无线传感网络密钥管理及认证综述

张国印 孙瑞华 马春光 朱华旻
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

摘 要 无线传感器网络因其灵活性和适用性而广泛应用于民用、军用、商用等领域,然而由于传感器结点自身的特点使得无线传感器网络与传统网络有着很大的不同。对有安全性要求的无线传感器网络而言,若在敌对环境中使传感器网络结点间能安全地进行通信,密钥管理和认证就显得十分重要。目前针对密钥管理和认证提出了许多方案,对这些方案做出了总结并给出了比较,同时对进一步的研究方向进行了分析。

关键词 无线传感器网络,密钥管理,认证,综述

Survey of Sensor Networks Key Management and Authentication

ZHANG Guo-yin SUN Rui-hua MA Chun-guang ZHU Hua-min
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

Abstract Because of the flexibility and extensive applicability of the wireless sensor networks, they can be applied into many fields such as civil, commercial and military. Based on nodes' characters, the sensor networks are quite different from the traditional networks. The key management and authentication are important to guarantee nodes' secure communication. Now there're many schemes for key management and authentication, in this paper the current schemes were classified and compared, also the future studying directions were pointed out.

Keywords WSN, Key management, Authentication, Survey

1 引言

无线传感网络由大量传感器结点组成,每个传感器结点一般由传感单元、处理单元、收发单元、电源单元等功能模块组成,可对外部环境进行感知,结点间可实现通信。

无线传感网络具有成本低、数量多、分布密集[1,2]的特点,被广泛应用于感知外界温度、压力、相对湿度等方面,有时也被部署于敌方战场以检测敌情。由于无线传感网络采用无线信道、有限电源、分布式控制等技术,结点容易被攻击者物理操纵,从而容易获取存储在传感结点中的所有信息。

现有的攻击方法主要有1)物理层有拥塞攻击、物理破坏;2)MAC层有DoS(Denial of Service)攻击[3]、碰撞攻击;3)网络层有虚假路由信息攻击、选择性转发/不转发攻击、sinkhole攻击[4]、Sybil攻击[5,6]、Wormholes攻击[7]、HELLO flood攻击[8]。因此信道加密、抗干扰、用户认证和其他安全措施都需要特别考虑,特别是当传感器结点布置于敌方阵地时。

针对现有攻击,目前提出了许许多多的无线传感网络密钥管理及认证的方法。本文对现有方案进行分类综述,并进行比较分析。

2 密钥管理方案

根据使用的密钥是否对称、结点的同异构、密钥在网络中是否可以动态改变及密钥连通率,可以将现有的方案分为对称密钥管理和非对称密钥管理、同构与异构密钥管理、静态与动态密钥管理、随机和确定密钥管理[9]。

当前方案以随机密钥管理居多,故在此将现有的方案按照随机密钥管理和确定密钥管理的方式进行分类。

2.1 随机密钥管理

随机密钥管理采用结点预先分配密钥,然后结点随机部署的方式。该方式主要研究的问题为如何使得结点存储较少的密钥能获得较高的连通率,及如何增强结点的抗毁性。

2.1.1 E-G随机密钥管理预分配方案

Eschenauer和Gligor最早利用Erdos随机图论的结果 $P_c=\lim_{n\to\infty}\Pr[G(n,p)\ is\ conneted]=\frac{1}{e^{e^{-c}}}$ 提出了一种随机密钥管理方案[10],其中 $p=\frac{\ln(n)-c}{n}$ 表示任意两结点间共享密钥的概率,c 为一实数,n 为随机图顶点的数量。由此可计算结点的期望连通度 $d=\frac{\ln(n)-c}{n}(n-1)$。再根据结点的通信范围来确定邻居数量,由此计算局部连通概率,结合组合数学知识,让每个结点从一个密钥池中随机选取密钥,由密钥池的大小可确定结点需存取的密钥数。

2.1.2 q-composite方案

Chan等人根据Eschenauer和Gligor的结果将其推广至

到稿日期:2009-03-31 返修日期:2009-07-16 本文受国家博士后科研基金(20070410896),黑龙江省博士后科研基金(LBH-206027)资助。
张国印 男,博士,教授,博士生导师,CCF高级会员,主要研究方向为网络与信息安全、嵌入式系统,E-mail:zhangguoyin@hrbeu.edu.cn;孙瑞华 男,硕士,主要研究方向为传感器网络、密码学;马春光 男,博士,教授,硕士生导师,主要研究方向为传感器网络、密码学;朱华旻 男,硕士,主要研究方向为传感器网络、计算机网络及应用。

q-composite 的情形[11]($q=1,2,3$)，即任意两结点之间想实现通信必须至少共享 q 个密钥。他们研究了被攻陷结点数量已知时其余结点被攻陷的概率，结果表明与 Eschenauer 和 Gligor 的方案相比，结点连接概率相同且 $q=1,2,3$ 被攻陷的结点数量较少时，未被攻陷的结点数量被攻陷的概率较小。一旦被攻陷的结点超过一定数量，未被攻陷的结点数量被攻陷的概率迅速增加。此外，文献[11]中还给出了多路径增强方案，由源结点随机产生若干密钥，通过不同的安全路径分别将密钥发送至目的结点中。源和目的结点同时将原密钥及新密钥进行异或操作得到新密钥，来实现通信，从而提高结点间的安全性。

