}} ... n_{\theta_{t_s}} n_{\theta_2}$ 遍历了 L_θ 的所有节点,所以 $D_{s+1}(\theta_1,\theta_2,\mu)$ 所包含的节点构成的集合 $S = \{n_q \mid n_q \in D_{s+1}(\theta_1,\theta_2,\mu)\} = L_\theta$,原命题成立.证毕. □

有了定理 2 和定理 3,我们便可以证明,通过逐步扩大 p 跳状态矩阵的跳数 p,能够准确地得到最短共谋链所对应的节点序列,并求得其长度.

定理 4. 如果存在 D_{p_0}, i_0, j_0, μ_0 使得 $\left|D_{p_0}(i_0,j_0,\mu_0)\right| = k+m$,而 $\forall q < p_0 \ \max_{i,j,\mu} \left|D_q(i,j,\mu)\right| < k+m$,则从 D_{p_0} 到 D_{2H_0-4} 所有拥有整个密钥空间的节点序列中,维度最小的节点序列所对应的共谋链是网络中长度最短的共谋

链,其中 $H_0=\dim[D_{p_0}(i_0,j_0,\mu_0)]$.

证明:设从 D_{p_0} 到 D_{2H_0-4} 所有拥有整个密钥空间的节点序列中,维度最小的节点序列为 $D_{p_{\min}}(\alpha,\beta,\gamma)$,令

$$H_{\min}=\dim[D_{p_{\min}}(\alpha,\beta,\gamma)],$$

所以

$$D_{p_{\min}}(\alpha,\beta,\gamma)\in\{D_t(i,j,\mu)\big||D_t(i,j,\mu)|=k+m,p_0\le t\le 2H_0-4\}$$

且

$$\dim[D_{p_{\min}}(\alpha,\beta,\gamma)]=\min(\dim[D_t(i,j,\mu)]),$$

$$\forall D_t(i,j,\mu)\in\{D_t(i,j,\mu)\big||D_t(i,j,\mu)|=k+m,p_0\le t\le 2H_0-4\}.$$

设 $D_{p_{\min}}(\alpha,\beta,\gamma)$ 所对应的共谋链为 L,需要证明的是 L 即为网络中长度最短的共谋链.

采用反证法.设 L 的长度为 $l_{\min}$,因为 $D_{p_{\min}}(\alpha,\beta,\gamma)$ 所对应的共谋链为 L,所以 $l_{\min}$=$H_{\min}$.假设最短共谋链不是 L 而是 L',其长度 l'<$l_{\min}$.由定理 3 可知,存在节点序列 $D_{p'}(\alpha',\beta',\gamma')$,满足 $D_{p'}(\alpha',\beta',\gamma')$ 所包含的节点构成的集合 $S=\{n_q\big|n_q\in D_{p'}(\alpha',\beta',\gamma')\}=L'$,令 $H'=\dim[D_{p'}(\alpha',\beta',\gamma')]$,则 l'=H'.由旅行商问题的结论可知,对于任意一个具有 t 个顶点的无向连通图,遍历其所有节点所需要的最少跳数不大于 2t–4,而共谋链可以看作是一个无向连通图,所以 p'≤2H'−4.

因为 $\left|D_{p'}(i',j',\mu')\right|=k+m$,所以 $p'\ge p_0$.若 $p'>2H_0-4$,则 $2H_0-4<2H'-4$,$H_0<H'$,这与 L' 为最短共谋链的假设相矛盾.若 $p'\le 2H_0-4$,则

$$D_{p'}(\alpha',\beta',\gamma')\in\{D_t(i,j,\mu)\big||D_t(i,j,\mu)|=k+m,p_0\le t\le 2H_0-4\},$$

而

$$\dim[D_{p_{\min}}(\alpha,\beta,\gamma)]=\min_{i,j,\mu}\{\dim[D_t(i,j,\mu)]\big||D_t(i,j,\mu)|=k+m,p_0\le t\le 2H_0-4\},$$

所以 $l_{\min}\le l'$,这与 $l'<l_{\min}$ 矛盾.

综上,前提假设——最短的不是共谋链 L 而是 L'是错误的,而原命题 $D_{p_{\min}}(\alpha,\beta,\gamma)$ 所对应的共谋链 L 即为网络中长度最短的共谋链是正确的,最短共谋链 L 的长度为 $l_{\min}$.证毕. □

实际上,定理 4 也给出了计算最短共谋链长度的方法,首先逐步扩大 p 跳状态矩阵的跳数找到 D_{p_0} 确定 H_0,再在 D_{p_0} 到 D_{2H_0-4} 中寻找拥有全部密钥空间的所有节点序列中维度最小的一个,它的维度即为最短共谋链的长度.以最短共谋链长度为优化目标便可以得到共谋问题的优化模型.

