# 无线传感器网络安全研究*)

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** 随着传感器网络研究的深入和不断走向实用,安全问题引起了人们的极大关注。由于传感器节点的计算速度、电源能量、通信能力和存储空间非常有限,且一般配置在恶劣环境、无人区域或敌方阵地中,这给传感器网络安全方案的设计提出了诸多挑战。本文分析了无线传感器网络(WSN)的安全需求,并从密钥管理、身份认证和攻防技术三个方面归纳了国内外传感器网络安全问题的研究进展情况。最后,基于对传感器网络安全未决问题的分析和评述,指出了今后该领域的研究方向。

**关键词** 传感器网络,安全,密钥管理,认证,网络攻防

## Research on the Security in 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** As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. Typical sensors posses limited computation, energy, computation, memory resources and they are always deployed in a harsh, unattended or hostile environment, so the security issues posed by sensor networks represent a rich and challenging field of research problems. In this paper, we propose various security requirements with regard to Wireless Sensor Network (WSN). Furthermore, we analyze status quo of WSN from three aspects: keymanagement, identity authentication as well as attacks and counter-measures. In conclusion, we point out its development direction based on the analysis and remark of problems remaining unsolved in WSN.

**Keywords** Sensor network, Security, Key management, Authentication, Attacks and countermeasures

## 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、多功能等特点的无线通信、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[1]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。

本文提出了传感器网络的安全需求,并从密钥管理、身份认证和攻防技术三个方面归纳了国内外传感器网络安全问题的研究进展情况。最后,基于对传感器网络安全未决问题的分析和评述,指出了今后该领域的研究方向。

## 2 无线传感器网络的安全需求

传感器网络具有许多鲜明特点,如通信能力有限、电源能量有限、计算速度和存储空间有限、传感器节点配置密集和网络拓扑结构灵活多变等,这些特点对于安全方案的设计提出了一系列挑战。一种比较完善的无线传感器网络解决方案应当具备如下基本特征[2~4]。

### 2.1 机密性

一个传感器网络不应当向其他网络泄漏任何敏感的信息。在许多应用(如密钥分发等)中,节点之间传递的是高度敏感的数据。这些数据一旦被攻击者获取,整个网络的安全将无法得到保障,因而通过密钥管理协议建立的秘密密钥及其它传感器网络中的机密信息(如传感器身份标识等),必须保证仅对授权用户公开。同时,因密钥泄漏造成的影响应当尽可能控制在一个小的范围内,从而使得一个密钥的泄露不至于影响整个网络的安全。解决数据机密性的最常用方法是使用通信双方共享的会话密钥来加密待传递的消息,该密钥不为第三方所知。在传感器节点之间的会话密钥建立后,可以通过多

*)基金项目:国家自然科学基金资助项目(60202005)。郎为民 博士研究生,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,研究方向为传感器网络、远程教育和网络安全。吴世忠 教授,主要从事网络攻防技术、应用密码学等方面研究。谭运猛 博士,副教授,研究方向为传感器网络、信息安全和应用密码学。

跳的方式在节点和基站之间建立安全的信道。

### 2.2 真实性

节点身份认证或数据源认证在传感器网络的许多应用中是非常重要的。在传感器网络中，攻击者极易向网络注入信息，接收者只有通过数据源认证才能确信消息是从正确的节点处发送过来的。同时，对于共享密钥的访问控制权应当控制在最小限度，即共享密钥只对那些已认证过身份的用户开放。在传统的有线网络中，通常使用数字签名或数字证书来进行身份认证，但这种公钥算法不适用于通信能力、计算速度和存储空间都相当有限的传感器节点。针对这种情况，传感器网络通常使用共享唯一的对称密钥来进行数据源的认证。

### 2.3 完整性

在通信过程中，数据完整性能够保证接收者收到信息在传输过程中没有被攻击者篡改或替换。在基于公钥的密码体制中，数据完整性一般是通过数字签名来完成的，但资源有限的传感器网络无法支持这种代价昂贵的密码算法。在传感器网络中，通常使用消息认证码来进行数据完整性的检验，它使用的是一种带有共享密钥的散列算法，即将共享密钥和待检验的消息连接在一起进行散列运算，对数据的任何细微改动都会对消息认证码的值产生较大影响。

