



专题：物联网技术与应用

可信物联网架构模型

殷安生¹, 张世君²

(1. 南京邮电大学, 江苏 南京 210003;

2. 中国电信股份有限公司连云港分公司, 江苏 南京 210037)

摘要: 物联网已经在世界范围内得到了广泛的关注和发展, 其安全性也面临严重威胁。然而由于物联网本身的特性, 很多在互联网领域的安全措施不能直接照搬过来。目前的安全策略主要是针对物联网受到的威胁逐一寻找解决方案, 协同机制分散。面对日益智能化、系统化、综合化的安全威胁, 提出一种三元两层的可信物联网架构, 根据物联网的功能设计一种全程可信安全机制, 从传感器设备的软件及硬件的完整性和安全性检查开始, 将可信链依次传递, 直到应用层, 并在应用层根据行为可信实现数据的处理和应用。同时将控制功能和数据功能分开, 不同的安全策略之间相互协作、相互检验, 从而有效提高物联网应对安全威胁的能力。

关键词: 物联网; 可信; 架构

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017270

A trusted IoT architecture model

YIN Ansheng¹, ZHANG Shijun²

1. Nanjing University of Posts and Telecommunications, Nanjing 210003, China

2. Lianyungang Branch of China Telecom Co., Ltd., Nanjing 210037, China

Abstract: The internet of things (IoT) has been widely concerned and developed in the world, and its security has been paid more and more attention. However, due to the characteristics of the IoT itself, a lot of security measures in the internet field can't be applied directly. The current security strategy mainly provide solutions according to the threat of the IoT one by one. In face of increasingly intelligent, systematic, integrated security threats, a trusted IoT architecture of two layers and tri-elements, which brought about a whole trusted security mechanism according to the function of IoT. Starting with the integrity and safety inspection of hardware and software of sensor devices, the trusted chain was transmitted until the application layer, and data was processed according to behavior trusted value in application layer. At the same time, the control function and the data function were separated, and the security strategies cooperated and verified with each other, therefore improving the ability of the IoT to deal with security threats effectively.

Key words: internet of things, trusted, architecture

收稿日期: 2017-08-20; 修回日期: 2017-09-22

基金项目: 江苏省教育厅高校自然科学研究面上项目 (No.17KJB520026)

Foundation Item: Natural Science Fund for Colleges and Universities in Jiangsu Province (No.17KJB520026)

1 引言

物联网 (internet of things, IoT) 主要是各种信息传感设备结合互联网产生的网络, 遍及智能家居、工业控制、物流监测、公共安全以及定位监测等众多领域。由于覆盖的领域广、接入设备器件海量、应用的多样性和复杂性, 使得物联网时代的安全问题变得更加严峻。Gartner 在安全报告中预测, 到 2020 年, 针对企业的安全性攻击 (经确认) 中, 有 25% 以上将涉及物联网。由于物联网直接与物理世界交互, 获取人及其周围环境的相关信息, 若出现安全威胁, 还会涉及生命财产损失^[1]。美国 McAfee 公司的信息安全专家 Barnabe 及其团队曾利用强大的无线电设备成功干扰了胰岛素泵的正常工作和控制了胰岛素泵的注射频率。360 公司安全团队攻破特斯拉 Model S 汽车的漏洞, 成功地远程控制了汽车。

《“十三五”国家信息化规划》在物联网发展的具体行动指南明确指出, 要注重信息安全保护。提出加强数据资源在采集、传输、存储、使用和开放等环节的安全保护, 推进数据加解密、脱密、备份与恢复、审计、销毁、完整性验证等数据安

全技术研发及应用。

物联网安全是一个贯穿全产业链环节的系统工程, 且攻击方式呈现出智能化、系统化、综合化趋势。仅仅从硬件或者软件又或者网络传输单一层面进行检测、管理与安全防护, 都很难从根本上杜绝安全隐患, 为了弥补当前分散、孤立、单一防御、外在附加的网络安全系统缺陷, 本文提出了一种可信物联网架构, 该架构实现物联网的全程可信, 以达到终端状态可监测、异常数据可评估、恶意行为可控制的目的。

2 可信物联网架构

现有的物联网安全措施多是根据物联网所面临的安全威胁分别制定相应的应对方法, 没有从系统架构上设定目标和策略, 甚至会因为某种安全技术手段带来新的问题。特别是与计算机网络相比, 物联网增加了感知层, 由于不依赖固定基础设施, 资源、电源局限性等特点, 相对于传统的网络, 物联网更易受到各种安全威胁和攻击, 包括窃听、数据篡改和重发、伪造身份和拒绝服务等。根据物联网的分层结构, 物联网所面临的安全威胁如图 1 所示, 其中, 处理层主要是利用

