无线传感器网络中的隐私保护研究*)

姚剑波[1,2]　文光俊[1]
(电子科技大学宽带光纤传输与通信网技术教育部重点实验室　成都 610054)[1]
(遵义师范学院　遵义 563002)[2]

摘　要　随着无线传感器网络的广泛应用，安全问题发生变化，通信安全成为重要的一部分，隐私保护日渐重要。首先分析了无线传感器网络的通信安全特点、通信安全的需求、面临的保密性威胁及攻击模型。最后，基于对无线传感器网络隐私保护问题的分析和评述，指出了今后该领域的研究方向。

关键词　无线传感器网络，通信安全，隐私保护，保密性

Research on Privacy Protection for Wireless Sensor Network

YAO Jian-bo[1,2]　WEN Guang-jun[1]
(Key Laboratory of Broadband Optical Fiber Transmission & Communication Networks, Ministry of Education, Chengdu 610054, China)[1]
(Zunyi Normal College, Zunyi 563002, China)[2]

Abstract　As wide applications of wireless sensor networks, security issues change and communication security becomes an important part of security issues. Privacy concerns have become the main obstacle to success when people are participants in wireless sensor networks. Privacy protection becomes more important increasingly. Communication security characteristics, communication security requirements, privacy threats and attack model in wireless sensor networks were analyzed. The development directions were pointed out based on the analysis and remark of privacy protecting problems remaining unsolved in wireless sensor networks.

Keywords　Wireless sensor network(WSN), Communication security, Privacy protection, Privacy

随着无线传感器网络(Wireless Sensor Network, WSN)理论与技术的不断成熟，其应用已经由国防军事领域扩展到环境监测、交通管理、医疗卫生、制造业、反恐抗灾等诸多领域，使人们在任何时间、任何地点和任何环境条件下都能够获得大量详实可靠的信息，真正实现"无处不在的计算"理念。

WSN 是一种大规模的分布式网络，常部署于无人维护、条件恶劣的环境当中，且大多数情况下传感节点都是一次性使用，从而决定了传感节点是价格低廉、资源极度受限的无线通信设备。在复杂的安全环境、多样的安全需求和资源限制等因素的综合影响下，WSN 的安全受到严峻的挑战。为 WSN 创造一个相对安全的工作环境，是关系到 WSN 能否真正走向实用的关键性问题。另外，在 WSN 中，安全的概念也发生了变化，通信安全是其中重要的一部分，隐私保护日渐重要[1]。

1　无线传感器网络的通信安全特点

通信安全保证 WSN 内数据采集、融合、传输等基本功能的正常进行，是面向网络基础设施的安全性。在 WSN 中，通信安全具有如下特性[1-5]：

(1)最小的资源消耗和最大的安全性能是一对矛盾，所以在解决 WSN 的安全问题时，必须考虑如下 5 个方面的限制：

1) 有限的能量

传感节点通常由电池供电，电池的容量一般不会很大。由于长期工作在无人值守的环境中，通常无法给传感节点充电或更换电池。

2) 有限的存储空间

传感节点一般包括三种形式的存储器，即 RAM、程序存储器、工作存储器。RAM 用于存放工作时的临时数据，一般不超过 2kB；程序存储器用于存储操作系统、应用程序以及安全函数等，工作存储器用于存放获取的传感信息，这两种存储器一般也只有几十 kB。

3) 有限的计算能力

传感节点 CPU 一般只具有 8bit，4MHz～8MHz 的处理能力。

4) 有限的通信带宽

由于无线信道本身的物理特性，它所能提供的网络带宽相对有线信道要低得多。WSN 中传输的数据大部分是经过节点处理过的数据，因此流量较小。根据目前观察到的现象特性来看，传感数据所需的带宽将会很低(1～100 kbit/s)。

5) 有限的通信距离

WSN 是利用"多跳"来实现低功耗下的数据传输，因此其设计的通信覆盖范围只有几十米。

(2)对一个单独的数据包来说，采取安全机制，需要增加的额外开销相对较小，而大量的开销花费在密钥分配上。

(3)WSN 在空间上的开放性，使得攻击者很容易进行窃听、截取、篡改、重放数据包。

(4)由于传感节点靠电池供电，因此 WSN 在资源消耗型攻击面前显得很脆弱，攻击者连续地发送数据包会消耗节点

*)基金项目：国家"973"计划基金资助项目(2007CB307100)。**姚剑波**　博士，研究方向为网络信息安全；**文光俊**　教授，博士生导师，主要从事通信与信息系统研究。

