无线传感器网络基于身份的密钥建立协议综述

付小晶 张国印 马春光
(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(WSN)的高度自治和资源严重受限等特点,使其安全问题比传统 Ad hoc 网络面临更大的挑战。密钥管理是 WSN 安全的一个基本问题,密钥建立作为密钥管理的重要内容,必须兼顾安全性和性能等方面因素。综述了 WSN 基于身份的密钥建立协议。介绍了基于身份密码体制的基本要素,给出了基于身份的密钥协商协议的安全属性和安全模型,详细分析比较了现有的 WSN 基于身份的密钥建立协议,指出了它们安全性和性能方面的不足,并对未来的研究方向进行了探讨。

关键词 基于身份密码体制,无线传感器网络,密钥建立,密钥协商
中图法分类号 TP393 **文献标识码** A

Survey on Identity-based Key Establishment Protocols for Wireless Sensor Networks

FU Xiao-jing ZHANG Guo-yin MA Chun-guang
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

Abstract Wireless sensor networks (WSN) security faces more challenges than traditional Ad hoc networks due to its highly self-organization and limited energy. Key management is one of the fundamental security issues in WSN. As a vital part of key management, session key establishment needs to achieve a trade-off between security and performance. In this paper, a survey on Identity-based key establishment in WSN was provided. We firstly described the identedity-based cryptography from its three fundamental primitives, then presented some security properties and security models of identity-based key agreement protocols, analyzed the existing identity-based key establishment protocols for WSN to point out their shortages, and finally discusses the research area of Identity-based key establishment for WSN in the future.

Keywords Identity-based cryptography, Wireless sensor networks, Key establishment, Key agreement

1 引言

无线传感器网络(WSN, Wireless Sensor Networks)是一种特殊的 Ad hoc 网络,与传统 Ad hoc 网络相比具有节点数量大、密度高、资源更加受限、节点移动较少、节点高度自治和节点容易失效等特点。因此,传统 Ad hoc 网络的密钥建立协议不能直接应用于 WSN。目前,WSN 中节点间的会话密钥建立通常采用 3 种方式:(1)基于密钥分配中心(KDC, Key Distribution Center)方式。SPINS 协议[1]是第一个采用此方式的协议,它要求基站和簇中所有节点分别共享一个对称密钥,任何一对节点的会话密钥建立必须依赖基站。该方式具有密钥存储量较低的优点,但基站的负载较重,容易成为网络中的性能瓶颈和攻击目标。(2)密钥预分配方式。典型协议有 E-G 方案[2]及其改进协议[3-5]。该方式以某概率保证相邻节点间存在一个共享密钥,采用路径密钥保证任意两个节点都能建立对密钥。一个节点若被捕获,便会泄露网络中其他节点的共享密钥。该方式存在密钥环中的密钥利用不充分、密钥存储量较大和安全性不高等缺点。(3)基于公钥方式。每个节点预装载公私钥对,采用公钥体制在两个节点之间建立唯一的共享会话密钥。节点被捕以及增加删除不影响其他节点的密钥。基于公钥方式比基于 KDC 方式和密钥预分配方式代价高,但具有密钥存储量低、密钥连通度高、网络扩展性好和安全性高等优点。

在 WSN 早期研究中,普遍认为公钥体制由于其计算复杂性的限制,不适用于资源受限的 WSN。但近年的研究成果[6-11]表明,公钥体制可以应用于 WSN。特别地,文献[12]指出,基于身份密码体制是最适合 WSN 的公钥体制。在 WSN 中采用基于身份密码体制实现会话密钥的建立具有如下优点:(1)无需繁重的证书机制,实现隐式的密钥认证,减少了证书管理开销。(2)无条件信任第三方可由基站充当。不用解决密钥托管问题,即不用担心基站知道所有用户私钥的问题。(3)身份信息可由特殊的信息充当,如地理位置等,在

到稿日期:2009-09-25 返修日期:2009-12-30 本文受国家博士后科学基金(20070410896),中央高校基本科研业务费专项资金(HEUCF100606)资助。

付小晶(1980-),女,博士生,主要研究方向为嵌入式系统、网络与信息安全等,E-mail:fuxiaojing@hrbeu.edu.cn;张国印(1962-),男,教授,博士生导师,主要研究方向为嵌入式系统、网络与信息安全等;马春光(1974-),男,教授,博士生导师,主要研究方向为密码学与信息安全、Ad hoc与传感器网络安全等。