2.1.3 基于正态分布的方案

在 Eschenauer 和 Gligor 的基础上，Du 等人提出了基于部署知识的密钥管理方案[12]。将预部署的目标区域划分为几个小的区域，对密钥池进行同样的操作，不过被划分的小密钥池间有重叠的密钥。每个区域有一个部署点，结点在部署点周围服从正态分布。在结点连接概率相同时，每个结点存储的密钥较少，进而已知被攻陷结点数量时，其余结点被攻陷的概率较小。

2.1.4 基于对称多项式的方案

基于 Eschenauer 和 Gligor 的方案，Liu 和 Ning 提出了一个基于对称多项式的加密方案[13]，该方案由 Carlo Blundo 等在 1995 年提出。任意结点都可以根据本结点的 ID 和其他结点的 ID 计算其存储的多项式的值。只要值相同，即可与其他结点实现通信。根据 Carlo Blundo 等的结果，在结点连接概率相同且已知被攻陷结点数量相同时，其余结点被攻陷的概率较小。

2.1.5 CPKS(Closest Pairwise Keys Scheme)方案

在文献[13]的基础上，Liu 和 Ning 又提出了 CPKS 方案[14,15]：利用 Chan 的随机配对密钥的原则(一个密钥仅随机唯一分配给一对结点)，每个结点在部署前在目标区域中有一个预期部署位置，结点实际散落位置在预期部署位置附近服从均匀分布(均匀分布的半径称为误差 ε)。根据该思路，文中计算出了结点的连接概率与部署误差的关系。该方案最突出的优点在于已知被攻陷结点数量时，其余结点被攻陷的概率为 0，缺点在于可扩展性不强，在添加新结点时需要复杂的操作。

2.1.6 CPPDS(Closest Polynomials Pre-Distribution Scheme)方案

CPPDS 方案[14,15]将目标区域划分为几个小区域，临近的小区域间共享一定数量的密钥。每个结点以小于某一误差的方式部署于期望位置附近，且根据期望位置所在的区域选择自己的密钥。研究了结点间共享密钥的概率及结点的抗毁性，所采用方法类似 CPKS。

2.1.7 基于部署后知识的方案

基于部署后知识的方案[14]假设结点存储空间足够大，将密钥池中每个密钥均匀映射至目标区域中的一个位置。每个结点部署前将其期望位置结点半径 r 内的密钥存储于结点存储器中，在实际部署后，结点根据自己的位置信息将所存密钥进行排序，删除一定数量权值较小的密钥。当结点间有共享密钥且在通信范围内时，结点之间可以通信。研究得出此时结点的连接概率随存储容量增加而增加，以及已知被攻陷结点数量时其余结点在密钥优先权计算前和计算之后被攻陷的概率。

2.1.8 HGKM 方案

在 Blundo 等人提出的对称多项式基础上，Canh 等人提出了一种利用部署知识的方案——HGKM[15]。将待部署目标区域划分为如图 1 所示的情形，对所有六边形做如下分类：标记(i,j)的六边形与标记为$(i+1,j)$，$(i+1,j+1)$归为 1-簇，标记为(i,j)的六边形与$(i,j-1)$，$(i-1,j)$归为 2-簇，标记为(i,j)的六边形与$(i,j+1)$，$(i-1,j+1)$归为 3-簇。为每个六边形分配结点。在簇划分完后，由多项式生产算法为每簇分配一多项式，由属于该簇的所有结点所共享。然后对每个六边形的结点进行部署，部署结点服从正态分布。结点部署后通过交换结点 ID 并计算多项式值的方式来发现共同密钥。该方案对不同部署距离时的本地连通率和全局连通率进行了计算，同时对结点抗毁性进行了分析。

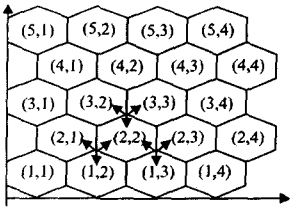

图 1 目标区域划分示意图

2.1.9 基于部署知识的方案

在文献[15,18]的基础上，Yu 等人的方案根据 Blom 的密钥管理方案[16]为结点建立配对密钥：将待部署目标区域划分为正方形或正六边形单元，为每个正方形或六边形分配结点，属于同一个正方形或六边形的结点称为一个组。事先产生一个全局公开矩阵 G 和一些秘密矩阵 A 和 B，每组结点共享矩阵 G，为每组结点分配一个唯一矩阵 A，根据自己的 ID 从 G 中选取相应的列，从 A 中选取相应的行，如此可保证组内结点一直共享配对密钥。为保证组间结点的连通性，文中定义(b,w)，其中 b 表示每组分配的最大 B 矩阵数，w 表示每结点挑选的最大矩阵行数。下面以 $b=2$ 为例，说明如何选择 B 矩阵数。

按照如下规则选择若干基本组，并分配不同的矩阵 B，其余组根据基本组确定自己的矩阵。

由上往下建立 y 轴，由左往右建立 x 轴，为每个六边形或正方形分配一二维坐标(r_i,c_i)。满足下列条件之一的单元被选为基本组，其余单元根据基本组分配的 B 矩阵选择自己的矩阵，如图 2 所示。

1)若 $r_i \bmod 2=0$ 且 $c_i \bmod 2=0$ 但 $r_i \bmod 4\neq 0$；

2)$r_i \bmod 4=0$ 且 $c_i \bmod 2=1$。

文中同时对某个单元结点被俘获后可能影响的单元进行了描述。在对结点连通性分析中，根据 Penrose 提出的随机最小生成树最长边原理研究了给定结点连通率时计算所需结点的感知半径；在局部安全性分析中给出了一个结点被俘获和 λ 个结点被俘获的理论分析。此外，文中对结点局部安全性和全局安全性进行了模拟，结果表明在选择合适的结点部