的电池能量，并浪费大量网络带宽。

(5)由于传感节点部署区域的特殊性，攻击者可以对节点本身进行破坏或破解。

(6)WSN是以数据通讯为中心的，相邻的节点可能采集到相同或者相近的数据。如果每个节点都发送数据包给基站，就会浪费珍贵的能量和带宽，为此，无线传感器网络需要进行数据融合，这就要求中间节点能够访问数据包的内容，在这种情况下，使用传统的端到端的安全机制是不合适的。

2 无线传感器网络的通信安全需求

WSN起源于军事应用领域，主要采用射频无线通信组网。由于网络中资源严格受限，为使有限的资源发挥最大的安全效益，要求具有如下通信安全需求[4,5]：

(1)节点的安全保证

传感节点是构成WSN的基本单元，节点的安全性包括节点不易被发现和节点不易被篡改。WSN中普通传感器节点的数量众多，少数节点被破坏不会对网络造成太大的影响。但敌手如果俘获节点，就可能从中读出密钥、程序等机密信息，甚至可以重写存储器将该节点变成一个“卧底”。为防止为敌所用，要求节点具备抗篡改能力。

(2)被动抵御入侵的能力

WSN安全系统的基本要求是：在局部发生入侵的情况下，保证网络的整体可用性。

1)对抗外部攻击者的能力：外部攻击者是指那些没有得到密钥、无法接入网络的节点。外部攻击者无法有效地注入虚假信息，但是可以进行窃听、干扰、分析通信量等活动，为进一步攻击收集信息。因此，对抗外部攻击者，首先需要解决机密性问题；其次，要防范能扰乱网络正常运转的简单网络攻击，如重放数据包等，这些攻击会造成网络性能下降；再次，要尽量减少入侵者得到密钥的机会，防止外部攻击者演变成内部攻击者。

2)对抗内部攻击者的能力：内部攻击者是指那些获得了相关密钥并以合法身份混入网络并发布欺骗信息的攻击节点。由于WSN不可能阻止节点被篡改，而且密钥可能被对方破解，因此总会有入侵者在取得密钥后以合法身份接入网络。由于至少能取得网络中一部分节点的信任，因此内部攻击者能发动的网络攻击种类更多，危害更大，也更隐蔽。

(3)主动反击入侵的能力

主动反击能力是指网络安全系统能够主动地限制甚至消灭入侵者，为此至少需要具备以下能力：

1)入侵检测能力：和传统的网络入侵检测相似，首先需要准确识别网络内出现的各种入侵行为并发出警报，其次，入侵检测系统还必须确定入侵节点的身份或者位置，只有这样才能随后发动有效反击。

2)隔离入侵者的能力：网络需要具有根据入侵检测信息，调度网络正常通信来避开入侵者，同时，丢弃任何由入侵者发出的数据包的能力。这样相当于把入侵者和己方网络从逻辑上隔离开来，可以防止它继续危害网络。

3)消灭入侵者的能力：要想彻底消除入侵者对网络的危害就必须消灭入侵节点。但是让网络自主消灭入侵者是较难实现的。由于WSN的主要用途是为用户收集信息，因此可以在网络提供的入侵信息的引导下，由用户通过人工方式消灭入侵者。

3 保密性威胁

借助WSN，很容易收集个人信息。有的机构将个人信息当作商品，进行收集、交换和出售。人们对这些行为越来越警觉，希望保护自己的隐私[6]。

在诸如战场等特定情形下，保密性是一本质特性。有三种类型的保密性威胁[7]：

(1)内容保密性威胁：因为消息的存在和所处位置的顺序关系，敌手能够确定信息交换的含义，这就存在内容保密性威胁。

(2)身份保密性威胁：如果敌手能够演绎出参与通信的节点，那就存在身份保密性威胁。

(3)位置保密性威胁：如果敌手能够推断出通信实体的物理位置或估计出相对通信实体的距离，那就存在位置保密性威胁。

WSN以收集信息为主要目的，通过有效地安置微小的传感节点，使自动获取数据的能力增加。敌手可以通过窃听、加入伪造的非法节点等方式获取敏感信息。随着WSN的广泛使用，保密性问题日益严重。如果敌手知道怎样关联传感器节点的多个输入，就能利用甚至表面无关的数据去获得有效信息。保密性问题的关键在于：并不是没有WSN就不能获取信息，但WSN加剧了保密性问题，因为通过远程访问，WSN使大量的信息容易使用，因此敌手不必亲临现场就能以低风险、匿名的方式获得信息。远程访问还允许一个敌手同时监听多个场所[8,9]。