应用中具有重要的意义。

本文主要探讨 WSN 基于身份的会话密钥建立机制；第 2 节概述了基于身份密码体制，介绍了基于身份的认证密钥协商协议基本原理；第 3 节介绍了 WSN 基于身份的密钥协商协议的安全属性和安全模型；第 4 节分析比较现有的 WSN 基于身份的密钥建立协议，指出了协议的优缺点；最后指出了 WSN 基于身份的密钥建立协议的研究方向。

2 基于身份密码体制概述

1984 年，Shamir 提出基于身份的公钥密码体制[13]。用户的公钥基于自己的身份信息，使得密钥分发简单，不使用数字证书，减少了数字证书带来的开销。2001 年，Boneh 与 Franklin 利用 Weil 对提出第一个实用的基于身份的公钥加密体制[14]。基于身份密码体制一般采用双线性对[15]。利用椭圆曲线上的 Weil 对或 Tate 对可构造有效的基于身份的密码系统。基于身份密码体制包含 3 个基本要素：基于身份的加密(IBE，Identity-based Encryption)、基于身份的签名(IBS，Identity-based Signature)和基于身份的认证密钥协商协议(IBAKA，Identity-based Signature Authenticated Key Agreement)。IBAKA 协议采用基于身份密码体制生成公私钥对，并以 Diffie-Hellman 密钥交换协议[16]为基础进行会话密钥的协商。本节简要介绍双线性对的定义、基于双线性对的基本困难问题以及一种典型 IBAKA 协议——Chen-Kudla 协议[17]的基本原理。

定义 1 双线性对 G_1、G_T 是阶为素数 q 的循环群。群 G_2 中的任一元素的阶整除 q。P_1 是群 G_1 的生成元，P_2 是群 G_2 的生成元，从群 G_2 到群 G_1 存在可计算群同构 ψ，使 $\psi(P_2)=P_1$。双线性对 $\hat{e}:G_1\times G_2\to G_T$ 满足以下条件：

(1)双线性(Bilinearity)。$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$ 对于任意 $P\in G_1$，$Q\in G_2$，$a,b\in_R Z_q^*$ 都成立；

(2)非退化性(Nondegeneracy)。对于任意 $P\in G_1$，$Q\in G_2$，存在 $\hat{e}(P,Q)\neq 1_{G_T}$，1_{G_T} 是 G_T 的单位元；

(3)可计算性(Computable)。存在一种有效的算法计算 $\hat{e}(P,Q)$。

定义 2 双线性 Diffie-Hellman(BDH)问题

对于 $a,b,c\in_R Z_q^*$，已知 $aP_i,bP_j,cP_k,i,j,k\in\{1,2\}$，计算 $\hat{e}(P_1,P_2)^{abc}$。

定义 3 判定双线性 Diffie-Hellman(DBDH)问题

对于 $a,b,c,r\in_R Z_q^*$，已知 $aP_i,bP_j,cP_k,\hat{e}(P_1,P_2)^r,i,j,k\in\{1,2\}$，判断 $r=abc$ 是否成立。

Chen-Kudla 协议基于 BDH 困难问题假设，由 3 个算法组成：参数建立(Setup)算法、私钥生成(Extract)算法和密钥协商(Key Agreement)算法。协议步骤如下：

(1)Setup

选择 $s\in_R Z_q^*$ 作为主密钥，选择 $S\in\{0,1\}^*$ 作为会话密钥标识。计算系统公钥 $P_{pub}=sP_1\in G_1$，选择 MtP(Map to Point)杂凑函数 $H_1:\{0,1\}^*\to G_2$，$H_2:\{0,1\}^*\to G_1$。

(2)Extract

给定共开身份 $ID\in\{0,1\}^*$，计算公钥 $Q_{ID}=H_1(ID)\in G_2$，将任意字符串映射成群 G_2 中的点。计算私钥 $d_{ID}=sQ_{ID}$。

(3)Key Agreement

①A 随机选择 $x\in_R Z_q^*$，计算 $E_A=xQ_A$，$S_A=xH_2(S)$，将 E_A,S_A 发送给 B；

②B 随机选择 $y\in_R Z_q^*$，计算 $E_B=yQ_B$，$S_B=yH_2(S)$，将 E_B,S_B 发送给 A；

③A 验证 $\hat{e}(H_2(S),E_B)=\hat{e}(S_B,Q_B)$，如果成立，计算 $K_{AB}=\hat{e}(\psi(d_A),xQ_B+E_B)$；

④B 验证 $\hat{e}(H_2(S),E_A)=\hat{e}(S_A,Q_A)$，如果成立，计算 $K_{BA}=\hat{e}(y\psi(Q_A)+\psi(E_A),d_B)$；