署分布和单元划分时结点具有更强的抗毁性，同时文中模拟了单元格大小对连通性和抗毁性的影响。

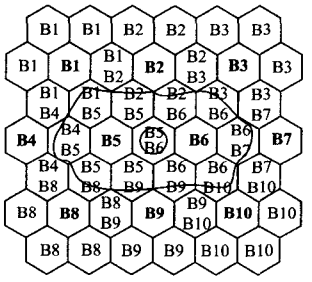

图 2　$b=2$ 时 B 矩阵分配及 $B5B6$ 中结点被俘获后可影响的单元示意图

这些部分主要的方案关系总结如图 3 所示。

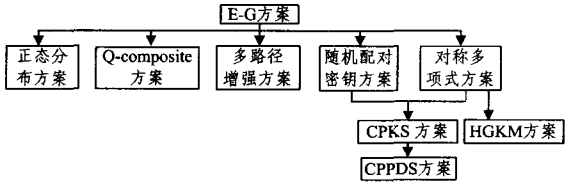

图 3　现有部分随机密钥管理方案关系

2.2　确定密钥管理

该方式使得结点的连通率为 1，主要研究问题为增强结点的抗毁性及减少结点存储密钥数量。

2.2.1　密钥空间分配方案

Blom 单密钥空间方案[18]利用对称矩阵的特性动态计算节点间的会话密钥，使得节点可与邻居中的任何一个节点共享会话密钥，即 $k_{ij}=A(i)\times G(j)=k_{ji}=A(j)\times G(i)$，采用 k_{ij} 和 k_{ji} 作为节点 i 和 j 之间的会话密钥。在受损节点数不超过阈值时，网络不会泄露任何机密信息。若有多于 λ 个的节点被俘获，则整个网络被俘获（λ 为网络可调节系数）。

为提高抗毁性，Du 等人将其扩展为多密钥空间随机密钥预分配方案[19]。文中定义 (D,G)，$D=\{D_1,\cdots,D_w\}$，令 $A_i=(D_i,G)$，每个节点从 A_i 中选取 τ 个密钥作为本节点的密钥子集。每个节点发现邻居节点是否与本地有共同的密钥空间。若有，则广播信息，该信息包含了密钥空间索引和 G_i。

2.2.2　基于组合论的密钥预分配方案

Camtepe 把组合设计理论（combinatorial design theory）用于设计 WSN 确定密钥预分配方案[20]。利用对称 BIBD（Balanced Incomplete Block Design，均衡不完全区组设计）和有限广义四边形，将对称 BIBD（参数为 $(n^2+n+1,n+1,1)$）映射至密钥分配中。在部署结点前，根据网络的规模 N 确定一素数 n 满足 $n^2+n+1\geqslant N$；由此产生 $n-1$ 个 n 阶正交拉丁方；再由正交拉丁方构建 n 阶仿射平面，由仿射平面构建投影平面并在此基础上进行密钥分配。这样使得任意两个结点的密钥连通概率为 1。

2.2.3　LEAP（localized encryption and authentication protocol）协议

根据不同类型消息交换具有不同的安全需求原则，Zhu 在 LEAP 协议[21]中建立了 4 种类型的密钥：个体密钥、配对密钥、组密钥和簇密钥。每个结点与基站共享唯一的个体密钥，若结点发现意外事件发生，则利用该密钥向基站发送警告信息，基站亦向该结点发送利用个体密钥加密的信息到该结点。组密钥用来实现基站与结点间的广播。簇密钥是结点与其邻居结点间共享的密钥，用以实现局部广播。配对密钥是结点与其直接邻居结点间共享的密钥，用以实现隐私或来源认证，不包括被动加入。

2.2.4　基于 EBS（exclusion basis systems）的动态密钥管理方案

EBS 方案[22,23,30]由 Morales 等提出，主要用于密钥动态管理。EBS 由三元组 (n,k,m) 组成，n 是用户数量，k 是结点所存储密钥数量，m 是密钥更新信息数。

一个 EBS 例子如表 1 所列。

表 1　一个 EBS 例子

	#1	#2	#3	#4	#5	#6	#7	#8
α	0	0	0	0	1	1	1	1
β	0	1	1	1	0	0	0	1
γ	1	0	1	1	0	1	1	0
δ	1	1	0	1	1	0	1	0
ε	1	1	1	0	1	1	0	1

$\alpha,\beta,\gamma,\delta,\varepsilon$ 表示密钥，#1－#8 表示用户。此例中 $k=3$，$m=2$。表中元素若为 0，表示用户不拥有相应的密钥，元素为 1 表示拥有相应的密钥。Morales 等证明了当且仅当 $\binom{k+m}{k}\geqslant n$ 存在一个 EBS。在新添加一个结点时，若 $n<\binom{k+m}{k}$，直接根据从 $\binom{k+m}{k}$ 个组合选取未使用的组合来给结点添加相应的密钥；若 $n=\binom{k+m}{k}$，则需增加新的元组，可通过增加 k（在原表基础上新加一行全为 1）或增加 m（在原表基础上新加一行全为 0）的方式来满足网络的要求，若增加 m，仅需对新结点做相应的密钥分配处理。若增加 k，还需对网络中已有结点进行密钥更新。当用户离开网络时，如 #1 离开网络，可通过广播消息 $\alpha(\gamma(\gamma'),\delta(\delta'),\varepsilon(\varepsilon')),\beta(\gamma(\gamma'),\delta(\delta'),\varepsilon(\varepsilon'))$ 的方式更新剩余结点的密钥。$\gamma(\gamma')$ 表示先使用 γ 对新密钥 γ' 进行加密，最后使用密钥 α 对这些信息加密。相应结点在收到信息后做相应处理，以更新密钥。