4 保密性攻击模型

在WSN中，针对保密性的攻击有如下几种[9-11]：

(1)窃听：这是对保密性最明显的攻击。借助窃听到的数据，敌手容易发现通信内容，通信量携带着传感器网络配置的控制信息；通信量包含的信息潜在地比通过特定服务器获得的信息更详细，窃听有效地突破了隐私保护。

(2)通信量分析：通信量分析与窃听明显结合在一起。在某些节点间传送信息包数目的增加将揭示特定传感器的合法行为。通过通信量分析，具有特殊角色或行为的节点将被有效识别。

(3)插入虚假数据：恶意节点通过受骗的传感器节点，欺骗系统减小数据失真。

(4)改变路由行为：为了获取信息，敌手把非法节点或被俘节点隐藏在WSN中，在非法节点或被俘节点伪装成为正常节点后，诱惑信息包，不正确地转发它们，甚至对所有的节点宣称自己是最好的路径。

5 隐私保护研究进展

WSN中的隐私保护研究起步于2003年，根据WSN潜在的保密性威胁和攻击，国际上对于WSN中的隐私保护作了如下几个方面的研究。

5.1 信息加密

现代安全技术依靠密钥来保护和确认信息，而不是依靠安全算法，所以通信加密密钥、认证密钥和各种安全启动密钥需要严格的保护[5]。对传输信息加密可以解决窃听问题，但需要一个灵活、强健的密钥交换和管理方案。由于WSN资源严格受限，使得非对称密码的许多算法，如Diffie-Hellman密钥协商算法无法在WSN上实现。根据共享密钥节点的个

数，可以把 WSN 中的密钥管理方法分为对密钥管理方案和组密钥管理方案。

5.1.1 对密钥管理方案

对密钥管理的一般方式是密钥预分配，即在传感器安置前把密钥存储进传感器。在安置后，每个传感器利用存储的密钥与其邻居建立秘密链路。密钥连通性，传感器节点与其邻居节点共享一个密钥的概率，是对密钥管理方案中要考虑的一个重要因数。

(1)预置全局密钥[12]：所有的传感器节点预配置一个相同的全局密钥。在安置之后，每对传感节点利用全局密钥获得一个新的对密钥。这个方案的抗俘获性低，任意一个节点被俘，将导致整个网络被俘。

(2)预置对密钥[13]：每个传感节点都存储 $N-1$(N 为网络节点总数)个对密钥。其中一个对密钥仅由该节点和其余 $N-1$ 个节点中的一个节点共享。这个方法具有好的抗俘获性，但却不实用，因为传感节点的存储资源受限且网络规模非常大，没有可扩展性。在网络安置之后，不能接受新节点加入，因为已安置节点没有新节点的密钥。

(3)随机密钥预分配[14]：基本的随机密钥预分配方案是由 Eschenauer 和 Gligor 首先提出的。

在密钥预分配阶段，每个传感节点从一个大的密钥池 K 中随机选择一个子集 k；在共享密钥发现阶段，两个节点在它们的子集中找到一个共享密钥作为通信密钥。两个传感节点间共享一个密钥的概率 p 为

$$\frac{((K-k)!)^2}{(K-2k)!\ K!}$$

在路径密钥建立阶段，通过在路径 $i,v_1,\cdots,v_n,j$ 上依次发送 $E_{K_{i,v_1}}(K_{i,j})$，$E_{K_{v_1,v_2}}(K_{i,j})$，$\cdots$，$E_{K_{v_n,j}}(K_{i,j})$，任何一对节点能安全地建立一个对密钥 $K_{i,j}$。