⑤A、B 得到共享秘密 $K=K_{AB}=K_{BA}=\hat{e}(\psi(Q_A),Q_B)^{s(x+y)}$，计算得到共享会话密钥 $SK=H_3(A,B,E_A,E_B,S_A,S_B,K)$。

3 WSN 基于身份的密钥建立协议安全性评价标准

密钥建立协议可分为两类[18]：(1)密钥传输协议，一方实体产生会话密钥并且安全传给另一方或多方。(2)密钥协商协议，各个通信实体共同参与共享会话密钥的生成，会话密钥值包含每个实体提供的份额。密钥协商协议比密钥传输协议具有较多的安全属性和优点，本节主要介绍 WSN 中 IBAKA 协议的安全属性和安全模型。

WSN 安全协议易遭受的攻击有：中间人攻击、拒绝服务攻击、消息重放攻击和反射攻击等。一个安全的 IBAKA 协议应该能够抵抗被动攻击和主动攻击，并且能够抵制基于身份密码系统易遭受的攻击——密钥生成中心(KGC)攻击。KGC 一般由基站充当，如果 KGC 的主密钥被攻陷，则所有用户的私钥泄露。一个安全的基于身份的密钥协商协议，除了密钥认证和密钥确认外，还需满足下面一些安全属性[17,19,20]：

(1)前向保密性(Forward Secrecy)：一个或多个参与实体的长期私钥泄漏，已建立的会话密钥不会被攻破。具体分为：

①部分前向保密性：一部分参与实体的长期私钥泄漏，已建立的会话密钥不会被攻破。

②完美前向保密性：如果所有参与实体的长期私钥泄漏，已建立的会话密钥不会被攻破。

③主密钥前向保密性(或者 KGC 前向保密性)：KGC 的主密钥泄漏(由此所有用户的长期私钥泄漏)，已建立的会话密钥不会被攻破。

(2)已知密钥安全(Known-key Security)：每一次密钥协商过程中，实体 A 和 B 都应该生成唯一的共享会话密钥，每一次协商的会话密钥是独立产生的，不会因其他会话密钥的泄露而暴露。

(3)抗密钥泄露伪装(Key-compromise Impersonation)：如果实体 A 的长期私钥泄漏，获得 A 的长期私钥的攻击者只具有冒充 A 的能力，而不能伪造其他实体与 A 生成会话密钥。

(4)未知密钥共享(Unknown Key-share Resilience)：在没有实体 A 知道的情况下，不能强制实体 A 与实体 B 共享一个会话密钥。

(5)非密钥控制(Key Control)：任何实体都不能强制会

话密钥是一个预先确定的值。

1993年，Bellare和Rgowaya首次提出密钥交换协议的可证安全方法，称为Bellare-Rgowaya(BR)模型[21]。可用于证明IBAKA协议安全性的安全模型有：

(1)BR扩展模型

Blake和Wilson等对BR模型作了扩展[22]，称作BJM模型，适用于IBAKA协议安全性分析。Chen等[23]利用BR模型和BJM模型证明了IBAKA协议的安全性，首次提出使用双线性对的IBAKA协议的形式化安全分析方法。Chen等对BR模型作了进一步扩展[17]，采用内置判定函数的方法使得模拟器能够利用敌手的帮助来计算会话密钥或者保持随机预言机回答的一致性。在BR扩展模型下安全的IBAKA协议满足已知密钥安全、未知密钥共享、抗密钥泄露伪装和非密钥控制等安全属性。

(2)CK扩展模型

2001年，Canetti和Krawczyk提出了一种形式化分析密钥交换协议的模型，称为Canetti-Krawczyk(CK)模型[24]。该模型采用了不可区分性的方法来定义安全。如果一个密钥交换协议用该模型证明是安全的，则能够确保该协议具备许多安全属性。文献[20]对CK模型增添一个新的攻击能力——攻陷KGC，对模型进行了扩展。CK扩展模型具有确保KGC前向保密性的能力，可以用于IBAKA协议安全性证明。

4 WSN基于身份的密钥建立协议

将基于身份的密码体制用于WSN密钥建立已经有一些研究成果[25-32]，本节按照密钥传输协议和密钥协商协议两类来具体阐述其中一些典型的协议，并分析比较其安全性和性能。

4.1 基于身份的会话密钥传输协议

程宏兵等[27]设计了一个基于BF-IBE[14]的可认证加密/解密算法，实现了消息保密传输和认证。在此基础上提出了一个WSN节点间可认证的密钥建立协议。

协议基本步骤：①欲建立会话密钥的通信实体A与B。A生成会话密钥，采用基于身份的可认证加密算法对会话密钥加密，然后将结果连同用会话密钥的密钥加密的消息密文一同传递给B。②B接收到消息后，采用可认证解密算法对A进行身份认证并解密得到会话密钥，进而解密得到消息明文。