Younis 在此基础上提出基于位置的 EBS 动态密钥管理方案 SHELL[26]。普通结点按照地理位置进行分簇，由簇头结点生成 EBS 矩阵。该方案可用于结点密钥的更新、结点添加、删除。

2.2.5　基于 IBC（identity-based cryptography）的密钥预分配方案

Zhang 提出了将 Bilinear Pairing 技术与地理信息相结合的 IBC 密钥管理方案[25]。与 CBC 相比，基于身份密码体制（IBC）的主要优点是结点的公钥由公开信息直接推导获得，无需对公钥进行认证，从而有效地降低了计算复杂度和通信负载，被认为比较适用于 WSN。

3　认证方案

无线传感网络认证方案可以从不同的角度划分为如下 3 种类型。

1）对称密钥和非对称密钥认证体制

根据现有认证方法使用的密钥对称性进行划分。对称密钥体制使用相同的加密密钥和解密密钥进行认证。该体制中要求不同的结点对间共享不同的密钥。非对称密钥体制结点

使用不同的密钥进行认证，一般使用私钥进行加密，公钥进行解密。

2)消息认证和身份认证体制

根据认证过程中使用的是对消息进行认证还是对身份进行认证加以划分。消息认证是对对方发来的消息进行合法性认证，身份认证指当外部结点加入网络时对外部组织身份进行的认证。

3)广播和单播认证体制

根据所使用的认证过程是一对一(即点对点)还是一对多(即一点对多点)的方式划分为单播和广播。单播相对比较简单，只要求两结点参与；多播需要将信息发送至多个结点并由多个结点完成认证过程。

本文按照消息认证和身份认证对现有方案进行分类。

3.1 消息认证

现有方案中主要采用对称密钥认证的方式实现消息认证。

3.1.1 SPINS(security protocols for sensor networks)协议

SPINS协议[26]包括SNEP(Secure Network Encryption Protocol)和μTESLA(micro Timed Efficient Streaming Loss-tolerant Authenticating Protocol)两部分。

1)SNEP用以实现通信的机密性、完整性、新鲜性及点到点的认证；SNEP机密性不仅具有加密功能，还具备语义安全性。SNEP采用计数器CTR方式实现语义安全性，加密方式如下：

$$E=\{D\}(K_{enc},C)$$

其中，E表示加密后密文；D表示加密前明文；K_{enc}表示加密密钥；C为计数器。

SNEP完整性和点到点认证通过消息认证码(message authentication code，MAC)协议实现。

$$M=MAC(K_{mac},C|E)$$

K_{mac}表示消息认证算法密钥，$C|E$为计数器值C和密文E的粘接，表明消息认证码是对计数器和密文一起进行的运算。

K_{enc}和K_{mac}两个密钥都是通过与基站共享的主密钥K_{master}按照相同算法推演出来的。

SNEP协议通过CTR模式支持数据通信的弱新鲜性。设A向B连续发送3个请求数据包：

$$A\rightarrow B:$$

$$\{R_{Ai}\}(K_{enc},C_i),MAC(K_{mac},C_i|\{R_{Ai}\}(K_{enc},C_i))(i=1,2,3)$$

通过计数器值，B能够判断这3个请求数据包是由A顺序发送过来的。得到这3个请求数据包后，B会将请求交由上层应用处理，并将相应消息回复给A。A从B收到3个RSP消息：

$$A\leftarrow B:$$

$$\{RSP_{Ai}\}(K_{enc},C_i'),MAC(K_{mac},C_i'|\{R_{Ai}\}(K_{enc},C_i'))(i=1,2,3)$$

A同样根据计数器值判断这3个响应是从B顺序发送过来的。此方案能有效抑制任何响应数据包的重放攻击，即实现了弱新鲜性认证。此新鲜认证存在的一个问题是A不能判断收到的响应数据包RSP_{A1}是否针对它发出R_1请求数据包的响应。如果A收到的回复消息不是按照请求包的发送顺序给出的，那么将不能为每个请求回送正确的响应。为此SNEP定义了强新鲜性认证方法。

SNEP协议通过Nonce机制实现强新鲜性。Nonce唯一标识当前状态且任何无关者都不能预测，通常由真随机数发生器产生。SNEP协议在每个安全通信的请求数据包中增加Nonce段，唯一标识请求包的身份。为保证安全性，Nonce字段要足够长。通信过程如下：

$$A\rightarrow B:N_A,\{R_{Ai}\}(K_{enc},C),MAC(K_{mac},C|\{R_{Ai}\}(K_{enc},C))$$

$$B\rightarrow A:\{RSP_{Ai}\}(K_{enc},C'),MAC(K_{mac},N_A|C'|\{RSP_{Ai}\}(K_{enc},C'))$$