Chan 等人对随机密钥预分配方案进行了改进[15]：每个节点存储一个 $(N-1)p(0<p<1)$ 个对密钥的随机集。因为两个节点连接的概率是 p，那么密钥的连通性是 p。所需存储的密钥减少，但保留了好的抗俘获性。

(4)基于位置的密钥预分配方案：基于位置的密钥预分配方案是对随机密钥预分配方法的改进。它假定每个传感节点都有一个可预知的期望位置，每个节点都预装 c 个最接近邻居的对密钥。这个方案所用的存储空间少，且连通性好[16]。

Du 等人把传感节点分为 $t\times n$ 组，按高斯分布把传感器安置在每个组内。在保持好的抗俘获性时，密钥连通性得到改进[17]。

(5)其它方法：还有一些基于其它技术的密钥预分配方案。Camtept 和 Yener 的基于分块设计的方案[18]。Du 等人的方案是每对节点计算密钥矩阵的通信域并用作对密钥[19]。Liu 等人的方案利用每对节点 (i,j) 的标识对称多项式 $P(x,y)$($P(x,y)=P(y,x)$)赋值得到对密钥 $K_{i,j}=P(i,j)$[20]。

5.1.2 组密钥管理方案

组密钥管理方案主要用于层次化的 WSN：

(1)对称组密钥管理：在每个节点给对称多变量多项式 $P(x_1,\cdots,x_t)$ 赋值，t 个节点间能产生一个对称密钥[21]。

(2)非对称组密钥管理：每个传感节点预装载 ECC(elliptic curve cryptography)域参数，在安置之后，每个节点计算 EC 公钥/私钥对，然后广播公钥给同一簇内的所有节点。ECC 的计算复杂性低于 DSA/RSA 密码系统，但高于对称密码系统[22]。

5.2 匿名机制

在 WSN 中，匿名阻止第三方了解参与通信的消息发送方和接收方的特性。匿名包括发送方和接收方间的发送方匿名、接收方匿名和无链接能力。通过匿名，敌手不能通过读从网络中截获的消息或从被俘传感节点转发来的消息确定发送和接收方的特性；也不能断定两个通信段是否属于同一通信。匿名机制使数据在传送前失去个性。因为全部匿名是困难的，所以在解决保密性问题时，需要在匿名和公用信息需求间作一平衡[11,23]。

(1)分散敏感数据：限制网络所发送信息的粒度，因为信息越详细，越有可能泄露隐私，比如，一个簇节点可以通过对从相邻节点接收到的大量信息进行汇集处理，并只传送处理结果，从而达到数据匿名化[11]。

(2)安全通信信道：使用安全通信协议(如使用 SPINS 协议[24])能预防窃听、插入虚假数据、改变路由行为等攻击[11]。

(3)改变数据通信量：以不固定的方式传送数据可以预防通信流量分析[11]。

(4)节点机动性：使传感节点移动能有效地防御位置保密性威胁[25]。

(5)传感节点使用假名：传感节点匿名使敌手弄不清哪一个节点是消息的真正发送者。为了保护每个节点的真正标识(ID)，用假名代替传感节点真正的标识(ID)[26,27]。

(6)使用匿名协议：Wadaa 等人提出了一种能量有效的协议，维持对等系统、簇结构、路由结构等网络虚拟设施的匿名[28]。

5.3 基于对策的方法

保证网络中的传感信息只有可信实体才可以访问，这可通过建立在保密性对策规范基础上的访问控制决议和认证来实现[3,29]。

(1)根据不同的密钥给数据以不同的保密级[30]。

(2)弱化节点的异构性，增加重要节点的冗余度。一旦系统的关键节点被破坏，通过选举机制或网络重组方式进行网络重构[31-33]。

(3)使用输出过滤(egress filtering)。通过认证冤路由的方式确认一个数据包是否是从它的合法子节点发送过来的，直接丢弃不能认证的数据包。这样攻击的数据包在前几级的节点转发过程中就会被丢弃，从而达到保护目标节点的目的[34]。