优点：可认证加密算法简单，没有点乘运算，提高了算法效率。实现认证机制、身份认证和消息认证同时完成。该协议与传统的基于PKI的密钥协商协议和密钥预分配方式相比具有一定优势。

缺点：会话密钥由一方确定，不具备密钥协商协议的许多基本属性，没有实现双向身份认证。

庞辽军等[28]提出一个采用IBS和对称密码算法相结合的签密方案，即对称密钥由签密方生成，解签密方可验证签名，并且解密得到对称密钥，进而解密得到消息明文。基于此签密方案设计了一个WSN节点间可认证的密钥建立协议。

协议基本步骤：①欲建立会话密钥的通信实体A与B。A生成密钥材料Key和一个随机数nonce，采用签密算法对其进行加密和签名，然后将结果发送给B。②B验证签名并解密得到Key和nonce。由Key按照一定的算法导出共享的会话密钥EK和消息完整性验证密钥IK。并用IK生成nonce等信息的消息完整性校验码MIC，将nonce和MIC等信息发送给A。③A利用相同的导出算法生成EK和IK，然后利用IK对MIC进行验证，完成对B的身份认证。

优点：协议可以抵制消息重放攻击和伪造攻击。采用了对称密码算法实现密钥材料的保密传输，代价较低。采用数字签名和消息验证码方法实现了双向交互认证。比传统的基于PKI的密钥协商协议效率高。

缺点：会话密钥由一方确定。不具备密钥协商协议的许多基本属性。协议采用3次双线性对运算，由于双线性对运算代价较高，对于资源非常受限的节点来说，协议代价仍不可忽视。

4.2 基于身份的密钥协商协议

杨庚等[29]提出一个适合WSN的基于身份的会话密钥协商方案。密钥的分配与建立过程只在网络拓扑形成阶段执行一次，共享会话密钥建立之后，通信数据都采用该会话密钥进行对称加密。协议基本思想：节点通过组播技术向邻居节点发送其身份信息，通信双方采用BF-IBE算法加密交换的参数，彼此得到密文信息，解密后得到交换的参数，采用DH密钥交换协议计算出共享会话密钥。

优点：协议实现简单，代价较小。通过仿真实验，该协议与基于KDC方式和密钥预分配方式的密钥建立协议相比，在能量消耗、平均运行时间和平均被俘概率方面具有一定的优势。

缺点：协议没有实现认证机制。会话密钥的建立只在节点加入或者节点移动的情况下进行。会话密钥一旦泄漏，将导致以前和以后所有通信数据的泄漏。

Zhang[30]针对WSN提出一个基于位置的抗捕获安全机制。提出了基于位置的相邻节点认证协议，节点的私钥由节点的身份(ID)和地理位置信息生成。节点采用消息认证码，通过三次握手与相邻节点实现双向认证。共享认证密钥由节点的私钥以及相邻节点的ID和地理位置信息生成。在认证过程中增加了相邻节点的位置检测，即利用双方地理位置信息计算出彼此的距离，来判断相邻节点是否确实在自己的相邻范围，阻止恶意节点冒充相邻节点进行认证。该文献提出了“立即”对密钥(IPKs，Immediate Pairwise Keys)和“多跳”对密钥(MPKs，Multi-hop Pairwise Keys)协商协议。IPKs由邻居节点认证阶段生成的认证密钥进一步生成。MPKs采用Chen-Kudla协议的简化版本实现，实现了多跳距离的两个节点之间的安全通信，假设多跳距离节点之间的路径由路由协议完成。

优点：将节点身份与地理位置信息绑定，减小被捕获节点的破坏范围。提供相邻节点的认证机制。“立即”对密钥提供了点到点的安全通信。“多跳”对密钥实现了端到端的安全通信。为WSN提供了较高的安全和连通度。协议采用较少的双线性对运算，具有较低的计算和通信代价。

缺点：“立即”对密钥协商协议不满足已知密钥安全、前向保密性等基本安全属性。“多跳”对密钥协商协议需要底层的路由协议完成多跳距离的节点间的路由路径建立。添加节点时，需要测量地理位置信息，才能生成节点的私钥，增加了网络扩展的代价。