A可通过响应包的认证码得知此回应包是针对N_A标识的请求消息给出的，而不必考虑回应的顺序问题。

2)μTESLA用以实现多点的广播认证，其思想是先广播通过K_{mac}认证的数据包，然后公布密钥K_{mac}。此举可能在广播包正确确认前伪造正确的广播数据包，其认证过程如图4所示。

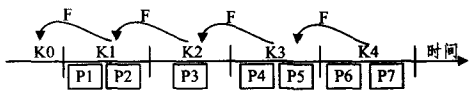

图4 μTESLA认证过程图

Liu提出使用多级μTESLA[27]来解决μTESLA中密钥延迟暴露及非实时认证问题而引发的DoS攻击。协议中引进了预定和广播初始化参数的方法，代替了在μTESLA协议中使用单播方式初始化安全参数的过程；其次采用多级密钥链模型，摒弃了μTESLA使用超长密钥链维持μTESLA生命周期的方法；另外使用冗余传输机制和随机选择策略完成密钥链的发布任务，以提高网络对包丢失的容忍度和抗击DoS攻击的能力。

3.2 身份认证

现有方案中以非对称密钥认证和秘密共享认证为主。非对称认证的实质是将耗能较大的计算交由认证发起方处理，耗能较小的计算交由认证验证方处理。秘密共享认证则由多结点对1个结点共同处理，以进行认证。

3.2.1 随机配对密钥认证

文献[11]利用随机配对密钥方案(一个密钥仅随机唯一分配给一对结点)来实现结点间的认证，将一结点对另一结点发送的消息进行解密从而知道对方的身份。

3.2.2 基于RSA公钥算法的TinyPK认证

TinyPK认证过程[28]如图5所示。

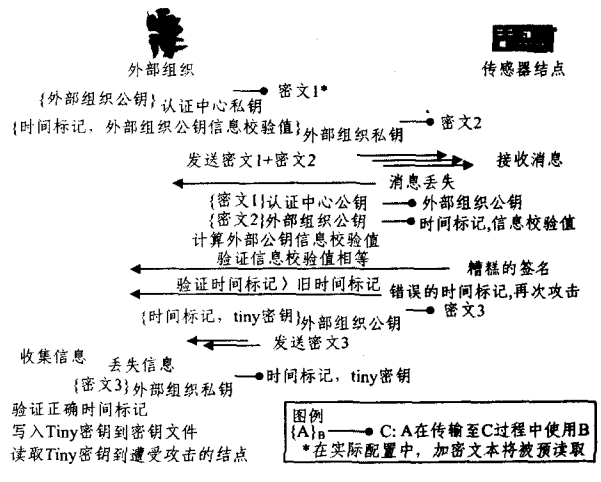

图5 TinyPK认证算法

TinyPK 认证协议采用请求-应答机制。该协议首先由外部组织给某个结点发送请求信息。请求信息中包含两部分：第一部分是自己的公钥，采用认证中心私钥签名；第二部分由时间标记和信息校验值组成，用外部组织自己的私钥签名(时间标记用来抗重播，信息校验用来保证信息完整性)。传感器结点在收到此信息后，用预置的认证中心公钥来验证信息包中的第一部分以验证外部组织身份，获取外部组织的公钥。接着用此公钥去验证信息的第二部分，来获取时间标记和信息校验值。最后传感器结点验证该时间标记和信息校验值。若都通过验证，则外部组织可获得合法身份。之后传感器结点采用外部组织公钥加密后将会话密钥传给外部组织，以此来建立两者之间的安全数据通信。

3.2.3 基于 ECC(Elliptic Curve Croptography)n 认证

ECC n 认证[29]假设外部组织通信范围内有 n 个结点，其中允许有 t 个结点被捕获运行与其他结点不同的程序，只有外部组织通过 $m(m\leqslant n-t)$ 个结点的认证后才可通过认证加入网络。

该认证过程用算法表述如下：

(1)EP 给在其通信范围内的 n 个传感器结点广播 1 个数据包$(U,cert_u)$，U 表示外部组织自己产生的身份值，$cert_u$ 表示合法外部用户从认证中心获取的证书，该证书仅由被认证中心私钥签名的外部组织的公钥组成，此举是为了让传感器结点在验证签名的同时获得外部组织的公钥。

(2)传感器结点 s_i 在收到此数据包后保存该数据包，然后返回给外部组织数据包$(s_i,nonce_i)$，s_i 表示结点本身的身份值，$nonce_i$ 表示一次性随机数。其他结点亦进行相同操作。

(3)外部组织在收到结点 s_i 返回的数据包后，先用散列函数计算出散列值 $h(U,s_i,nonce_i)$，再用自己的私钥签名后发送给结点 $s_i(1\leqslant i\leqslant m)$，即向结点 s_i 发送 $sign_U(h(U,s_i,nonce_i))$。

(4)每个传感器结点 s_i 先验证 $cert_u$ 来获取外部组织的公钥，然后用外部组织的公钥去验证采用外部组织私钥签名的散列值 $h(U,s_i,nonce_i)$，同时获得该散列值。然后传感器结点用散列函数计算 $U,s_i,nonce_i$ 的散列值并与之前获得的散列值进行对比。若相同，则外部组织通过了该结点的认证。

(5)每个让外部组织认证通过的结点 s_i 都依据对称共享密钥对计算出一个消息认证码(即 MAC)，并返回给外部组织，外部组织在至少获得 m 个 MAC 值后才能获得网络的合法身份。