(4)多路径路由，通过多个路径传输部分信息，并在目的地进行重组[25,35,36]。

5.4 信息洪泛

伪装实际数据通信流量，使敌手难于通过分析网络流量去追踪数据源[7,36]。

(1)基线洪泛：当一个消息到达中间节点时，节点首先检查是否已经收到并转发过该消息。如果没有，节点就把该消息广播给自己的所有邻居节点，否则就抛弃该消息。

(2)概率洪泛：在概率洪泛中，整个网络仅有部分节点参与数据转发，其余节点简单地抛弃它们收到的消息。

(3)带有欺骗信息的洪泛：基线洪泛和概率洪泛仅能减小违反保密性的机会。敌手仍然有机会监听通常的通信量，甚至单独的信息包。为了降低违背保密性的风险，增强洪泛协议，从而引入虚假信息源，在网络中注入欺骗消息。即使敌手俘获信息包，也无法确定是否是真正的信息包。

(4)幻影洪泛：在幻影洪泛中，每个消息都经历两个阶段，

首先是步移阶段，可以是随机步或定向步；随后是洪泛阶段，把消息分发到接收节点。

5.5 贪婪随机步

信源节点和接收节点都减少随机步。接收节点首先初始化一个 N 跳随机步，随后信源节点初始化一个 M 跳的随机步。一旦源信息包到达这两条路径的交点，就通过由接收节点建立的路径转发。局部广播用于检测路径的交点。为了最小化沿随机步反向追踪的机会，在节点中存储一个活力过滤器(bloom filter)过滤步进。在每一阶段，活力过滤器检查中间节点，确保最小化反向追踪[37]。

5.6 循环诱骗

传感器网络安置后，在信源发送消息给基站之前，产生几个环路，每个环路包含几个传感节点。当消息沿着从源到基站的路径转发并与预配置的环路相遇时，激活环路，开始沿环路循环欺骗消息。当攻击节点到达这点时，不能区分消息，只能随机选择节点进行下一跳。通过增加消息所经路径上的环路，就能增加敌手查找信源节点所需的期望时间[38]。

6 隐私保护研究方向

目前，有关无线传感器网络隐私保护问题的研究才刚刚起步，虽然做了一些初步探索，但方法还不成熟。发现和探索保密性威胁存在的地方，观察和开发解决隐私保护问题的方法是重要的。

(1)现有的预置密钥管理方案可扩展性不强，而且不支持网络合并。如何在资源受限的网络环境下，建立支持网络合并，且具有灵活的可扩展性的预置密钥管理方案是一个需要进行深入研究的问题。

(2)从安全的角度来看，非对称密码体制的安全强度在计算意义上要远远高于对称密码体制。如何优化非对称加密算法，使之适用于资源受限的无线传感器网络，任然是一个需要进一步研究的问题。

(3)仅用加密的方法不能保护系统的隐私。在事件驱动型传感器网络中，传感节点只有在监测到事件时，才发送消息。敌手使用相应频段的接收设备就可以接收链路中的信号，进行窃听。敌手不必知道原始消息的具体内容，仅凭观察到消息的存在就断定监测事件出现了。在传统网络中，可以用周期性地发送空闲包的方法来隐藏真正的消息包，但在传感器网络中，由于传感节点资源严格受限，采用这样的方法来保护隐私是行不通的。在这种情形下，如何隐藏传感信号是一个需要研究的问题。

(4)传感器网络是以数据为中心的网络，通过在网络内聚合多个传感数据，可以减少通信次数、降低通信能耗，从而延长网络的生存期。如何在确保传感数据正常聚合的情形下，实现隐私保护，特别是网络中存在恶意节点的情况下，如何保护隐私是一个值得进一步研究的问题。

(5)在传感器网络中，位置资源隐私保护是一个重要问题，现有的网络路由，如洪泛、随机步以及循环诱骗等都不成熟。开发适合于资源受限的无线传感器网络的位置资源隐私保护网络路由是十分必要的。

参 考 文 献

[1] 周贤伟，覃伯平，徐福华. 无线传感器网络与安全. 北京：国防工业出版社，2007

[2] 曾志峰，邱慧敏，朱龙海. 无线传感器网络中的安全威胁分析及对策. 计算机应用研究，2007，24(1)：140-143

[3] 戴宁江，邱慧敏. 无线传感器网络的安全问题及对策. 中国无线电，2006(10)：47-50

[4] 于海斌，曾鹏，梁韦华. 智能无线传感器网络系统. 北京：科学出版社，2006

[5] 王殊，阎敏杰，胡富平，等. 无线传感器网络的理论及应用. 北京：北京航空航天大学出版社，2007

[6] Whitman M E，Mattord H J. 信息安全原理(第2版). 齐立博，译. 北京：清华大学出版社，2006

[7] Ozturk C，Zhang Y，Trappe W，et al. Source-location privacy for networks of energy-constrained sensor // Proceedings of 2nd IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems(WSTFEUS'04). May 2004