Kampanakis[31]对基于身份的密码体制在下一代传感器网络中的应用和可行性进行了研究。采用混合网络(Hybrid

Networks)结构解决了资源受限的节点不能有效地执行公钥操作的困难，使得公钥体制不再因为其计算复杂性而受限于WSN。提出了混合网络结构WSN中两个节点进行密钥协商的基本思想。混合网络由大量低端节点(MicaZ,TelosB)和少量高端节点(Imote2)构成。高端节点执行代价高的操作，如数据聚合等操作。低端节点之间进行安全通信时，需要高端节点的参与才能建立共享会话密钥。每个节点存储自己的私钥 d_{ID} 和密钥协商交换信息 $d_{ID}Q_{ID}$。为了降低计算和通信开销，高端节点可以预存储一些低端节点的密钥协商交换信息。混合网络结构WSN密钥协商过程如图1所示。

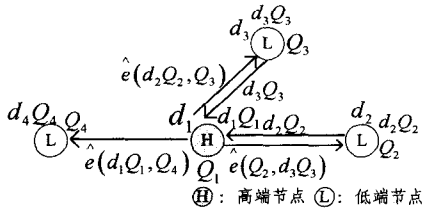

图1 混合网络结构的WSN密钥协商过程

“L-H”对密钥协商，即低端节点 i 与高端节点 k 的对密钥协商过程：

①节点 i 将 d_iQ_i 传递给节点 k；②节点 k 计算得到会话密钥；③节点 k 计算 $E_{ki}=\hat{e}(Q_k,Q_i)$，将 E_{ki} 传递给节点 i；④节点 i 计算得到会话密钥 $K=(E_{ki})^{d_i}=\hat{e}(Q_k,Q_i)^{d_id_k}$。

“L-L”对密钥协商，即在高端节点 k 的参与下低端节点 i 与低端节点 j 的对密钥协商过程：

①节点 i 将 d_iQ_i 传递给节点 k；②节点 k 计算 $E_{ij}=\hat{e}(Q_j,d_iQ_i)$，将 E_{ij} 传递给节点 j；③节点 j 计算得到会话密钥 $K=(E_{ij})^{d_j}=\hat{e}(Q_j,Q_i)^{d_id_j}$；④节点 j 将 d_jQ_j 传递给节点 k；⑤节点 k 计算 $E_{ji}=\hat{e}(d_jQ_j,Q_i)$，将 E_{ji} 传递给节点 i；⑥节点 i 计算得到会话密钥 $K=(E_{ji})^{d_i}=\hat{e}(Q_j,Q_i)^{d_id_j}$。

优点：密钥协商过程中，高端节点可以高效地执行代价较高的公钥操作，如双线性对运算等，将结果传递给低端节点，节约了低端节点的能源。

缺点：低端节点之间进行密钥协商，需要与高端节点进行通信，增加了协议的复杂性和通信代价。当大量的低端节点需要通信时，高端节点的计算和通信负载将成为整个网络通信的瓶颈。该协议只提供一个混合网络结构WSN密钥协商协议的基本框架，协议需要进一步完善。

Zhang[32]提出了一个异构WSN密钥建立协议。网络由大量低端节点(簇内节点)和少量高端节点(簇头节点)组成。由于高端节点和低端节点通信范围的差异以及不同节点之间能量消耗的差异，导致非双向链路节点的存在。非双向链路节点只能与其他节点进行单向通信，不能建立共享会话密钥。本文针对非双向链路节点，提出了簇内节点对密钥建立和簇头节点对密钥建立协议。协议的基本思想是双向链路的节点直接建立共享会话密钥。非双向链路的节点需要与其相邻双向链路节点建立信任关系，协商会话密钥，以后借助相邻双向链路节点与其他节点进行安全通信。协议采用消息认证码实现了相邻节点认证。簇内节点采用随机密钥预分配方法建立认证和会话密钥。簇头节点之间采用基于身份的密钥协商协议建立认证和会话密钥。

优点：考虑了非双向链路节点的密钥建立，实现了相邻节点身份认证，提高了节点的使用率和网络连通度。普通节点采用随机预分配密钥方法建立会话密钥，减小了协议代价。高端节点采用基于身份的密钥协商协议，采用节点预先存储双线性对运算结果的方法来降低协议计算代价。

缺点：大量的低端节点之间采用随机密钥预分配方法建立共享密钥，仍然具有抗节点捕获能力差、网络扩展性差等缺点。非双向链路簇内节点只能与其相邻节点建立共享密钥，不能与簇头节点建立共享密钥，并且要求非双向链路节点和相邻节点构成强连通分量，本文仅考虑3个节点构成的强连通分量。