3.2.4 基于秘密共享的认证

文献[31]提出了一个基于秘密共享的认证方案。任意结点均可发起对目标结点 T 的认证，目标结点 T 通知 PC(处理中心)自己被选中做认证处理，然后由 PC 将 T 的秘密划分为 $|N|-1$ 份，连带各结点 ID 号一起广播给其余 $|N|-1$ 个结点(此 $|N|-1$ 个结点构成集合 $N\backslash\{T\}$)，各结点在接收到消息后做如下算法：

/ * 对于$\in N\backslash\{T\}$的每个结点挑选质疑者，此处以结点 u 为例 * /
采用投硬币的方式以概率 p 选择 u 的后继者 v
若 $v\neq T$
　选择 v 作为质疑者
广播 v 是质疑者的消息
发送 u 接收到的 T 的消息和 u ID 给结点 v
执行 $challengers:=challengers\cup\{v\}$
　否则
　做空操作
/ * 一旦结点收到 v 是质疑者或其他结点第一次广播的 share(即 PC 广播给该结点的 T 的密码)消息时执行该操作 * /
若 $u=v$ 则 / * 说明 u 知道自己被选为质疑者 * /
对所有 $t_i\in N\backslash\{T\}$
接收消息$\langle share_i,t_i\rangle$
$retrievedShares[i]=share_i$
由 retrievedShares 构建 T 的原秘密 secret
发送请求秘密消息给 T
从 T 接收消息 $Tsecret$
若 $Tsecret$=secret / * 说明 T 通过认证 * /
广播"true"消息
否则 / * T 未通过认证 * /
广播"false"消息
否则 / * $u\neq v$ * /
发送$\langle share,u\rangle$给结点 v
$challengers:=challengers\cup\{v\}$

在所有质疑结点对 T 进行投票后，$N\backslash\{T\}$中所有结点对质疑结点投票进行计数。若"true"个数超过$\frac{1}{2}(|N|-1)$，则 T 通过网络认证，否则未通过网络认证。在 T 认证后，需通过安全渠道与 PC 交互，更新自己的秘密。

4 现有部分密钥管理方案比较

现给出部分密钥预分布方案的结点连通概率及抗毁性比较如表 2 所列。

表 2 现有部分密钥管理方案之比较

方案	结点连通率	抗毁性
E-G 方案	$1-\frac{((P-k)!)^2}{(P-2k)!\ P!}$	$1-(1-\frac{k}{P})^x$
Q-composite 方案	$1-\sum_{i=0}^{q-1}\frac{\binom{\lvert S\rvert}{i}\binom{\lvert S\rvert-i}{2(m-i)}\binom{2(m-i)}{m-i}}{\binom{\lvert S\rvert}{m}^2}$	$\sum_{i=q}^{m}(1-(1-\frac{m}{\lvert S\rvert})^x)^i\frac{p(i)}{p}$
基于正态分布的方案	$\frac{\int_{x=0}^{X}\int_{y=0}^{Y}\sum_{j\in\psi}\sum_{i\in\psi}f_R(d_{jz}\mid n_j\in group\ j)\cdot g(d_{iz}\mid n_i\in group\ i)\cdot p(\lambda(i,j))\mathrm{d}x\mathrm{d}y}{\int_{x=0}^{X}\int_{y=0}^{Y}\sum_{j\in\psi}\sum_{i\in\psi}f_R(d_{jz}\mid n_j\in group\ j)\cdot g(d_{iz}\mid n_i\in group\ i)\mathrm{d}x\mathrm{d}y}$	$1-(1-\frac{m}{\lvert S\rvert})^x$
基于对称多项式的方案	$1-\prod_{i=0}^{s'}\frac{s-s'-i}{s-i}$	$1-\sum_{i=0}^{t}\binom{N_c}{i}(\frac{s'}{s})^i(1-\frac{s'}{s})^{N_c-i}$

CPKS 方案	$\gamma p(\|\|\dot{u},\dot{v}\|\|\leqslant d_r\|\tilde{u})$	0
CPPDS 方案	$\dfrac{\sum_{C_{j_c,j_r}\in S_{i_c,i_r}} p(\|\|\dot{u},\dot{v}\|\|\leqslant d_r\|C_{i_c,i_r},C_{j_c,j_r})}{\sum_{\forall C_{j_c,j_r}} p(\|\|\dot{u},\dot{v}\|\|\leqslant d_r\|C_{i_c,i_r},C_{j_c,j_r})}$	$1-\sum_{i=0}^{t}\binom{m}{k}p_c^k(1-p_c)^{m-k}$
基于部署后知识方案	$\int_0^{d_r}\int_0^{2\pi}\dfrac{p(\rho)\rho}{\pi d_r^2}\mathrm{d}\rho\mathrm{d}\theta$	$1-\sum_{i=0}^{t}p_c(i)$(据实际情形,$p_c(i)$分两种情形)
多密钥空间预分配方案	$1-\dfrac{((\omega-\tau)!)^2}{(\omega-2\tau)!\ \omega!}$	$P(S_1$ is compromised$\|\ C_x)$
基于格子方案	1	$1-\sum_{i=0}^{t}\binom{m}{k}p_c^k(1-p_c)^{m-k}$