优化变量为密钥的分配方案 X,是一个 $N_c\times(k+m)$的矩阵,其元素为 1 或 0,若将密钥 k_j 分配给节点 n_i 则 $X(i,j)$=1,否则 $X(i,j)$=0.目标函数为最短共谋链的长度.因此,共谋问题的优化模型可以表述如下:

$$\max\quad f(X)=\min(\dim[D_t(i,j,\mu)])$$

$$\text{s.t.}\quad\begin{cases}D_t(i,j,\mu)\in\{D_t(i,j,\mu)\big||D_t(i,j,\mu)|=k+m,p_0\le t\le 2H_0-4\}\\ \sum_{\beta=1}^{k+m}X(\alpha,\beta)=k\\ i,j,\mu,t,\alpha,\beta\in Z\\ 1\le i,j,\alpha\le N_c,1\le\beta\le k+m\end{cases}$$

3 共谋问题的离散粒子群优化方法

Eberhart 和 Kennedy 受鸟群觅食行为的启发于 1995 年提出了基本粒子群优化(particle swarm optimization,简称 PSO)方法[24].PSO 是一种基于群智能的进化计算技术,通过群体中粒子间的合作产生的群体智能指导优化搜索过程,已经成功运用在很多连续优化问题上[25,26].Eberhart 和 Kennedy 针对离散优化问题,于 1997 年又提出了二进制离散粒子群算法(discrete binary version of the particle swarm optimization,简称 DPSO),简称离散粒子群算法[27].本文采用的便是这种 DPSO 方法来对共谋问题进行优化的.

3.1 基本粒子群算法与离散粒子群算法

在基本粒子群算法中,每个粒子位置 $X_i=(x_{i_1},x_{i_2},...,x_{i_D})$ 代表一个可能的最优解,其速度 $V_i=(v_{i_1},v_{i_2},...,v_{i_D})$ 代表粒子两次迭代过程中的位移.每次迭代过程中,根据当前的粒子个体最优解 $p_i=(p_{i_1},p_{i_2},...,p_{i_D})$ 和群体最优解 $g=(g_1,g_2,...,g_D)$ 来更新粒子的位置和速度,其中 t,t+1 表示迭代次数,$rand1$,$rand2$ 是介于(0,1)之间的随机数,w 是惯性常数,c_1,c_2 是加速度常数.

$$v_{i_d}(t+1)=wv_{i_d}(t)+c_1rand_1[p_{i_d}-x_{i_d}(t)]+c_2rand_2[g_d-x_{i_d}(t)],$$

$$x_{i_d}(t+1)=x_{i_d}(t)+v_{i_d}(t).$$

离散粒子群算法在基本粒子群算法基础上,利用 sigmoid 函数将粒子的速度从实数空间转变到概率空间,进而求得粒子的位置,粒子位置及速度更新方法如下,其中 $rand3$ 是介于(0,1)之间的随机数.

$$v_{i_d}(t+1)=wv_{i_d}(t)+c_1rand_1[p_{i_d}-x_{i_d}(t)]+c_2rand_2[g_d-x_{i_d}(t)],$$

$$S(v_{i_d})=\frac{1}{(1+\exp(-v_{i_d}))},$$

$$x_{i_d}(t+1)=\begin{cases}1, & \text{if } rand3<s(v_{i_d})\\ 0, & \text{if } rand3\geq s(v_{i_d})\end{cases}.$$

3.2 共谋问题的离散粒子群优化算法及其实现步骤

在基于 EBS 的动态密钥管理方法中,每个节点有且仅有 k 个密钥,而且节点的密钥组合是互不相同的,所以针对共谋问题,还需对粒子的位置、速度及其更新方式作进一步限制.

设网络中有 N_c 个传感器节点,每个节点从 k+m 个密钥中选择 k 个,所以粒子 i 第 t 次迭代的位置 x_i^t 可以表示为一个 N_c×(k+m)的、元素取值为 0 或 1 的矩阵,$x_i^t(\alpha,\beta)=1$ 表示节点 n_α拥有密钥 k_β,$x_i^t(\alpha,\beta)=0$ 则表示 n_α不拥有密钥 k_β. $v_i^t(\alpha,\beta)$ 表示 $x_i^t(\alpha,\beta)$ 的速度,$S[v_i^t(\alpha,\beta)]$ 代表其 sigmoid 函数值.