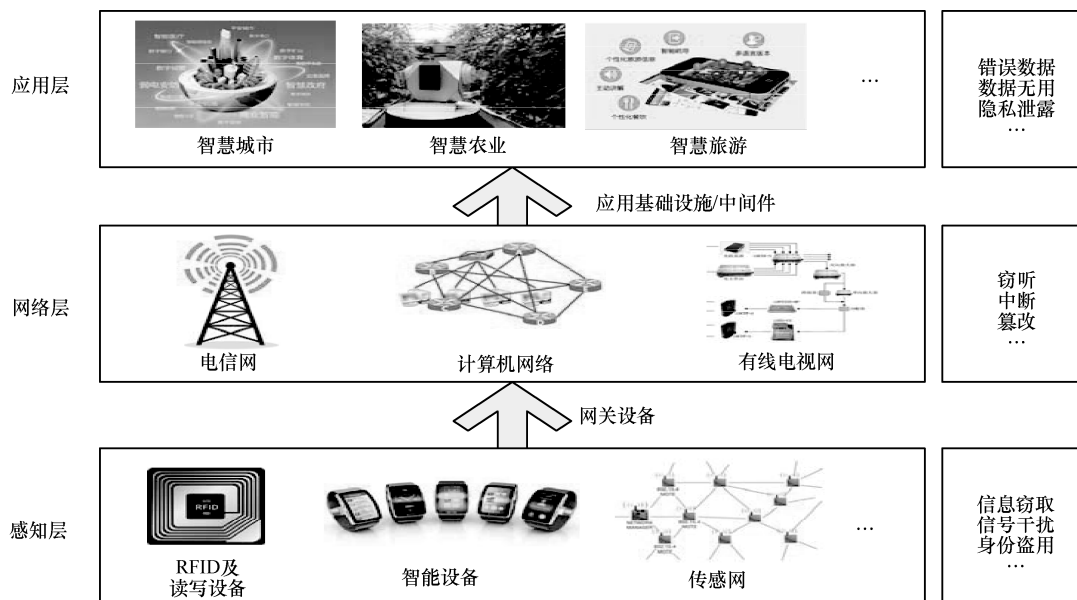


图1 物联网架构及安全威胁



云计算和大数据方法处理数据，其安全威胁和应对方法相对闭环且与当前网络中的安全威胁相同，因此本文不再讨论。

感知层是物联网不同于其他网络的重要组成部分,然而由于感知层的存在,物联网更加不安全。Weber^[2]指出物联网安全体系需针对物联网感知节点易遭攻击、计算资源受限导致无法利用高复杂度的加解密算法保证自身安全等物联网安全所面临的特殊问题展开研究。如图 1 所示,传感器设备和 RFID 设备与计算机网络中的终端在计算能力、防护能力方面都存在显著差别,特别是引入移动节点后带来的安全和认证问题更加复杂,现有移动节点的研究工作较多关注节点的数据收集和生存周期^[3],但是在密钥协商^[4]、漫游认证^[5]等方面都存在很多问题,因此提出了利用漫游证明信息完成匿名认证^[6]、可信无线匿名认证协议^[7]、移动可信匿名漫游协议^[8,9]等。RFID 由于置于公共空间甚至无人看管,其面临的安全威胁更加急切,包括数据泄露、信号干扰、设备劫持等。因此有包括静电屏蔽^[10]、更改频率、Sleep 标签等物理方法^[11]来确保 RFID 设备安全,也有学者利用节点的移动性和相互协作方法探测节点是否被俘获^[12]。目前针对 RFID 的安全协议主要有随机 Hash Lock 协议、LCAP 等^[13],用于数据加密的密钥生成协议^[14]以及密钥分配算法^[15]。密钥管理和认证方式主要采用以互联网为核心的集中管理方式和以各自异构网络为中心的分布式管理方式两种^[16]。

在传输层的安全主要涉及路由协议、链路的窃听、阻断、篡改等。应用层的安全威胁主要有信息泄露、数据篡改、用户隐私泄露、越权访问、信息抵赖等。Medaglia^[17]指出物联网在用户隐私和信息安全传输机制中存在诸多不足。物联网的数据隐私安全保护包括隐私同态技术^[18]、信息隐藏技术^[19]以及使用安全多方计算解决蜂窝网中位置隐私^[20]等。