根据上表内容及原文分析,在部署连通率要求不高的情形下,可使用 E-G 方案;在预知结点被俘获的数量较少时,可使用 Q-composite 方案;当具有有利条件可对结点进行分组部署及对连通率要求较高时,可使用基于正态分布的方案;当对结点的抗毁性要求较高时,可使用基于对称多项式的方案和多密钥空间预分配方案;在结点部署前若可对结点进行大致定位,可使用 CPKS 方案及 CPPDS 方案;在结点具有较大的存储能力时,可使用基于部署后知识方案;当可以对结点进行固定位置安放时,可使用基于格子的方案。此外,若要求结点连通率为 1,可使用确定密钥管理。

结束语 本文介绍了无线传感网络密钥管理及认证方案,并给出了这些方案的部分比较。现有密钥管理方案从 3 个方面来考虑,以增强网络的各方面性能(如连通率、抗毁性);密钥池角度(密钥池分块、映射等)、部署方式角度(正态分布、均匀分布、固定安放等)、目标区域角度(小区域、正方形、六边形等);现有认证方案从对称密钥体制和非对称密钥体制方面做了较多的研究,同时有其他一些方法逐渐引入到认证过程中来,如基于秘密共享的认证。

无线传感网络的安全威胁主要归因于分布性和开放性,致使传统的许多安全方法都无法适用。针对现有方案存在的问题,以下几个方向将是重点研究的问题:

1)如何利用概率分布和对密钥池进行处理,以提高结点的共享密钥概率及抗毁性;

2)如何利用结点部署后的位置信息进行相关处理;

3)现有方案中大多假设结点感知半径是固定的。如何研究结点半径动态调整下结点的连通概率及抗毁性,也将是一个重要的问题。

4)研究支持丢包率的密钥管理和认证。目前绝大部分方案都是假设网络不存在丢包的情况来实现密钥管理和认证。而很多密钥协议的密钥生成、更新阶段,对于信息包交换的可靠性来说要求却是很高的,应考虑允许一定丢包率的现实情况来实现密钥管理协议。

参 考 文 献

[1] Shih E, Cho S, Ickes N, et al. Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks [C]// Christopher R, Mahmoud N, Michele Z, eds. Proc. of the 7th Annual Int'l Conf. on Mobile Computing and Networking (MobiCom 2001). Rome: ACM Press, 2001: 272-287

[2] Akyildiz I F, Su W, Sankarsubramaniam Y, et al. Wireless Sensor Networks: a survey[J]. Computer Networks, 2002, 38: 393-422

[3] Wood A, Stankovic J. Denial of service in sensor networks[J]. IEEE Computer, 2002, 35(10): 54-62

[4] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures [C]// Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications. 2003: 113-127

[5] Newsome J, Shi E, Song D, et al. The sybil attack in sensor networks: Analysis and defenses[C]// Proceedings of the Third International Symposium on Information Processing in Sensor Networks. 2004: 259-268

[6] 邱慧敏. Sybil 攻击原理和防御措施[J]. 计算机安全, 2005(10): 63-65

[7] Hu Yih-Chun, Perrig A, Johnson D B. Wormhole Attacks in Wireless Networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 2(2): 370-381

[8] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures[J]. Elsevier's AdHoc Networks Journal, 2003, 1(2/3): 293-315

[9] 苏忠, 林闯, 封富君, 等. 无线传感网络密钥管理的方案和协议[J]. 软件学报, 2007, 18(5): 1218-1231

[10] Eschenauer L, Gligor V D. A key management scheme for distributed sensor networks [C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. November 2002: 41-47

[11] Chan Haowen, Perrig A, Song D. Random Key Predistribution Schemes for Sensor Networks [C]// Proc. of the 2003 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2003: 197-213

[12] Du W, Deng J, Han Y S, et al. A key management scheme for wireless sensor networks using deployment knowledge [C]// Proceedings of IEEE INFOCOM'04. 2004

[13] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks[C]// Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03). 2003: 52-61

[14] Liu D, Ning P. Improving key pre-distribution with deployment knowledge in static sensor networks[J]. ACM Journal on Sensor Networks, 2005, 1(20): 204-239

[15] Liu D, Ning P. Location-based pairwise key establishments for static sensor networks[C]// ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN '03). 2003: 72-82

[16] Canh Ngo Trong, Lee Young-Koo, Lee Sungyoung. HGKM: A Group-based Key Management Scheme for Sensor Networks Using Deployment Knowledge[C]// Proceedings of the Communication Networks and Services Research Conference. 2008: 544-551

(下转第 11 页)

for dominating set: A linear problem kernel for the planar case [C]// Proc. 8th Scandinavian Workshop on Algorithm Theory. LNCS. vol. 2368, Springer, 2002: 150-159

[16] Fomin F V, Thilikos D T. Dominating sets in planar graphs: branch-width and exponential speed-up[C]// 14th ACM-SIAM Symposium on Discrete Algorithms. 2003: 168-177

[17] Fomin F V, Grandoni F, Kratsch D. Solving connected dominating set faster than 2^n[C]// Proc. 26th International Comference on Foundations of Software Technology and Theoretical Computer Science. LNCS. vol. 4337, Springer, 2006: 152-163

[18] Guha S, Khuller S. Approximation algorithms for connected dominating sets[J]. Algorithmica, 1998, 204: 374-387

[19] Ruan L, Du H, Jia X, et al. A greedy approximation for minimum connected dominating set [J]. Theoretics Computer Science, 2004, 329: 325-330

[20] Liu C, Song Y. Exact Algorithms for Finding the Minimum Independent Dominating Set in Graphs[C]// ISAAC. LNCS. vol. 4288, Springer, 2006: 439-448

