一种基于无线传感器网络的密钥管理方案*)

郎为民[1] 杨宗凯[1] 吴世忠[2] 谭运猛[1]

(华中科技大学电子与信息工程系 武汉430074)[1] (中国国家信息安全测评中心 北京100091)[2]

摘 要 本文提出了一种无线传感器网络中的密钥管理方案,该方案支持密钥建立和更新等过程,并采用邻近节点概率否决投票的方法由基站撤消受节点的密钥集。同时,考虑到传感器节点资源有限的特点,方案中相关的协议和算法都比较简单,并完全避开了代价昂贵的公钥运算,从而使得方案的计算、存储和通信开销都比较小,执行效率大大提高。

关键词 无线传感器网络,密钥管理,安全方案

A Key Management Scheme for Wireless Sensor Network

LANG Wei-Min[1] YANG Zong-Kai[1] WU Shi-Zhong[2] TAN Yun-Meng[1]

(Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)[1]

(China National Information Security Testing Evaluation and Certification Center, Beijing 100091)[2]

Abstract This paper proposes a key management scheme for wireless sensor network, which supports key establishment, re-keying and revocation of the key ring owned by a compromised sensor node via probabilistic negative polling of its neighbors. Furthermore, the related protocols or algorithms are very simple and no expensive public-key operation is required in view of resource-starved sensor nodes, which minimizes the storage, computation, communication overhead and improves the efficiency of our scheme.

Keywords Wireless sensor network, Key management, Security scheme

1 引言

近年来,随着无线通信、集成电路、嵌入式计算及微机电系统等技术的飞速发展和日益成熟,具有感知能力、计算能力和通信能力的微型无线传感器开始在世界范围内出现。这些传感器具有低成本、低功耗、多功能等特点和无线通信、数据采集、信息处理、协同合作等功能。由这些微型传感器节点构成的传感器网络,能够协作地实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息,并对这些数据进行处理,从而获得详尽而准确的信息,将其传送到需要这些信息的用户。因此,传感器网络[1]是信息感知和采集的一场革命,它能够在任何时间、任何地点和任何环境条件下提供大量详实可靠的信息,因而可以被广泛应用于军事斗争、国家安全、环境监测、交通管理、医疗卫生、制造业和反恐抗灾等领域。

由于传感器网络一般配置在恶劣环境、无人区域或敌方阵地中,加之无线网络本身固有的脆弱性,因而传感器网络安全[2,3]引起了人们的极大关注。传感器网络的许多应用(如军事目标的监测和跟踪等)在很大程度上取决于网络的安全运行,一旦传感器网络受到攻击或破坏,将可能导致灾难性的后果。如何在节点计算速度、电源能量、通信能力和存储空间非常有限的情况下,通过设计安全机制,提供机密性保护和身份认证功能,防止各种恶意攻击,为传感器网络创造一个相对安全的工作环境,是一个关系到传感器网络能否真正走向实用的关键性问题。

传感器网络的研究始于20世纪90年代末期,但安全问题的研究成果近几年才陆续出现,各种密钥管理方案[4~8]不断被提出。但由于传感器网络还未被真正地模型化和量化,无线传感器网络安全方案正处于理论研究阶段,距离实际应用和形成普遍接受的标准还相差甚远。

本文第2节给出了无线传感器网络的参考模型和基本工作流程;第3节全面描述了密钥管理方案中有关的协议和算法;第4节详细分析了方案的安全性和效率;最后对全文进行总结。

2 无线传感器网络的参考模型

传感器网络是由一组传感器以 Ad Hoc 方式构成的无线网络,其目的是协作地监测、感知、采集和处理网络覆盖区域中感知对象的信息,并发布给需要这些信息的用户。传感器网络是由大量体积小、成本低的传感器节点组成的,这些节点具有无线通信、传感、数据处理等功能。一个典型的传感器网络[1]通常包括传感器节点、簇头、基站、无线或有线网络、用户等部分,如图1所示。

集成有传感单元、数据处理单元和通信模块的传感器节点可以随机或者特定地散布在指定的感知区域内,通过自组

*)国家自然科学基金资助项目(60202005)资助.郎为民 博士研究生,讲师,研究方向为传感器网络、信息安全和应用密码学.杨宗凯 博士后,教授,博士生导师,研究方向为电子商务、远程教育和网络安全.吴世忠 教授,主要从事网络攻防技术、应用密码学等研究.谭运猛 博士,副教授,研究方向为电子支付、信息安全和应用密码学.