4.3 密钥建立协议安全性和性能比较

4.1节和4.2节中的密钥建立协议在安全性和性能方面的比较结果如表1所列。Zhang-I[30]协议和Zhang-II[30]协议分别表示“立即”对密钥和“多跳”对密钥协商协议。计算代价包括身份认证的计算代价和密钥建立的计算代价。其中，P 表示双线性运算，S_1 表示群 G_1 上的乘法运算，E 表示群 G_T 上的幂运算。密钥传输协议的计算代价为参与密钥建立的各个实体总的计算代价。密钥协商协议的计算代价只列出一个实体的计算代价(其他参与实体相同)。由于各方实体的密钥建立计算代价不同，Kampanakis[31]协议分别列出了“L-H”对密钥和“L-L”对密钥协商各个参与实体的计算代价。Yuanyuan Zhang[32]协议分别列出了2种拓扑结构下非双向链路节点密钥协商中各个参与实体的计算代价。

基于公钥体制的密钥建立协议是否能有效地应用于WSN中，主要取决于公钥操作的计算代价和节点通信的能耗。现有的WSN基于身份的密钥建立协议为了减小计算代价而采用的方法主要是尽量减少公钥操作，例如尽量减少双线性对数量，只在少部分高端节点进行双线性对运算；利用消息认证码代替数字签名实现身份认证；离线计算一些公钥操作，如双线性对运算，部署前将计算结果装载在节点中。现有协议存在的缺点主要有：(1)大多数协议只能实现部分安全属性，协议安全性缺少完备的证明。(2)一些协议没有考虑KGC的前向安全问题，不满足KGC前向保密性。(3)只能实现隐式的密钥认证，缺少高效的双向身份认证机制。(4)大多数协议只是针对WSN节点资源受限的特点，对于节点高度自治、节点容易被捕获和节点易失效等自身特点考虑不足。

表1 典型的WSN基于身份的密钥建立协议比较

协议	网络结构	密钥建立方式	身份认证	已知密钥安全	前向保密性	抗密钥泄露伪装	网络扩展性	计算代价
Cheng[27]	—	传输	√	—	—	—	强	2P
Pang[28]	—	传输	√	—	—	—	强	$3P+S_1+E$
Yang[29]	—	协商	×	√	√	√	强	$2P+E$
Zhang-I[30]	—	协商	√	×	×	√	一般	P
Zhang-II[30]	—	协商	√	√	√	√	一般	$2P+2S_1$

Kampanakis[31]	异构	协商	×	×	×	×	强	S_1+E,$2P+S_1+E$ 或 S_1+E,S_1+E,$2P$
Zhang[32]	异构	协商	√	√	√	√	差	$4P+2S_1$ 或 $3P+2S_1$

结束语 目前,WSN基于身份的密钥建立协议主要针对WSN节点资源受限的特点,将现有的基于身份的密码算法经过简化用于WSN密钥建立。协议在安全性和效率方面还有所欠缺,下一步的研究方向主要有:

(1)充分考虑WSN自身特点,对基于身份的密码体制进行研究,设计实用的WSN密钥协商协议。在密码系统实现方面也需要进一步研究,如提高双线性对运算的性能等。

(2)可双向认证的密钥协商协议。由于基于身份的密码系统一般使用双线性对,双线性对运算对资源非常受限的节点来说代价仍然较高。引入认证机制,尤其是使用双线性对运算的认证密钥计算和数字签名等,会增加协议的代价。如何设计高效的认证机制需要进一步研究。

(3)可证安全的密钥协商协议。WSN节点高度自治和容易被捕获的特点使其私钥泄漏问题比传统网络严重,提高协议的安全性需要进一步研究。基站(KGC)的安全性需要更多地考虑。并且需要研究适合于WSN的IBAKA协议安全模型。根据不同安全要求和应用需求设计不同安全级别的可证安全密钥协商协议。

(4)群组密钥协商协议。现有协议主要是对密钥的建立。分层的WSN一般按簇来组织,不同簇的多个成员之间需要交换信息,经过较少轮在多方实体间建立共享会话密钥其效率比传统方案的高。研究适合于WSN的基于身份的群组信任模式下的多方会话密钥建立是未来的研究方向之一。

(5)异构WSN密钥协商协议。异构WSN中节点的结构和功能不同,计算和存储可以不同,运行的协议也可以不同。现有协议采用的WSN网络模型都只包含单个基站和功能单一的传感器节点,并且假定节点是静止的。对于包含多个基站以及特殊节点(如移动手持终端、入侵监测单元等)的异构WSN的可认证密钥协商协议需要进一步研究。可以充分发挥异构WSN中高性能节点的作用,使基于身份密码体制有效地应用于WSN密钥建立协议中。计算代价和通信代价的平衡是进一步的研究问题。