[21] Randerath B, Schiermeyer I. Exact Algorithms for Minimum Dominating Set[R]. zaik-469. Köln, Germany: Zentrum fur Angewandte Informatik, 2004

[22] Gaspers S, Liedloff M. A branch-and-reduce algorithm for finding a minimum independent dominating set in graphs [C]// Proc. 32nd International Workshop on Graph-Theoretic Concepts in Computer Science. LNCS. vol. 4271, Springer, 2006: 78-89

[23] Kratsch D, Liedloff M. An exact algorithm for the minimum dominating clique problem[C]// Proc. 2nd International Workshop on Parameterized and Exact Computation. LNCS. vol. 4169, Springer, 2006: 128-139

[24] Raman V, Saurabh S, Sikdar S. Efficient exact algorithms through enumerating maximal independent sets and other techniques[J]. Theory of Computing Systems, 2007, 42: 563-587

[25] Fomin F V, Gaspers S, Saurabh S. Branching and treewidth based exact algorithms [C]// Proc. 17th International Symposium on Algorithms and Computation. LNCS. vol. 4288, Springer, 2006: 16-25

[26] van Rooij J M M, Bodlaender H L. Exact Algorithms for Edge Domination[R]. UU-CS-2007-051. Netherlands: Department of Information and Computing Sciences, Utrecht University, 2007

[27] Carr R, Fujito T, Konjevod G, et al. A 2 1/10 approximation algorithm for a generalization of the weighted edge-dominating set problem[J]. Journal of Combinatorial Optimization, 2001, 5(3): 317-326

[28] Fujito T, Nagamochi H. A 2-approximation algorithm for the minimum weight edge dominating set problem[J]. Discrete Applied Mathematics, 2002, 118(3): 199-207

[29] Parekh O. Edge domination and hypomatchable sets[C]// Symposium on Discrete Algorithms. ACM Press, 2002: 287-291

[30] Fernau H. Edge dominating set: efficient enumeration-based exact algorithms[C]// Proc. 2nd International Workshop on Parameterized and Exact Computation. LNCS. vol. 4169, Springer, 2006: 142-153

[31] Fernau H. On parameterized enumeration[C]// Proc. 8th Annual International Conference on Computing and Combinatorics. LNCS. vol. 2387, Springer, 2002: 151-179

[32] Fomin F V, Gaspers S, Saurabh S, et al. On two techniques of combining branching and treewidth[R]. No. 337. Norway: Department of Informatics, University of Bergen, 2006

[33] Weston M. A fixed - parameter tractable algorithm for matrix domination[J]. Information Processing Letters, 2004, 90: 267-272

[34] Chen J, Kanj I A, Meng J, et al. On effective enumerability of NP problems[C]// Proc. of the 2nd International Workshop on Parameterized and Exact Computation. LNCS. vol. 4169, Springer, 2006: 215-226

(上接第 6 页)

[17] Zhen Yu, Yong Guan. A Key Management Scheme Using Deployment Knowledge for Wireless Sensor Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2008, 19 (10): 1411-1425

[18] Blom R. An optimal class of symmetric key generation systems [C]// Beth T, Cot N, Ingemarsson I, eds. Proc. of the EUROCRYPT'84. New York: Springer-Verlag, 1984: 335-338

[19] Du W, Deng J, Han Y S, et al. A pairwise key pre-distribution scheme for wireless sensor networks[C]// Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03). 2003: 42-51

[20] Camtepe S A, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks [C] // Proc. of the Computer Security—ESORICS. Berlin: Springer-Verlag, 2004: 293-308

[21] Zhu S, Setia S, Jajodia S. LEAP: Efficient security mechanisms for large-scale distributed sensor networks [C] // Proc. of the 10th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2003: 62-72

[22] Morales L, Hal Sudborough I, Eltoweissy M, et al. Combinatorial Optimization of Multicast Key Management[C]//Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03)-Track 9-Volume 9. 2003: 332-340

[23] Eltoweissy M, Heydari H, Morales L, et al. Combinatorial optimization of key management in group communications[J]. Journal of Network and Systems Management, 2004, 12(1): 33-50

[24] Younis M, Ghumman K, Eltoweissy M. Location-aware combinatorial key management scheme for clustered sensor networks[J]. IEEE Trans. on Parallel and Distribution System, 2006, 17(8): 865-882

[25] Zhang Y C, Liu W, Lou W J, et al. Location-based compromise-tolerant security mechanisms for wireless sensor networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 247-260

[26] Perrig A, Szewczyk R, Tygar J, et al. SPINS: Security protocols for sensor networks[J]. ACM Wireless Network, 2002, 8(5): 521-534

[27] Liu D, Ning P. Multilevel μ TESLA : Broadcast authentication for distributed sensor networks[J]. ACM Trans. on Embedded Computing Systems, 2004, 3(4): 800-836

[28] Watro R, Kong D, Cuti Sue-fen, et al. TinyPK: Securing Sensor Networks with Public Key Technology [C] // Proceedings of the 2nd ACM Workshop on the Security of Ad Hoc and Sensor Networks. ACM Press, 2004: 59-64

[29] Benenson Z, Gedicke N, Raivio O. Realizing Robust User Authentication in Sensor Networks [C] // Workshop on Real-World Wireless sensor Networks(Realwsn). 2005

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

[31] Bauer K, Lee Hyunyoung. A Distributed Authentication Scheme for a Wireless Sensing System[J]. ACM Transactions on Information and System Security, 2008, 11(13): 1-6