采用与文献[28]类似的方法,根据粒子速度选择新的粒子位置时,在节点密钥组合互不相同的前提下,将 sigmoid 函数值最大的 k 个密钥分配给节点.对于粒子 i 第 t+1 次迭代的位置 x_i^{t+1},其 N_α节点的密钥分配方案 $\{\beta_1,\beta_2,...,\beta_k\}$ (即 $x_i^t(\alpha,\beta_i)=1,1\leq i\leq k$,其他为 0)是在所有可以选择的密钥分配方案集合$\Omega$中,使得 k 个 sigmoid 函数值之和最大的方案.即

$\{\beta_1,\beta_2,...,\beta_k\}\in\Omega$,而 $\forall\{\gamma_1,\gamma_2,...,\gamma_k\}\in\Omega$,$\sum_{j=1}^{k}S[v_i^t(\alpha,\beta_j)]\geq\sum_{c=1}^{k}S[v_i^t(\alpha,\gamma_c)]$,所以粒子位置及速度的更新方法为

$$v_i^{t+1}(\alpha,\beta)=wv_i^t(\alpha,\beta)+c_1rand_1[p_i(\alpha,\beta)-x_i^t(\alpha,\beta)]+c_2rand_2[g(\alpha,\beta)-x_i^t(\alpha,\beta)],$$

$$s[v_i^t(\alpha,\beta)]=1\Big/\{1+\exp[-v_i^t(\alpha,\beta)]\},$$

$$x_i^{t+1}(\alpha,\beta)=\begin{cases}1, & \text{if } \beta\in\{\beta_1,\beta_2,...,\beta_k\}\\ 0, & \text{else}\end{cases}.$$

根据第 3.3 节和第 4.2 节的分析,可以将采用 DPSO 优化共谋问题的过程表示为如下步骤:

步骤 1:随机给定一种密钥分配方案,利用它初始化粒子的位置.随机初始化粒子速度.初始化循环结束条件,包括循环次数上限,最小误差准则等.

步骤 2:根据第 3.3 节中的优化模型,计算各粒子的目标函数值 $f(x_i)$,进而求得局部最优解 p_i 和和全局最优解 g.

步骤 3:根据局部最优解和全局最优解更新粒子位置和速度.

步骤 4:检查结束循环条件,若没达到,返回步骤 2.

步骤 5:退出.

4 仿真实验

为了验证本文提出的优化模型及优化方法的准确性和有效性,我们针对多种网络配置情况进行了仿真实验.由于基于 EBS 的动态密钥管理方法通常应用在分簇结构的网络内,每个簇形成一个 EBS.而簇的范围通常在几百米,节点个数几十个.因此,为模拟网络中的一个簇,仿真网络拓扑结构采用边长 L=300m 的正方形区域,随机布置 N_c=10~100 个节点,节点的通信半径为 35m.由第 1.1 节可知必须保证 $\binom{k+m}{k} \geq n_c$,因此,EBS 结构选择每个节点拥有 k=2~7 个密钥,$k+m$=9,11,13.

同时,我们将本文方法仿真结果与密钥随机分配和 Shell[19]这两种分配方法进行了比较.这两种方法也同为基于 EBS 的动态密钥管理方法,与本文方法的区别在于,每个节点的 k 个管理密钥分别采用随机分配和基于启发式搜索两种方式.为了更好地反映统计规律,所有结果均为 100 次仿真实验结果的平均值.

随着被捕获的节点数目的增加,被捕获的密钥数目也会不断增加,网络的安全性会不断下降,直至被捕获的节点形成共谋链,全部密钥被捕获,网络安全性完全丧失.在这个过程中,通常以捕获节点数目与被捕获密钥比例(占密钥总数的比例)之间的关系来表示网络对捕获节点的抵抗性(resilience against node compromise),而以最短共谋链的长度来表示使网络安全体系失效的难易程度.它们都是无线传感器网络密钥体系安全性的重要参数.