### 2.4 新鲜性

在传感器网络中，基站和簇头需要处理很多节点发送过来的采集信息，为防止攻击者进行任何形式的重放攻击(将过时消息重复发送给接收者，耗费其资源使其不能提供正常服务)，我们必须保证每条消息是新鲜的。简单地说，新鲜性是指发送方传给接收者的数据是在最近时间内生成的最新数据。由于密钥可能需要进行更新，因而新鲜性还体现在密钥建立过程中，即通信双方所共享的密钥是最新的。

### 2.5 扩展性

无线传感器中传感器节点数量大，分布范围广，环境条件、恶意攻击或任务的变化可能会影响传感器网络的配置。同时，节点的经常加入或失效也会使得网络的拓扑结构不断发生变化。传感器网络的可扩展性表现在传感器数量、网络覆盖区域、生命周期、时间延迟、感知精度等方面的可扩展极限。因此，给定传感器网络的可扩展性级别，安全解决方案必须提供支持该可扩展性级别的安全机制和算法，来使传感器网络保持良好的工作状态。

### 2.6 可用性

传感器网络的安全解决方案所提供的各种服务能够被授权用户使用，并能够有效防止非法攻击者企图中断传感器网络服务的恶意攻击。一个合理的安全方案应当具有节能的特点，各种安全协议和算法的设计不应当太复杂，并尽可能地避开公钥运算，计算开销、存储容量和通信能力也应当充分考虑传感器网络资源有限的特点，从而使得能量消耗最小化，最终延长网络的生命周期。同时，安全性设计方案不应当限制网络的可用性，并能够有效防止攻击者对传感器节点资源的恶意消耗。

### 2.7 自组织性

由于传感器网络是由一组传感器以 Ad Hoc 方式构成的无线网络，它是以自组织的方式进行组网的，这就决定了相应的安全解决方案也应当是自组织的，即在传感器网络配置之前无法假定节点的任何位置信息和网络的拓扑结构，也无法确定某个节点的邻近节点集。

### 2.8 鲁棒性

传感器网络一般配置在恶劣环境、无人区域或敌方阵地中，环境条件、现实威胁和当前任务具有很大的不确定性。这要求传感器节点能够灵活地加入或去除、传感器网络之间能够进行合并或拆分，因而安全解决方案应当具有鲁棒性和自适应性，能够随着应用背景的变化而灵活拓展，来为所有可能的应用环境和条件提供安全解决方案。此外，当某个或某些节点被攻击者控制后，安全解决方案应当限制其影响范围，保证整个网络不会因此而瘫痪或失效。

## 3 无线传感器网络安全的研究进展

传感器网络的研究起步于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，且大多数方案都是基于 Ad Hoc 及传统网络的安全机制，密钥管理体制也并非完全意义上的分布式自组织解决方案，而是分级式的管理方案。因此，在传感器网络还未被模型化和量化之前，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。目前，国际上对于传感器网络安全的研究主要集中在如下几个方面。

### 3.1 密钥管理

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，也包括密钥的行政管理制度和管理人员的素质。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，密钥的泄密将直接导致明文内容的泄漏。

Eschenauer 和 Gligor[5]提出了一种分布式传感器网络中的密钥管理方案。在该方案中，密钥分发包括密钥预分发、共享密钥发现和路径密钥建立三个过程；密钥更新通过基站生成一个简单的密钥撤消指令(包括受攻击节点密钥环上所有的密钥标识符)来完成，该指令使用基站与每个传感器节点共享的密钥加密并进行单播通信，来声明该列表被撤消；密钥更新通过基站重新分配给节点一个密钥环，并再次重新启动邻近节点发现机制和路径密钥建立机制来完成。

Chan[6]等提出一种传感器网络中的随机密钥预分发方案，该方案包括三种安全机制：一是 $q$ 个复合密钥管理方案，它与 Eschenauer 和 Gligor[5]提出的密钥分发方案相似，不同之处是任意传感器节点之间共享的密钥至少是 $q$ 个，而不是一个，以此来减小某个或某些节点被攻击者控制后对传感器网络安全的影响；二是多路径密钥加强方案，即节点 $A$ 选择 $j$ 个随机数 $V_1, V_2, \cdots, V_j$，通过 $j$ 条路径传送给 $B$，节点 $B$ 收到所有的随机数后，通过计算 $K' = K_{AB} \oplus V_1 \oplus V_2 \oplus \cdots \oplus V_j$ 实现对原始共享密钥 $K_{AB}$ 的更新，并将 $K'$ 作为新的共享密钥；三是随机密钥对分发方案，它支持分布式节点撤消，并能有效防止对传感器节点的恶意复制和生成。