结束语 WSN自身的特点使它面临着比传统无线网络更大的安全挑战,传统Ad hoc网络的密钥建立协议不能直接应用于WSN中。基于身份的密钥协商适合WSN的会话密钥建立,无需繁重的证书机制,不用解决密钥托管问题,而且身份信息可由地理位置等特殊信息充当,在应用中具有重要的意义。现有的WSN基于身份的密钥建立协议主要是基于身份的对密钥协商协议,并且一般基于简单的WSN网络模型。异构WSN可证安全的对密钥和组密钥协商协议是未来的研究方向之一。

参 考 文 献

[1] Perrig A, Szewczyk R, Wen V, et al. SPINS: Security Protocols for Sensor Networks[C]// Proceedings of the 7th Annual Int'l Conf. on Mobile Computing and Networks. 2001: 189-199

[2] 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. 2002: 41-47

[3] Pietro R D, Mancini L V, Mei A. Random-key Assignment for Secure Wireless Sensor Networks[C]// Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks. 2003: 62-71

[4] Chan H, Perrig A, Song D. Random Key Predistribution Sch-emes for Sensor Networks[C]// Proceedings of the IEEE Symposium on Security and Privacy. 2003: 197-213

[5] Ren K, Zeng K, Lou W J. A New Approach for Random Key Pre-distribution in Large-scale Wireless Sensor Networks[J]. Wireless Communication and Mobile Computing, 2006, 6(3): 307-318

[6] Wander A S, Gura N, Eberle H, et al. Energy Analysis of Public-key Cryptography for Wireless Sensor Networks[C]// Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications. 2005: 324-328

[7] Piotrowski K, Langendoerfer P, Peter S. How Public Key Cryptography Influences Wireless Sensor Node Lifetime[C]// Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks. 2006: 169-176

[8] Liu A, Ning P. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks[C]// Proceedings of the 7th International Conference on Information Processing in Sensor Networks. 2008: 245-256

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

[10] Li J J, Tan L, Long D Y. A New Key Management and Authentication Method for WSN Based on CPK[C]// Proceedings of the 2008 ISECS International Colloquium on Computing, Communication, Control, and Management. 2008: 486-489

[11] Arazi O, Qi H. Load-balanced Key Establishment Methodologies in Wireless Sensor Networks[J]. International Journal of Security and Networks, 2006, 1(3/4): 158-166

[12] Oliveira L B, Dahab R, Lopez J, et al. Identity-Based Encryption for Sensor Networks[C]// Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops. 2007: 290-294

[13] Shamir. Identity-based Cryptosystems and Signatures Schemes [C]// Proceedings of CRYPTO 84 on Advances in Cryptology. 1985: 47-53

[14] Boneh D, Franklin M. Identity Based Encryption from the Weil Pairing[C]// Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. 2001: 213-229

[15] Dutta R, Barua R, Sarkar P. Pairing-based Cryptographic Protocols: A Survey[DB/OL]. Cryptology ePrint Archive, Report 2004/064. http://eprint.iacr.org/2004/064.pdf, 2004

[16] Diffie W, Hellman M E. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[17] Chen L, Cheng Z, Smart N P. Identity-based Key Agreement Protocols from Pairings[J]. International Journal of Information Security, 2007, 6(4): 213-241

[18] Menezes A, Van Oorschot P C, Vanstone S. Handbook of Applied Cryptography[M]. Boca Raton, FL, USA: CRC Press, 1996

[19] Law L, Menezes A, Qu M H, et al. An Efficient Protocol for Authenticated Key Agreement[J]. Designs, Codes and Cryptography, 2003, 28(2): 119-134

[20] 李兴华，马建峰，文相在. 基于身份密码系统下 Canetti-Krawczyk 模型的安全扩展[J]. 中国科学 E 辑：信息科学，2004，34(10)：1185-1192

[21] Bellare M, Rogaway P. Entity Authentication and Key Distribution[C]// Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology. 1993: 232-249

[22] Blake-Wilson S, Johnson D, Menezes A. Key Agreement Protocols and Their Security Analysis[C]// Proceedings of the 6th IMA International Conference on Cryptography and Coding. 1997: 30-45

[23] Chen L, Kulda C. Identity based Authenticated Key Agreement Protocols from Pairing[C]// Proceedings of 16th IEEE Computer Security Foundations Workshop. 2003: 219-233

[24] Canetti R, Krawczyk H. Analysis of Key-exchange Protocols and Their Use for Building Secure Channels[C]// Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology. 2001: 453-474

[25] Yang G, Rong C M, Veigner C, et al. Identity-based Key Agreement and Encryption for Wireless Sensor Networks[J]. IJCSNS International Journal of Computer Science and Network Security, 2006, 6(5B): 182-189