[8] 骆盈盈，李春芳. 传感器网络中的安全性和保密性. 计算机工程与设计，2006，27(7)：1277-1278

[9] Chan H，Perrig A. Security and privacy in sensor networks. IEEE Computer Magazine，2003：103-105

[10] Perrig A，Stankovic J，Wagner D. Security in wireless sensor networks. Commun. ACM，2004，47(6)：53-57

[11] Gruteser M，Schell G，Jain A，et al. Privacy - aware location sensor networks // 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS). 2003

[12] Lai B，Kim S，Verbauwhede I. Scalable session key construction protocol for wireless sensor networks // IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES). Austin，Texas，December 2002

[13] Sanchez D，Baldus H. Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks // Proc. of the First International Conference on Security and Privacy for Emerging Areas in Communication Networks. 2005：277-288

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

[15] Chan H，Perrig A，Song D. Random Key Pre - distribution Schemes for Sensor Networks // Proc. of the IEEE Security and Privacy Symposim 2003. 2003

[16] Liu D，Ning P. Location-based pairwise key establishment for static sensor networks // 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. 2003

[17] Du W，Deng J，Han Y，et al. A key management scheme for wireless sensor networks using deployment knowledge // IEEE Infocom04. 2004

[18] Camtepe S A，Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks // 9th European Symposium on Research Computer Security. 2004

[19] Du W，Deng J，Han Y，et al. A pairwise key pre-distribution scheme for wireless sensor networks // Proceedings of the 10th ACM Conference on Computer and Communications Security CCS03. 2003

[20] Liu D，Ning P. Establishing pairwise keys in distributed sensor networks // 10th ACM Conference on Computer and Communications Security CCS03. 2003

[21] Blundo C，Santis A，Herzberg A，et al. Perfectly-secure key distribution for dynamic conferences // Crypto 92. 1992

[22] Mahimkar A，Rappaport T S. SecureDAV：A Secure Data Aggregation and Verification Protocol for Sensor Networks // Pro-

(下转第 112 页)

Smart 协议及本文两个协议的通信性能和计算复杂度见表 1。可信第三方协议通信占用的带宽与 Smart 方案相同，协议执行时比 Smart 方案多 4 次椭圆曲线上的标量乘法运算，但无需点的加法运算，整体性能与 Smart 相差无几；无第三方协议占用的带宽和点乘运算比 Smart 协议多，但协议运行无需第三方密钥分发和托管开销。

表 1　新的协议与 Smart 协议的性能分析

	通信量(二进制位)	计算量(操作数)
Smart 协议	4L	2M+2A+2P
协议 1	4L	6M+2P
协议 2	6L	6M+2A+2P

结束语　本文在分析密钥协商协议的安全属性和 Smart 方案的基础上，提出了两个新的协议：一个基于可信第三方实现公钥分发，通信双方利用私钥完成身份认证与密钥协商；另一个无需第三方支持，结合 CDH 和 BDH 问题给出简洁有效的安全协商模型。两个协议都隐含认证，且在实体身份点映射安全可控的应用环境中，可抵抗中间人攻击。

随着 IBE 公钥体制的发展，基于 ID 的双线性配对密钥协商协议研究越来越受关注。下一步的研究将继续关注对开放网络环境下各类新攻击的抵抗问题，并展开双线性对协议的性能优化研究。

参 考 文 献

[1] Wilson S B, Johnson D, Menenes A. Key Agreement Protocols and their Security Analysis// The 6th IMA International Conference on Cryptography and Coding. LNCS Vol. 1355. Springer-Verlage, 1997: 30-45

[2] Diffie W, Hellman M E. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22: 644-654

[3] LiC K, Chen qun. Identity Based Authenticated Key Agreement Protocols from Pairings. Hewlett-Packard Laboratories, Bristol, 2002

[4] 冯姚刚. 基于 Weil 对的成对密钥协商协议. 软件学报, 2006, 17

[5] Shamir A. Identity based cryptosystems and signature schemes// Lecture Notes in Computer Science. 1984, 196: 47-53