Jolly[7]等提出一种节能的密钥管理协议，该协议建立在 IBSK(基于身份标识的对称密钥)方案[8]的基础上。由于假设每个节点只能与簇头或基站进行通信，因而每个传感器节点在密钥预分发时只需存储两个对称密钥，协议支持对于受攻击节点的撤消。该方案采用多层网络体系结构，使得由密钥管理带来的能量消耗大大降低。

Perrig[3]等提出一种传感器网络安全协议 SPINS，它由两个部分构成：SNEP(安全网络加密协议)通过使用计数器和消息认证码来提供数据机密性、通信双方数据认证和数据

新鲜性等基本安全机制，但它不能提供高效的广播认证；μTESLA是TESLA[9]的一种扩展形式，能够提供广播认证。

Satia和Jajodia[10]提出一种局部加密和认证协议LEAP，它是一个传为传感器网络设计的用来支持网内数据处理和密钥管理协议，同时限制受攻击节点对网络中邻近节点的影响。LEAP支持四种类型密钥的建立：与基站共享的主密钥；与其它节点共享的会计密钥；与多个簇内节点共享的簇密钥和与所有传感器网络内节点共享的群密钥。该协议的通信开销和能量消耗都较低，且在密钥建立和更新过程中能够最大限度地减少基站的参与。

Du和Deng[11]提出传感器网络中的一种密钥对预分发方案，它是Blom[12]密钥预分发方案的一种改进形式，主要使用矩阵和连接图的方法实现密钥的分发。该方案能够最大限度地减少受攻击节点对网络中邻近节点的影响。当受攻击节点数目小于门限值时，除受攻击节点外的其它任何节点的受影响概率接近于0。这种理想的特性了和降低了小规模网络的初始开销。

Liu和Ning[13]在基于多项式的密钥预分发方案[14]的基础上，给出了建立密钥对的通用框架，并提出了两个实例：随机子集指派密钥预分发方案和基于栅格的密钥预分发方案，这两种方案具有密钥对建立概率高、通信开销低和允许节点失效等特点。

Wadaa[15]等提出一种可扩密钥管理方案，该方案借助基于位置信息的虚拟网络基础设施来完成密钥管理任务，其主要特征是节点能够动态自主地计算自己基于位置信息的标识符，并使用该标识符来计算群密钥的初始子集；方案的扩展性好，支持大规模传感器网络安全群通信中的密钥建立和管理；协议的通信开销较小，大大节省了能量消耗。

在建立密钥管理方案时，通常假设在网络配置前，与传感器节点分布相关的信息是未知的。Du和Deng[16]指出在许多应用环境中，特定的配置信息是事先可知的，从而提出一种新的运用配置信息的随机密钥预分发方案。该方案避免了不必要的密钥分配，其性能（如连接概率、存储效率和对受害节点影响程度的控制等）都有了显著的改善。

### 3.2 身份认证

由于传感器网络配置环境一般比较恶劣，加之无线网络本身固有的脆弱性，因而极易受到各种各样的攻击。为保证信息的安全传递，需要有一种机制来验证通信各方身份的合法性。在传统的有线网络中，公钥基础设施有效地解决了这个问题，它通过对数字证书的使用和管理，来提供全面的公钥加密和数字签名服务。通过公钥基础设施，可以将公钥与合法拥有者的身份绑定起来，从而建立并维护一个可信的网络环境。非对称加密体制具有很高的计算、通信和存储开销，这决定了在资源受限的传感器上使用数字签名和公钥证书机制是不可行的，必须建立一套综合考虑安全性、效率和性能并进行合理折衷的传感器网络身份认证方案。

Perrig[3]等在μTESLA方案中对TESLA进行了改进，通过引入推迟公布对称密钥的方法来达到非对称加密的效果。该方案解决了先前TESLA存在的认证初始数据包使用数字签名、密钥公开过程能量消耗大和存储单向密钥链开销高等问题，并使计算方法和步骤趋向简化。同时，该方案提供了两种广播流认证方法：节点通过基站广播数据和节点直接广播数据。