2 丁勇,虞平,龚俭.自动入侵响应系统的研究[J].计算机科学,2003(10)

3 Geib C W, Goldman R P. plan recognition in intrusion detection systems [J]. IEEE, 2001

4 Ye Nong, Li Xiaoyang. Probabilistic techniques for intrusion detection based on computes audit data [J]. IEEE Transactions on System, 2001.31

5 张永,陆余良.攻击树在多阶段入侵检测系统中的应用[J].计算机应用与软件,2004.8

织的方式构成网络，借助于节点中内置的形式多样的传感器探测所在周边环境中的热、红外、声纳、雷达和地震波等信号及温度、湿度、噪声、移动物体的大小、速度和方向等技术指标，并将捕获到的有用信息通过初步的数据处理和信息融合后，以相邻节点接力传送的方式传送到基站。基站也可以用同样的方式将信息发送给各节点。基站直接与有线或者无线网络相连以实现用户与传感器之间的通信。传感器网络中的部分或全部节点可以移动，且每个节点都具备动态搜索、定位和恢复连接的能力。

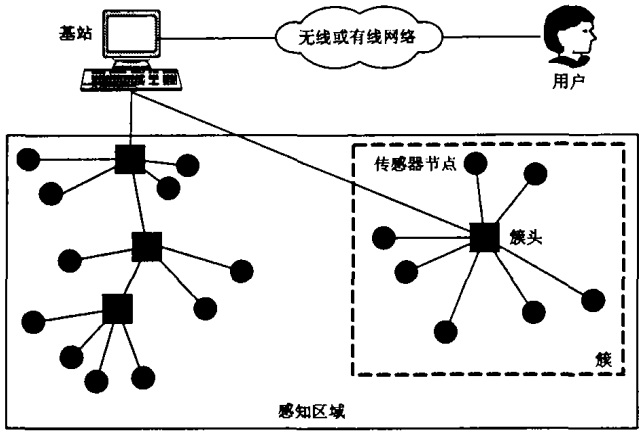

图1　传感器网络的参考模型

3　基本协议

密钥管理是数据加密技术中的重要一环，它处理密钥从生成到销毁的整个生命周期的有关问题，涉及到系统的初始化、密钥的生成、存储、备份/恢复、装入、验证、传递、保管、使用、分配、保护、更新、控制、丢失、吊销和销毁等多个方面的内容。它涵盖了密钥的整个生命周期，是整个加密系统中最薄弱的环节，密钥的泄漏将直接导致明文内容的泄漏。本文提出的密钥管理方案包括密钥建立、密钥更新和密钥撤消等过程。

3.1　密钥建立协议

在传感器网络中，一个完整的密钥建立过程通常包括三个阶段，即密钥预分发、单跳密钥发现和多跳密钥建立。

(1)基站产生 n 个密钥及其对应的标识符($2^{17}\leqslant n\leqslant 2^{20}$)，这些密钥和标识符形成一个密钥池 P，即

$$P=K\cup D$$

$$K=\{k_1,k_2,\cdots,k_n\},D=\{ID_1,ID_2,\cdots,ID_n\}$$

其中 k_i 为基站生成的密钥，ID_i 为密钥 k_i 对应的标识符。

(2)基站从 n 个密钥中随机选出 r 个密钥，组成某个传感器节点 A 的密钥环 R_A，并将密钥环加载到 A 的存储器中，即

$$R_A=K_A\cup D_A$$

$$K_A=\{k_{A1},k_{A2},\cdots,k_{Ar}\},k_{Ai}\in_R K$$

$$D_A=\{ID_{A1},ID_{A2},\cdots,ID_{Ar}\}$$

其中 $k_{Ai}\in_R K$ 表示 k_{Ai} 在集合 K 中随机地选取，ID_{Ai} 为密钥 k_{Ai} 对应的标识符。基站保存每个传感器节点的密钥环(包括 r 个密钥及其对应的标识符)。