[26] 杨庚，王江涛，程宏兵，等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报，2007：35(1)：180-184

[27] Cheng H B, Yang G. An Authenticated Identity-based Key Establishment and Encryption Scheme for Wireless Sensor Networks[J]. The Journal of China Universities of Posts and Telecommunications, 2006, 13(2): 31-38

[28] 庞辽军，焦李成，王育民. 无线传感器网络节点间认证及密钥协商协议[J]. 传感技术学报，2008，21(8)：1422-1426

[29] 杨庚，程宏兵. 一种有效的无线传感器网络密钥协商方案[J]. 电子学报，2008，36(7)：1389-1395

[30] Zhang Y H, 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

[31] Kampanakis P T. Identity-based Cryptography Feasibility & Applications in Next Generation Sensor Networks[DB/OL]. http://www.lib.ncsu.edu/theses/available/etd-08042007-125351/unrestricted/etd.pdf, 2007

[32] Zhang Y Y, Gu D W, Li J R. Exploiting Unidirectional Links for Key Establishment Protocols in Heterogeneous Sensor Networks[J]. Computer Communications, 2008, 31(13): 2959-2971

（上接第 20 页）

[35] Chai Y, Wang Q, Jia J, et al. A novel gait recognition method via fusing shape and kinematics features[A]// Int. Conf. on Multimedia and Expo[C]. Springer Berlin, 2006: 80-89

[36] Ekinci M. Human identification using gait [J]. Turkish Journal of Electrical Engineering and Computer Sciences, 2006, 14(2): 267-291

[37] Lu J, Zhang E. Gait recognition for human identification based on ICA and fuzzy SVM through multiple views fusion [J]. Pattern Recognition Letters, 2007, 28(16): 2401-2411

[38] Tyagi A, Davis J, Keck M. Multiview fusion for canonical view generation based on homography constraints[A]// ACM Int. Workshop on Video Surveillance and Sensor Networks[C]. 2006: 61-69

[39] Wang Y, Yu S, Wang Y, et al. Gait recognition based on fusion of multiview gait sequences[A]// Int. Conf. on Biometrics[C]. 2006: 605-611

[40] Huang G, Wang Y. Gender classification based on fusion of multi-view gait sequences[A]// Asian Conf. on Computer Vision [C]. Tokyo, Japan: Springer, 2007: 462-471

[41] Kale A, Roy-chowdhury A K, Chellappa R. Fusion of gait and face for human identification[A]// Int. Conf. Acoustics, Speech, and Signal Processing[C]. 2004: 901-904

[42] Lee T K M, Ranganath S, Sanei S. Fusion of Chaotic Measure Into a New Hybrid Face-Gait System for Human Recognition [A] // Int. Conf. on Pattern Recognition[C]. 2006: 541-544

[43] Liu Z, Sarkar S. Outdoor recognition at a distance by fusing gait and face [J]. Image and Vision Computing, 2007, 25: 817-832

[44] Geng X, Wang L, Li M, et al. Adaptive fusion of gait and face for human identification in video[A]// IEEE workshop on Applications of Computer Vision[C]. USA, 2008: 1-6

[45] Zhou X, Bhanu B, Han J. Human recognition at a distance in video by integrating face profile and gait[A] // Audio and Video-based Biometric Person Authentication[C]. 2005: 533-543

[46] Zhou X, Bhanu B. Feature fusion of face and gait for human recognition at a distance in video[A]// Int. Conf. on Pattern Recognition[C]. 2006: 529-532

[47] Zhou X, Bhanu B. Integrating face and gait for human recognition at a distance in video [J]. IEEE Trans. Systems Man Cybernetic. Part B, 2007, 37(5): 1119-1137

[48] Zhou X, Bhanu B. Feature fusion of side face and gait for video-based human identification [J]. Pattern Recognition, 2008, 41(3): 778-795

[49] Zhang T, Li X, Tao D, et al. Multimodal biometrics using geometry preserving projections [J]. Pattern Recognition, 2008, 41(3): 805-813

[50] Doretto G, Chiuso A, Soatto S, et al. Dynamic textures [J]. International Journal of Computer Vision, 2003, 51: 91-109

[51] Bissacco A, Saisan P, Soatto S. Gait recognition using dynamic affine invariants[A] // Int. Conf. Symp. Math. Theory of Networks and Systems[C]. 2004

[52] Wright J, Yang A, Ganesh A, et al. Robust face recognition via sparse representation [J]. IEEE Trans. on Pattern Analysis and Machine Intelligence, 2009, 31(2): 210-227