Satia和Jajodia[10]在局部加密和认证协议LEAP中指出，由于μTESLA不提供实时认证而导致时延和存储量偏大，因而它不适用于传感器网络中节点与节点之间的数据流认证。该文提出了基于单向密钥链的认证方案，该方案的突出特点是它支持数据源认证、网内数据处理和节点的被动加入，并运用概率型激励方案来有效地检测和阻止传感器网络中的假冒攻击。

Liu和Ning[17]指出，μTESLA认证方案在广播认证消息之前，需要以单播的方式在基站和节点之间分发某些信息，这限制了该方案的可扩展性，尤其是对于大规模的传感器网络。该文通过预先决定并广播初始参数的方式，来取代基于单播的初始信息分发，并进一步研究了几种提高网络性能、鲁棒性和安全性的技术，最终提出的协议具有低开销、容许数据包丢失、可扩展性强和防止重放攻击及拒绝服务攻击等特点。

Bohge和Trappe[18]根据传感器网络中无线设备计算和通信能力的不同，提出了三层分级式传感器网络的认证框架。该框架针对底层传感器节点的资源有限性，提出了使用TESLA证书来进行实体认证。这种认证方法保证了在网络拓扑变化时，对加入节点进行认证并最终建立信任关系。同时，该框架也提供了数据源认证功能，且可以根据节点的计算资源规模分配认证任务，高层节点可以进行数字签名运算。

### 3.3 攻防技术

目前无线传感器网络存在的主要攻击类型包括DoS攻击、Sybil攻击、Sinkhole攻击、Wormhole攻击、Hello泛洪攻击和选择转发攻击。

(1)DoS攻击。许多网络都存在着拒绝服务攻击，传感器网络也不例外。一些传感器网络的配置对于功能强大的攻击者来说是相当脆弱的。DoS攻击是指任何能够削弱或消除传感器网络正常工作能力的行为或事件，硬件失效、软件漏洞、资源耗尽、环境干扰及这些因素之间的相互作用都有可能导致DoS攻击。Wood和Stankovic[19]详细分析了传感器网络物理层、链路层、网络路由层和传输层可能存在的DoS攻击，并给出了相应的对策。

(2)Sybil攻击。Douceur[20]首次给出了Sybil攻击的概念，即在无线网络中，单一节点具有多个身份标识，通过控制系统的大部分节点来削弱冗余备份的作用。同时，提出了一种使用可信证书中心来验证通信实体身份以防止Sybil攻击，这种解决方案显然不适用于传感器网络。Newsome[21]系统分析了Sybil攻击对传感器网络诸多功能（包括路由、资源分配和非法行为检测等）的危害，对Sybil攻击进行了科学的分类，提出了运用无线资源检测来发现Sybil攻击，并使用身份注册和随机密钥分发方案建立节点之间的安全连接等方法来防止Sybil攻击。

(3)Sinkhole攻击。在这种攻击中，攻击者的目标是吸引所有的数据流通过攻击者所控制的节点进行传输，从而形成一个以攻击者为中心的黑洞。Sinkhole攻击通常使用功能强大的处理器来代替受控节点，使其传输功率、通信能力和路由质量大大提高，进而使得通过它路由到基站的可靠性大大提高，以此吸引其它节点选择通过它的路由。对于传感器网络中存在的Sinkhole攻击，目前一般通过对路由协议进行精细设计来进行有效的防止[22]。

(4)Wormhole攻击。在Wormhole攻击中，攻击者将在一部分网络上接收的消息通过低时延的信道进行转发，并在网络内的各族进行重放。Wormhole攻击最为常见的形式是两个相距较远的恶意节点互相勾结，通过使用攻击者拥有的带

外信道中继数据包的方式进行转发。Hu[23]等提出一种检测Wormhole攻击的技术，但该技术要求节点之间必须具备严格的时间同步，从而不适用于传感器网络。同时，Hu等又提出了一种检测和阻止传感器网络中wormhole攻击的方案[24]，该方案使用地理或临时约束条件来限制数据包的最大传输距离，并给出一种新的高效协议TIK来对接收到的数据包进行实时认证。Kwok[25]提出一种由GPS节点和非GPS节点通力协作来防止Rormhole攻击的方法，并对其进行了实现。Hu和Evans[26]则提出使用定向天线的防御方案，设计出一种节点共享方向性信息的合作协议，来防止Wormhole终端冒充邻近节点。