(3)传感器节点 A 计算与基站共享的密钥 K_{BA}：

$$K_{BA}=\{ID_B\}_{K_{AM}}$$

$$K_{AM}=k_{A1}\oplus k_{A2}\oplus\cdots\oplus k_{Ar}$$

并将其加载到存储器中。其中，ID_B 表示基站的身份标识，$\{M\}_{K_i}$ 表示使用秘密密钥 K_i 对消息 M 进行加密。

至此，密钥预分发阶段结束，该阶段保证了簇内任意两个节点能够以某一概率在各自的密钥环上找到双方共享的会话密钥。

(4)传感器网络配置时，节点 A 被随机或者特定地散布在指定的感知区域内。在簇形成过程结束后，它广播一个信息：

$$A\rightarrow *:D_A,L_A$$

其中，$*$ 表示节点 A 所在簇内的任意节点，L_A 表示节点 A 的位置信息。

(5)收到该信息的所有节点将确信它在节点 A 的传输范围内，即二者在同一个簇中，并通过遍历其密钥环，检查是否存在与 A 广播的密钥标识符集相交的元素。假定节点 C 在其密钥环上发现存在与 A 标识符集相交的元素 ID_{AC}，则证明节点 C 与 A 共享有与 ID_{AC} 对应的会话密钥 K_{AC}。于是，节点 C 返回给 A 一响应消息：

$$C\rightarrow A:\{ID_{AC},L_C\}_{K_{AC}}$$

(6)A 使用共享会话密钥 K_{AC} 对响应消息进行解密，确信其密钥环与节点 C 有交集。

单跳密钥发现过程使得节点能够通过广播消息的方式，找到簇内与其共享有密钥环上某个会话密钥的节点。在单跳密钥发现过程结束后，节点 A 保存已找到共享实体的密钥，并将密钥环上其余密钥删除。

(7)对于簇内尚未与 A 建立共享密钥的节点来说，可以通过如下过程生成会话密钥。假定节点 D 在单跳密钥发现过程结束后，仍未与节点 A 建立共享密钥，但它找到与节点 C 共享的会话密钥 K_{DC}，且节点 A 与节点 C 也共享有密钥 K_{AC}。此时，A 发送一个挑战信息给节点 C 在对其进行身份认证后，该信息包含 A 和 D 共享的密钥 K_{AD} 及 A 的位置信息 L_A：

$$A\rightarrow C:\{K_{AD},L_A\}_{K_{AC}}$$

(8)节点 C 解密消息，并将其使用密钥 K_{DC} 对消息再次加密后转发给节点 D：

$$C\rightarrow D:\{K_{AD},L_A\}_{K_{DC}}$$

(9)节点 D 验证挑战消息的合法性，并发送一个响应信息给节点 A：

$$D\rightarrow A:\{nonce,L_D\}_{K_{AD}}$$

其中，$nonce$ 是一个随机数，L_D 是节点 D 的位置信息。

(10)节点 A 使用共享密钥 K_{AD} 对响应消息进行解密，确信与 D 共享的密钥已经建立。

在多跳密钥建立过程结束后，簇内任意两个节点之间都共享有一个会话密钥。

3.2　密钥撤消协议

当某个传感器结点失效或受到攻击后，撤消该节点密钥环上的密钥集是非常必要的。密钥撤消的方法是基站发动邻近节点对网络中失效节点或可疑节点进行概率否决投票，当票数超过某个门限值后，由基站实施对该节点所拥有的会话密钥集进行撤消。

(1)为对节点 A 密钥环上的密钥集进行有效的撤消，基站生成一个密钥撤消指令 I_{Rev}，该指令包含 K_A、D_A 及基站的身份信息 ID_B 和位置信息 L_B，由基站使用与每个节点共享的密钥加密后进行单播通信，声明该密钥环被撤消。若假定基站与节点 C 进行单播通信，则密钥撤消指令格式如下：

$$I_{Rev}=\{K_A,D_A,L_B\}_{K_{BC}}$$

(2)节点 C 使用 K_{BC} 对指令进行解密，确信该指令是由基站发送过来的。若验证通过，节点 C 将密钥环中的 ID_{AC} 及其对应的密钥 K_{AC} 删除。