4.1 最短共谋链的长度

图 3~图 5 分别为在相同的密钥池大小($k+m$=9)、不同节点数目 N_c 和节点密钥数量 k 的情况下,采用随机分配方案、Shell 和本文方法所得到的最短共谋链长度.若 k 增加,则捕获单个节点获得的密钥信息会变大,所以在 3 种分配方案中,最短共谋链的长度都会随着 k 的增加而减少.随着 N_c 增加,网络中节点密度变大,节点的邻居数增加,使得节点之间可以更容易地形成共谋,所以最短共谋链的长度也会缩短.

而在这 3 种不同的密钥分配方案中,本文的方法明显优于其他两种.在 N_c 和 k 较小的情况下,这种优势体现得尤为明显.例如在 k=3,N_c=20 的条件下,采用本文的优化模型和方法,Shell 和随机分配的方法得到的最短共谋链长度分别为 20,4,3.15,若捕获一个节点的概率为 0.1,则捕获全部密钥,使网络安全性完全丧失的概率 3 种情况下分别为 10^{-20},10^{-4},7.1×10^{-4}.采用本文的优化模型和方法相比于其他两种方法捕获全部密钥的难度提高了 10^{16},1.4×10^{15} 倍.

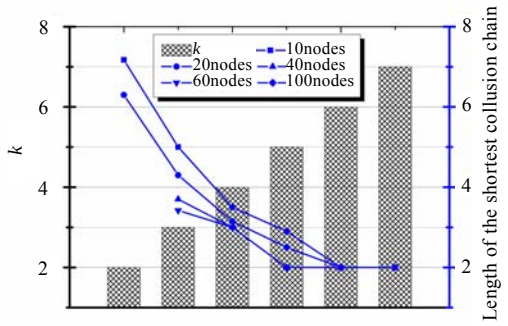

Fig.3 Relationship among the length of the shortest collusion chain, number of nodes and key number of a single node in random key distribution approach

图 3 随机密钥分配条件下,最短共谋链长度与节点数、节点密钥数的关系曲线

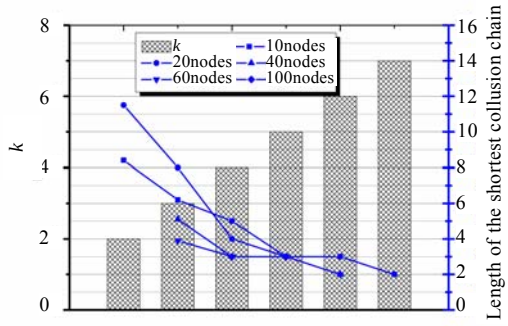

Fig.4 Relationship among the length of the shortest collusion chain, number of nodes and key number of a single node in Shell

图 4 Shell 条件下,最短共谋链长度与节点数、节点密钥数的关系曲线

4.2 网络对捕获节点的抵抗性

我们针对 N_c=40,k=3,$k+m$=9,11,13 这 3 种情况进行了网络对捕获节点抵抗性的仿真实验,其结果如图 6~图

8 所示.从图中我们可以明显地看到,在捕获同样数目的节点情况下,采用 DPSO 优化后,被捕获密钥比例明显优于随机分配的方法和 Shell 中的方法.很显然,这是因为在利用优化模型优化共谋链的长度过程中,也同时降低了节点通过共谋能够获得的密钥数目,所以提高了网络对节点捕获的抵抗性.而随着密钥池数目 $k+m$ 变大,3 种方案中网络对于捕获节点的抵抗性都得到了改善,因为密钥重叠的可能性降低了.

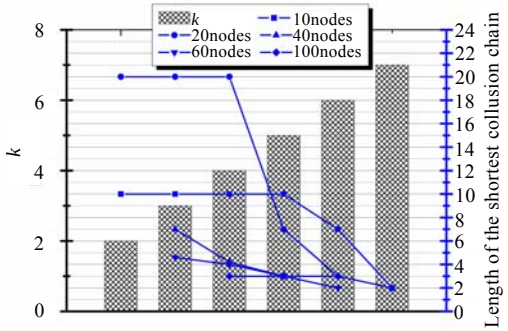

Fig.5 Relationship among the length of the shortest collusion chain, number of nodes and key number of a single node in our approach

图 5 采用本文的优化模型和方法条件下,最短共谋链长度与节点数、节点密钥数的关系曲线

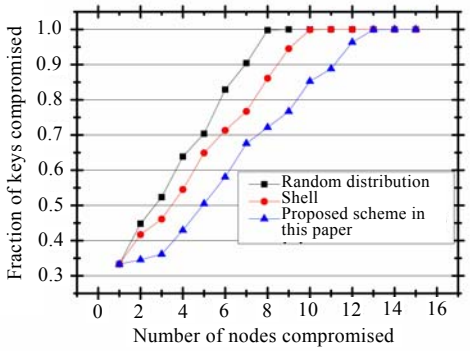

Fig.6 Relationship between the fraction of keys compromised and the number of nodes compromised ($k+m$=9)