(5)HELLO泛洪攻击。它是一种针对传感器网络的新型攻击，由于许多协议要求节点广播HELLO数据包来发现其邻近节点，收到该包的节点将确信它在发送者的传输范围内，即二者在同一簇内。假如攻击者使用大功率无线设备广播路由或其他信息时，它能够使网络中的部分甚至全部节点确信攻击者就是其邻近节点。这样，攻击就可以与邻近节点建立安全连接，网络中的每个节点都试图使用这条路由与基站进行通信，但由于一部分节点距离攻击者相当远，加上传输能力有限，发送的消息根本不可能被攻击者接收而造成数据包丢失，从而使网络陷入一种混乱状态。最简单的对付HELLO泛洪攻击是通信双方采取有效措施进行相互的身份验证[22]。

(6)选择转发攻击。多跳传感器网络通常是基于参与节点可靠地转发其收到信息这一假设的。在选择转发攻击中，恶意节点可能拒绝转发特定的消息并将其丢弃，以使得这些数据包不再进行任何传播。然而，这种攻击者冒着邻近节点可能发现这条路由失败并寻找新路由的危险。另一种表现形式是攻击者修改节点传送来的数据包，并将其可靠地转发给其它节点，从而降低被人怀疑的程度；解决方案是由节点进行概率否决投票并由基站或簇头对恶意节点进行撤消。多径路由也是地付选择转发攻击比较有效的方法[27]。

## 4 无线传感器网络安全的研究方向

目前，有关传感器网络安全问题的研究还处于起步阶段，由于传感器网络的体系结构和模型还没有最终形成标准，因而无线传感器网络安全研究面临着许多不确定的因素。现有的各种安全解决方案多是在借鉴传统网络特别是无线ad hoc网络安全方案的基础上提出来的，具有一定的局限性。总的来看，传感器网络安全仍然存在着如下尚未解决的实际问题。

(1)入侵检测问题。在传感器网络节点不具有全局唯一身份标识的条件下，恶意节点可能在网络配置前已经存在，并和其它节点一起参与密钥的预分发和建立过程，从而达到窃听和破坏信息的目标。因而，在源认证和数据流认证之前，必须设计相应的方案来确认通信一方不是恶意节点。目前，有些无线传感器安全解决方案假设每个节点具有全网唯一的身份标识，并在此基础上构建身份认证方案，这不符合传感器网络的实际情况。

(2)传感器安全方案和技术方案的有机结合问题。传感器网络由于在电源能量、计算能力、存储空间及通信带宽等方面都非常有限，因而安全解决方案不能设计得太复杂，并尽可能地避开公钥运算，以适应传感器网络资源受限的特点。如何在不显著增加网络开销和的情况下，综合考虑安全性、效率和性能问题，在满足安全性需求的前提下，使性能和效率达到最优，从而构造出理想的传感器网络安全方案，并设计相应的协议和算法，是一个需要进行深入研究的问题。

(3)管理和维护节点的密钥数据库问题。由于传感器网络中节点、簇头和基站之间的通信都需要会话密钥来保证其安全性，因此，每个节点需要维护和保持一个密钥数据库。在节点存储能力有限的条件下，如何依据节点计算、存储和通信能力确定簇的规模和数据库存储密钥的数目，以及如何在密钥建立、密钥更新和密钥撤消等阶段动态地维护和管理数据库，这些都是需要进一步研究的问题。

(4)安全路由问题。现有的传感器网络路由协议对电源消耗和性能指标都进行了优化处理，但很少考虑网络的安全性。由于传感器网络配置的特殊性，加之无线网络本身固有的脆弱性，使其极易受到各种攻击，而传感器网络中的许多类型的攻击需要通过提高路由的安全设计来实现，这就要求在进行路由协议和算法的设计中，必须将网络的安全性作为一种设计目标，分析信任需求，建立威胁模型，确定安全目标。

## 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, Szewczyk R, Wen V, et al. SPINS: security protocols for sensor networks. Journal of Wireless Networks, 2002, 8(5): 521～534

4 Perrig A, Stankovic J, Wagner D. Security in Wireless Sensor Networks. Communications of the ACM, 2004, 47(6): 53～57

5 Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks. In: Proc. of the 9th ACM Conf. on Computer and Communications Security (CCS2002). Washinigton D. C.. ACM Press, Nov. 2002. 41～47

6 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

7 Jolly G, Kuscu M C, Kokate P, Younis M, et al. A low-energy Key Managenment 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

8 Carman D, Kruus P, Matt B. Constraints and approaches for distributed sensor network security: [Technial Report # 00-010]. NAI Labs, September 2000. pages 1～26. Available at: http://download. nai. com/products/media/nai/zip/nailabsreport-00-010-final. zip. D.