(3)其它节点同样依照上述协议，撤消 A 密钥环上的密钥，以保证部分节点受到攻击后不会影响整个传感器网络的安全。

3.3　密钥更新协议

在许多分布式传感器网络中，通常每两个节点共享密钥

(下转第154页)

对数据传输密钥和新的共享密码段进行加密后传输到客户端，客户端用会话密钥对数据传输密钥和新共享密码段解密后放置在KeyMan模块中返回存储成功，服务器则用新的共享密码段替代安全数据库中的旧共享密码段，成功后发给客户端初始化成功信息并在客户端显示其所提供的服务，然后开始业务动作。以后的数据传输都由会话开始产生的数据传输密钥加密和解密，直至会话结束。新一轮的会话便会重新对客户端进行身份认证，启用上一次随机产生的共享密码段，进行服务器端初始化产生新的数据传输密钥，因而每一次连接的会话密钥和数据传输密钥对都不相同，这样大大提高了数据交换的安全性。

应用层的端对端安全通信模型对数据的加密和解密不依赖下层协议和硬件，只采用MIDP2.0规定的HTTPS协议，受底层变化影响很小，有很强的可移植性。采用的对称加密算法标准AES Rijndael，速度快、低延迟、消耗系统资源少，不在传输层进行协议转换，所以不存在由"WAP缺口"所带来的安全威胁，可见是一个比较理想的安全通信解决方案。

结束语 本文介绍了移动计算环境所面临的诸多安全威胁和MIDP2.0新的安全机制及网络模型，分析了MIDP 2.0的平台安全性，并提出了在纯Java环境下构建从J2ME到J2EE的、适用于资源有限的MIDP 2.0平台的应用层端到端的安全通信模型，为移动电子商务提出了集移动设备MIDP应用安全环境和客户服务器通信安全于一体的完整解决方案。

参考文献

1 Schwiderski-Grosche S, Knospe H. Secure mobile commerce. Electronics & Communication Engineering Journal, Oct. 2002
2 Antovski L, Gusev M. M-Payments. In: 25th Int. Conf. Information Technology Interfaces ITI, Cavtat, Croatia, June 2003
3 Boddupalli P, Al-Bin-Ali F, Davies N, Friday A, Storz O, Wu M. Payment Support in Ubiquitous Computing Environments. In: Proc. of the Fifth IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2003)
4 Ericsson. Mobile Applications with J2ME, a White Paper. July 2001
5 http://java.sun.com/products/midp/index.jsp, [Online], 2004 Available, JSR37, JSR118
6 http://java.sun.com/products/cdc/index.jsp, [Online], 2004 Available, JSR36, JSR218
7 http://java.sun.com/products/cldc/index.jsp, [Online], 2004 Available, JSR30, JSR139
8 Schmid M, Hill F. Protecting Data from Malicious Software. In: Proc. of the 18th Annual Computer Security Applications Conf. ACSAC, 2002
9 Kolsi O, Virtanen T. MIDP2.0 Security Enhancements. IEEE, 2004
10 Dankers J, Garefalakis T, Schaffelhofer R, Wright T. Public key infrastructure in mobile systems. Electronics & Communication Engineering Journal, Oct. 2002
11 Raju G V S, Akbani R. Elliptic Curve Cryptosystem and its Applications. IEEE, 2003
12 Richardson K W. UMTS overview. Electronics & Communication Engineering Journal, June 2000
13 Kambourakis G, Rouskas A, Gritzalis S. Using SSL/TLS in Authentication and Key Agreement Procedures of Future Mobile Networks. IEEE, 2002
14 Enrique Ortiz C. The Generic Connection Framework. Aug. 2003. http://developers.sun.com/techtopics/mobility/midp/articles/genericframework.html.
15 Forum WAP. WAP 2.0 Technical White Paper. Jan. 2002
16 Levi A, Savas E. Performance Evaluation of Public-Key Cryptosystem Operations in WTLS Protocol. In: Proc. of the Eighth IEEE Intl. Symposium on Computers and Communication, ISCC 2003
17 The Advanced Encryption Standard (Rijndael). [Online], 2004. Available at: http://home.ecn.ab.ca/~jsavard/crypto/co0401.htm
18 Daemen J, Rijmen V. The Design of Rijndael. published bySpringer-Verlag, 2002
19 Sun Microsystems. Java 2 Platform Enterprise Edition Specification, v1.4. Final Release 11/24/2003