图 6 捕获节点数目与被捕获密钥比例的关系曲线($k+m$=9)

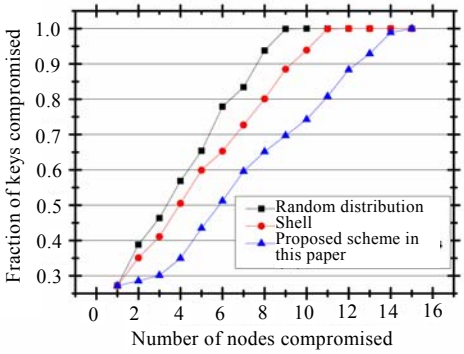

Fig.7 Relationship between the fraction of keys compromised and the number of nodes compromised ($k+m$=11)

图 7 捕获节点数目与被捕获密钥比例的关系曲线($k+m$=11)

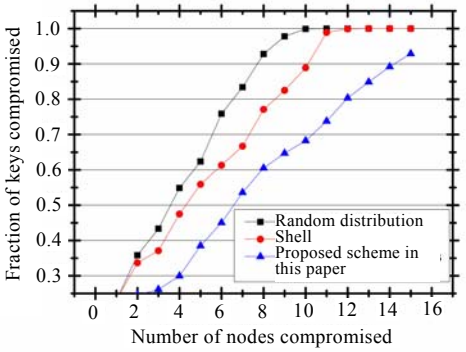

Fig.8 Relationship between the fraction of keys compromised and the number of nodes compromised ($k+m$=13)

图 8 捕获节点数目与被捕获密钥比例的关系曲线($k+m$=13)

5 结 论

本文研究了基于 EBS 的无线传感器网络动态密钥管理方法中的共谋问题.它是影响密钥系统安全性的主要因素.通过分析共谋问题的特性及其形成过程,将共谋链与 p 跳状态矩阵建立起了一一对应的关系,得到了最短共谋链长度的计算方法,并以它为目标建立了共谋问题的优化模型.利用离散粒子群算法对该优化问题进行了求解,仿真结果表明,与相关文献相比,采用本文提出的优化模型及优化方法,可以有效地提高网络的抗捕获性能和降低整个网络的难度,从而增强了网络的安全性.

References:

[1] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. Computer Networks, 2002,38(4): 393−422.

[2] Qi H, Iyengarb S, Chakrabartyk K. Distributed sensor networks-a review of recent research. Journal of the Franklin Institute, 2001,338(6):655−668.

[3] Aboelaze M, Aloul F. Current and future trends in sensor networks: A survey. In: Proc. of the 2005 Int'l Conf. on Wireless and Optical Communications Networks. Dubai: IEEE Press, 2005. 551−555.

[4] Sohrabi K, Gao J, Ailawadhi V, Pottie GJ. Protocols for self-organization of a wireless sensor network. Personal Communications, 2000,7(5):16−27.

[5] Ren Fengyuan, Huang Haining, Lin Chuang. Wireless Sensor networks. Journal of Software. 2003,14(7):1282−1291(in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1282.htm

[6] Boudriga N, Obaidat M. Mobility, sensing, and security management in wireless ad hoc sensor systems. Computers and Electrical Engineering, 2006,32(3):266−276.

[7] Shi E, Perrig A. Designing secure sensor networks. IEEE Wireless Communications, 2004,11(6):38−43.

[8] Slijepcevic S, Potkonjak M, Tsiatsis V, Zimbeck V, Srivastava MB. On communication security in wireless ad-hoc sensor networks. In: Proc. of the 11th IEEE Int'l Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2002). Pittsburgh: IEEE Press, 2002. 139−144.

[9] Du WL, Deng J, Yunghsiang SH, Pramod KV. A key predistribution scheme for sensor networks using deployment knowledge. IEEE Trans. on Dependable and Secure Computing, 2006,3(1):62−77.

[10] Zhu S, Setia S, Jajodia S. LEAP: Efficient security mechanisms for large-scale distributed sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security (CCS 2003). Washington: ACM Press, 2003. 62−72.

[11] Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. In: Proc. of the 9th ACM Conf. on Computer and Communications Security. Washington: ACM Press, 2002. 41−47.