9 Perrig A, Canetti R, Tygar J D, et al. The TESLA broadcast Authentication Protocol. Cryptobytes, 2002, 5(2): 2～13

10 Zhu S, Satia S, Jajodia S. LEAP: Effcient Security Mechanisms for Large-Scale Distributed Sensor networks. In: Proc. of ACM Conf. on Computing and communication Security (CCS'2003). Washington: ACM Press, Oct. 2003. 62～72

11 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

12 Blom R. An optimal class of symmetric key generation systems. In: Advances in Cryptology: Proc. of EUROCRYPT 84-A Workshop on the Theory and Application of Cryptographic Techniques. Paris: Springer-Verlag, Volume 209 of Lecture Notes in Computer Science, 1985. 335～338

13 Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. In: Proc. of the 10th AcM Conf. on computer and Communications Security (CCS), Washington: ACM Press, Oct. 2003. 52～61

14 Blundo C, Santis A D, Herzberg A, Kutten S, Vaccaro U, Yung M. Perfectly-secure key distribution for dynamic conferences. In: Advances in Cryptology-CRYPTO'92: 12th Annual Intl. Cryptology conf. Santa Barbara, California, USA: Springer-Verlag, Volume 740 of Lecture Notes in Computer Science, 1993. 471～486

15 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

16 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
17 Liu D, Ning P. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In: Proc. of the 10th Annual Network and Distributed System Security Symposium (NDSS2003). San Diego, California: Internet Society Press, February 2003. 263～276
18 Bohge M, Trappe W. An Authentication framework for Hierarchical Ad Hoc Sensor Networks. In: Proc. of ACM Workshop on Wireless Security (WISE'03). San diego, California, USA: ACM Press, Sep. 2003. 79～87
19 Wood A, Stankovic J. Denial of Service in sensor networks. IEEE Computer, 2002, 35(10): 54～62
20 Douceur J R. The sybil attack. In: Proc. of First International workshop on Peer-to-peer systems (IPTPS'02). Cambridge .MA, USA: Springer-Verlag, Volume 2429 of Lecture Notes in computer Science, 2002. 251～260
21 Newsome J, Shi E, Song D, et al. The Sybil Attack in Sensor Networks Analysis & Defenses. In: Proc. of Third Intl. Symposium on Information Processing in Sensor Natworks (IPSN'04). Berkeley, California, USA: ACM Press, April 2004. 259～268
22 Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and counter-measures. In: First IEEE Intl. Workshop on Sensor Network Protocols and Applications (SNPA 2003). Anchorage, AK, USA: IEEE computer Society, May 2003. 113～127
23 Hu Y C, Perrig A, Johnson D B. Wormhole detection in wireless ad hoc networks: [Technical report TR01-384]. Department of Computer Science, Rice University, June 2002
24 Hu Y-C, Perrig A, Johnson D B. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. In: Proc. of the Twenty-second Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM 2003). San Francisco, CA: IEEE computer Society, 2003, 3: 1976～1986
25 Kwok J. A Wireless Protocol to Prevent Wormhole Attacks. A Thesis in TCC 402 Pressented to the Faculty of the School of Engineering and Applied Science University of Virginia, March 2004. 1～52. Available at: www. sc. virginia. edu/～evans/theses/dwok. pdf
26 Hu L, Evans D. Using Directional Antennas to Prevent Wormhole Attacks. In: Proc. of the 11th Annual Network and Distributed System Security Symposium (NDSS2004). San Diego, Cailfornia: Internet Society Press, Feb. 2004. 144～154
27 Ganesan D, Govindan R, Shenker S, et al. Highly-resilient, energy-efficient multipath routing in woreless sensor networks. Mobile Computing and Communications Review, 2001, 4(5): 1～3

(上接第53页)