（上接第148页）

的生命周期会超过两个节点的生命周期。但在一些情况下（如恶意攻击、密钥被破解等），密钥将失效或过期，因而共享密钥需要随着时间进行更新。密钥更新可以看作是节点密钥的自我撤销过程，需要基站重新分配给该节点一个规模为 k 的密钥环，并重新启动单跳密钥发现和多跳密钥建立过程。

4 性能分析

4.1 安全性分析

在单跳密钥发现过程中，节点 A 广播的是密钥标识符集而不是密钥本身，从而提高了通信双方建立共享密钥的安全性，攻击者无法从标识符集中获取任何与密钥有关的信息，由于它不知道 K_{AC}，因而无法伪造节点 C 对 A 的响应信息；在多跳密钥建立过程中，节点 A 在发送信息给节点 C 之前进行了身份认证，确信节点 C 不是恶意节点，且发送的消息都使用会话密钥进行了加密，因而攻击者无法破解消息的内容；在密钥撤消过程中，密钥撤消指令是由基站使用与每个传感器节点共享的密钥加密后进行单播通信的，从而有效地防止了攻击者冒充基站发布虚假的密钥撤消指令。当某节点受到攻击后，邻近节点可以向基站报告该节点行动可疑，并进行概率否决投票，当票数达到某个门限值时，基站考虑对该节点拥有的密钥集进行撤消，从而最小化部分节点受攻击后对整个网络安全的影响范围。

4.2 效率分析

在构建传感器网络密钥管理方案时，我们充分考虑到节点计算速度、电源能量、通信能力和存储空间非常有限的特点，密钥建立、更新和撤消等协议和算法都设计得比较简单，并避开了代价昂贵的公钥运算，完全使用对称加密算法来实现，计算、存储和通信开销都较小，从而使得方案的执行效率大大提高。

结论 本文提出了一种传感器网络中的密钥管理方案，它支持密钥建立、更新和撤消等过程。同时，考虑到传感器节点计算速度、电源能量、通信能力和存储空间非常有限的实际情况，方案中有关的协议和算法设计得都比较简单，并使用对称加密算法来代替了代价昂贵的公钥算法，从而使得方案的各种开销都比较小，执行效率大大提高。

参考文献

1 Akyildiz I F, Su W, Sankarasubramaniam Y, et al. A survey on sensor networks. IEEE Communications, 2002, 40(8): 102～114
2 Chan H, Perrig A. Security and Privacy in Sensor Networks. IEEE Computer, 2003, 36(10): 103～105
3 Perrig A, Stankovic J, Wagner D. Security in Wireless Sensor Networks. Communications of the ACM, 2004, 47(6): 53～57
4 Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proc. of IEEE 2003 Symposium on Research in Security and Privacy, Berkeley, CA: IEEE Computer Society, 2003. 197～213
5 Jolly G, Kuscu M C, Kokate P, et al. A Low-Energy Key Management Protocol for Wireless Sensor Network. In: Proc. of the Eighth IEEE Intl. Symposium on Computers and Communication (ISCC'03). Turkey: July 2003, 1: 335～340
6 Du W, Deng J, Han Y S, Varshney P. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security (CCS), Washington: ACM Press, Oct. 2003. 1～10
7 Wadaa A, Olariu S, Wilson L, et al. Scalable Cryptographic Key Management in Wireless Sensor Networks. In: Proc. of the 24th Intl. Conf. on Distributed Computing Systems Workshops (ICDCSW'04). Tokyo: IEEE Computer Society, March, 2004. 796～802
8 Du W, Deng J, Han Y S, et al. A Key Management Scheme for Wireless Sensor Networks Using Deploying Knowledge. In: Proc. of INFOCOM2004. Hong Kong: IEEE Computer Society, March 2004. 172～183