[12] Ren K, Zeng K, Lou WJ. A new approach for random key pre-distribution in large-scale wireless sensor networks. Wireless Communication and Mobile Computing, 2006,6(3):307−318.

[13] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proc. of the 2003 IEEE Symp. on Security and Privacy (SP 2003). Berkeley: IEEE Press, 2003. 197−213.

[14] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2003. 52−61.

[15] Du W, Deng J, Han YS, Varshney PK. A pairwise key pre-distribution scheme for wireless sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. Washington: ACM Press, 2003. 42−51.

[16] Eltoweissy M, Heydari H, Morales L, Sadborough H. Combinatorial optimization of key management in group communications. Journal of Network and Systems Management, 2004,12(1):33−50.

[17] Eltoweissy M, Moharrum M, Mukkamala R. Dynamic key management in sensor networks. IEEE Communications Magazine, 2006,44(4):122−130.

[18] Eltoweissy M, Wadaa A, Olariu S, Wilson L. Group key management scheme for large-scale sensor networks. Ad Hoc Networks, 2005,3(5):668−688.

[19] Younis MF, Ghumman K, Eltoweissy M. Location-Aware combinatorial key management scheme for clustered sensor networks. IEEE Trans. on Parallel and Distributed Systems. 2006,17(8):865−882.

[20] Riaz R, Ali A, Kim KH, Ahmad F, Suguri H. Secure dynamic key management for sensor networks. In: Innovations in Information Technology. Dubai: IEEE Press, 2006. 1−5.

[21] Moharrum M, Eltoweissy M, Mukkamala R. Dynamic combinatorial key management scheme for sensor networks. Wireless Communication and Mobile Computing, 2006,6(7):1017−1035

[22] Kim JM, Cho JS, Jung SM, Chung TM. An energy-efficient dynamic key management in wireless sensor networks. In: Proc. of the 9th Int'l Conf. on Advanced Communication Technology. Gangwon-Do: IEEE Press, 2007. 2148−2153.

[23] Li LC, Li JJ, Tie L, Pan J. ACKDs: An authenticated combinatorial key distribution scheme for wireless sensor networks. In: Proc. of the 8th ACIS Int'l Conf. on Software Engineering, Artificial Intelligence, Networking, and Parallel Distributed Computing (SNPD). Qingdao: IEEE Press, 2007. 262−267.

[24] Kennedy J, Eberhart RC. Particle swarm optimization. In: Proc. of the IEEE Conf. on Neural Networks. Perth: IEEE Press, 1995. 1942−1948.

[25] Hu W, Li ZS. A simpler and more effective particle swarm optimization algorithm. Journal of Software, 2007,18(4):861−868 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/861.htm

[26] Zhou C, Gao HB, Gao L, Zhang WG. Particle swarm optimization (PSO) algorithm. Application Research of Computers, 2003,12:7−11 (in Chinese with English abstract).

[27] Kennedy J, Eberhart R. A discrete binary version of the particle swarm algorithm. In: Proc. of the 1997 IEEE Int'l Conf. on Systems, Man, and Cybernetics. Orlando: IEEE Press, 1997. 4104−4108.

[28] Li XY, Tian P, Hua J, Zhong N. A hybrid discrete particle swarm optimization for the traveling salesman problem. Lecture Notes in Computer Science 4247, 2006. 181−188.

附中文参考文献:

[5] 任丰原,黄海宁,林闯.无线传感器网络.软件学报,2003,14(7):1282−1291. http://www.jos.org.cn/1000-9825/14/1282.htm

[25] 胡旺,李志蜀.一种更简化而高效的粒子群优化算法.软件学报,2007,18(4):861−868. http://www.jos.org.cn/1000-9825/18/861.hml

[26] 周驰,高海兵,高亮,章万国.粒子群优化算法.计算机应用研究,2003,12:7−11.

孔繁瑞(1981－),男,辽宁沈阳人,博士生,主要研究领域为无线传感器网络的安全性.

焦飞(1982－),男,硕士,主要研究领域为无线传感器网络,能源安全与控制.

李春文(1958－),男,博士,教授,博士生导师,主要研究领域为复杂网络,非线性控制理论,电力系统优化.

谷琦彬(1985－),男,硕士,主要研究领域为无线传感器网络,能源安全与控制.

丁青青(1964－),女,副教授,主要研究领域为网络安全技术,新能源与能源安全.