链：该信任链以本地策略 POLICY 为根，向下一级一级进行扩展，最后的叶子结点为当前所请求操作的公钥。两种信任链如图3所示。

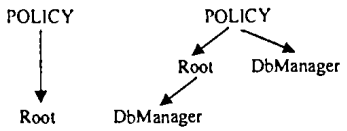


图3 直接信任链与传递信任链

TME 中一致性检测算法的目的就在于要在本地策略库和所搜集的凭证集中找出一条信任链，该信任链以本地策略 POLICY 为根。根据当前所请求操作的凭证或策略的 XML 文档，一致性检测算法提取出其中的 Authorizer 及 Licensees 元素，再根据这些元素的值搜索上一级授权者，一直到最后一级，如果最后一级授权者为关键字 POLICY，则一致性检测成功，向 XML/SNMP 转换网关返回结果允许该操作，否则拒绝该操作请求。具体算法描述如下：

a) 一致性检测算法首先逐一分析所搜集到的凭证集(由 XML/SNMP 转换网关传入)；从每个凭证中解析出如下几个元素：Authorizer，Licensees，operation，Signature，并将这些元素存到一个数组 Trust 里面；

b) 解析完所有凭证之后，分析 Trust 数组，从所请求操作的 Authorizer 所在数组元素开始，验证该元素里的 Signature 域，并逐级往上搜索 Licensees 域与本级 Authorizer 域相同的数组元素，一直到找到 Authorizer 域为 POLICY 为止，在上面搜索的过程中所搜索到的数组元素形成了一条信任链 $t$，如果在搜索过程中所有 Signature 域均合法，最后成功找到 Authorizer 域为 POLICY 的元素，并且信任链 $t$ 上的所有元素的 operation 域均相同，则向 XML/SNMP 转换网关返回同意该请求的结果，然后将该信任链加上成功标记并写入本地信任库；

c) 若上述步骤中任何一步验证不合法或出错，则向 XML/SNMP 转换网关返回出错，拒绝该请求，将该信任链加上失败标记写入本地信任库。

**结束语** 通过分析当前安全管理系统中存在的问题，本文讨论了安全管理系统中引入信任管理的必要性，并在本课题组所提出的基于 XML 的安全管理平台中引入了信任管理机制，提高了安全管理平台自身的安全性。针对基于 XML 的安全管理平台对自身安全的特殊要求，扩展了传统的基于策略的信任模型，加入了本地信任库和双向信任的机制，实现了安全管理平台中客户方与服务方的相互信任，并为下一步信任度评估的研究提供了基础。

信任机制在安全管理中的应用是一个崭新的研究课题，在基于 XML 的安全管理平台的研究中，我们在深入了解了信任管理以及相关领域的研究现状的基础上，做了一些尝试和改进，未来的工作主要集中在以下几个方面：基于历史声誉的信任度模型，改进一致性检测算法；性能测评和改进。

## 参 考 文 献

1 Cisco Secure Policy Manager. http://www. cisco. com/warp/public/cc/pd/sqsw/sqppmn/index. shtml
2 Tivoli http://www-306. ibm. com/software/tivoli/
3 Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management. In: Proc. 17th Symposium on Security and Privacy. Oakland: IEEE, 1996. 164～173
4 Blaze M, Feigenbaum J, Strauss M. Compliance Checking in the PolicyMaker Trust Management System. Financial Cryptography 1998. 254～274
5 徐锋，吕建. Web 安全中的信任管理研究与进展. 软件学报，2002，13(11)：2057～2064
6 徐锋，吕建，等. 一个软件服务协同中的信任管理框架设计. 计算机科学，2003，30(9)：152～154
7 Blaze M, Ioannidis J, Keromytis A D. Experience with the KeyNote Trust Management System: Applications and Future Directions. iTrust 2003. 284～300
8 Blaze M, Feigenbaum J, Keromytis A D. KeyNote: Trust Management for Public-Key Infrastructures. In: Christianson B, Crispo B, William, S, et al. eds. Cambridge 1998 Security Protocols Intl. Workshop. Berlin: Springer-Verglag, 1999. 59～63
9 Blaze M, Feigenbaum J, Ioannidis J, Keromytis A D. The KeyNote Trust Management System Version 2. Internet RFC 2704. http://www. faqs. org/rfcs/rfc2704. html, Sep. 1999
10 Chu Y-, Feigenbaum J, LaMacchia B, Resnick P, Strauss M. REFEREE: Trust Management for Web Applications. World Wide Web Journal, 1997, 2(2): 127～139
11 IBM. IBM Trust Establishment Policy Language. http://www. hrl. il. ibm. com/TrustEstablishment/PolicyLanguage. asp
12 Grandison T, Sloman M. A Survey of Trust in Internet Applications. IEEE Communications Surveys and Tutorials, 2000, 4(4): 2～16