[6] Dan Boneh M F. Identity-Based Encryption from the Weil Pairing// The Proceedings of Crypto. Springer-Verlag, 2001, 2139: 213-229

[7] Smart N P. An identity based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 2002, 38: 630-632

[8] Li S, Yuan Q. A New Efficient ID-Based Authenticated Key Agreement Protocol. School of Mathematical Sciences. Peking University, Beijing: 2005

[9] Ryu E, Yoon E, Yoo K. An Efficient ID-Based Authenticated Key Agreement Protocol// Networking 2004. 2004, 3042

[10] Wang Y. IEEE 1363.3 Submission: Implicitly Authenticated ID-Based Key Agreement Protocol. UNC Charlotte

[11] Divya Nalla K C R. ID-based tripartite Authenticated Key Agreement Protocols from pairings. Dept of Computer/Info. Sciences. University of Hyderabad, Hyderabad

[12] Chien H Y. Improved ID-based Tripartite Multiple Key Agreement Protocol from Pairings. Department of Information Management, ChaoYang University of Technology, 2004

[13] Colin B, Anish M. Protocols for Authentication and Key Establishment. ISBN 3-540-43107-1. Berlin, Springer-Verlag, New York, Heidelberg, 2003

(上接第 22 页)

ceedings of IEEE Global Telecommunications Conference (Globecom) 2004. Dallas, TX, USA, Nov. 2004

[23] Gruteser M, Grunwald D. A methodological assessment of location privacy risks in wireless hotspot networks// First International Conference on Security in Pervasive Computing. 2003

[24] Perrig A, Szewczyk R, Wen V, et al. SPINS: Security Protocols for Sensor Networks// Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking. ACM Press, 2001: 189-199

[25] Deng J, Han R, Mishra S. Countermeasures against traffic analysis attacks in wireless sensor networks// Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). Washington, DC, USA: IEEE Computer Society, 2005: 113-126

[26] Misra S, Xue G. Efficient anonymity schemes for clustered wireless sensor networks. International Journal of Sensor Networks, 2006, 1(1/2): 50-63

[27] Ouyang Y, Le Z, Xu Y, et al. Providing anonymity in wireless sensor networks// 10th International Conference on Parallel and Distributed Systems (ICPADS 2004)

[28] Wadaa A, Olariu S, Wilson L, et al. On providing anonymity in wireless sensor networks// 10th International Conference on Parallel and Distributed Systems (ICPADS 2004). Newport Beach, CA, USA, 2004: 411-418

[29] Molnar D, Wagner D. Privacy and security in library rfid: Issues, practices, and architectures// ACM CCS. 2004

[30] Shao M, Zhu S, Zhang W, et al. pDCS: Security and Privacy Support for Data-Centric Sensor Networks// IEEE INFOCOM 2007

[31] Girao J, Westhoff D, Schneider M. CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks// 40th International Conference on Communications. IEEE ICC, May 2005

[32] Castelluccia C, Mykletun E, Tsudik G. Efficient Aggregation of Encrypted Data in Wireless Sensor Networks. Mobiquitous, 2005

[33] He W, Liu X, Nguyen H, et al. PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks// 26th Annual IEEE Conference on Computer Communications IEEE INFOCOM 2007. Anchorage, Alaska, May 2007

[34] Wood A D, Stankovic J A. Denial of Service in Sensor Networks [J]. IEEE Computer, 2002, 35 (10): 54-62

[35] Carbunar B, Yu Y, Shi L, et al. Query privacy in wireless sensor networks// Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conferenc. June 2007: 203-212

[36] Deng J, Han R, Mishra S. INSENS: Intrusion-tolerant Routing in Wireless Sensor Network Security[R]. Tech. Rep. CU-CS-939-02. Department of Computer Science, University of Colorado, November 2002

[37] Xi Y, Schwiebert L, Shi W. Preserving privacy in monitoring-based wireless sensor networks// Proceedings of the 2nd International Morkshop on Security in Systems and Networks (SSN'06). IEEE Computer Society, 2006

[38] Ouyang Y, Le X, Chen G, et al. Entrapping adversaries for source protection in sensor networks// World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006. International Symposium, June 2006: 10