物联网所面临的安全威胁多层、多维、多样化,且日趋智能化、系统化、综合化,当前分散孤立的网络安全措施疲于奔命,甚至相互掣肘。为此本文提出一种三元两层可信物联网架构模型,如图2所示。

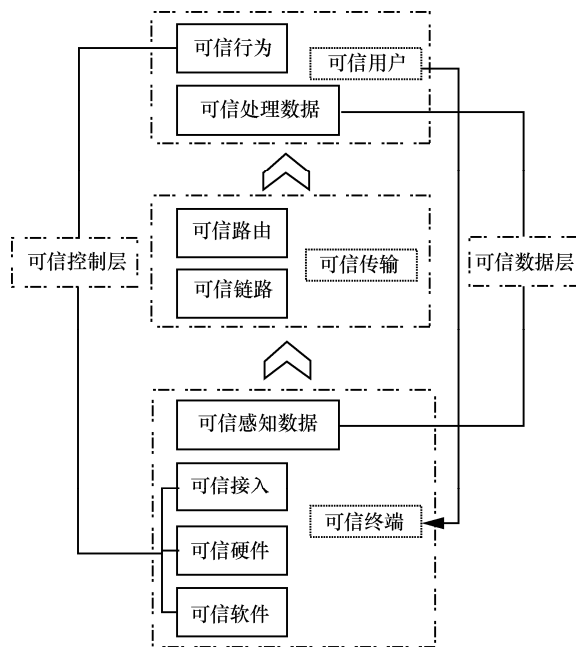


图 2 可信物联网架构模型

三元指的是可信终端、可信传输和可信用户，与物联网的三层结构相对应；两层指的是可信控制层和可信数据层。两层架构主要是从可信的角度进行区分，在可信控制层，首先对底层的软硬件设备进行完整性和安全性检查，符合安全标准的设备才可以接入网络，然后通过可信链传递的方法依次规范传感器设备或智能终端的行为，使得其行为符合预期。可信数据层包括可信感知数据和可信处理数据。可信感知数据是指在感知层的设备能按照系统的意愿来获取数据，并且获取的是真实的数据；可信处理数据指的是可信感知数据在经过可信传输到达可信处理层之后，进行预处理和加工之后送往应用层，应用层获取的数据是感知层真实情况的反映。

各层安全策略之间是相互联系、相互协作的, 例如感知层的安全策略可能没有发现传感器节点

或 RFID 设备采集了错误的数据,但是通过在应用层的技术手段可以发现终端的数据是否可信,从而发现或减弱恶意节点的危害,同时检验底层的安全手段是否有效。

下文分别从可信终端、可信传输和可信用户分别介绍可信物联网的安全威胁及应对措施。在三元两层物联网架构中,安全策略和指导思想在各层之间是相似和贯通的。

2.1 可信终端

可信终端包括可信软硬件和可信接入。其中,可信软硬件是以硬件附着的可信组件执行平台完整性和安全性检测,如可信移动模块(mobile trusted module, MTM)。可信组件的功能分为两个阶段实现:第一阶段是验证终端的可信度,第二个阶段是在验证终端可信度的基础上继续验证终端行为的可信度。在第一阶段主要完成完整性和安全性检查,终端设备在加电启动时检查处理器、存储器等设备是否完整,同时检查 RFID 设备、智能终端、WSN 等从加电开始的启动过程是否符合规定程序,包括读取的数据和启动的程序是否符合流程。第二阶段在确保终端设备软硬件的完整性和安全性之后,继续检测设备接入网络后的行为,建立一条从 BIOS 开始的信任链,从启动引导到操作系统再到应用,一级验证一级,将信任关系延续下去并扩展到应用的边界。

在执行可信接入时一个很重要的工作就是密钥协商和认证。目前的认证主要是读卡器设备与后台之间有认证加密过程,而读卡器与 RFID 设备之间的信道没有加密认证,信道并不安全,因此需要通过双向认证实现信道加密及 RFID 设备辨识,由于设备的性能决定了只能使用轻量化的认证协议。LEAP (lightweight extensible authentication protocol) [21]是由 Cisco 公司设计的轻量级认证协议,Watro 等人 [22]提出了基于低指数级 RSA 的 TinyPK 实体认证方案,然而在 TinyPK 中,如果某个认证节点被捕获了,那么整个网络都将变得不安全,

Hsieh 等人 [23]提出的强用户认证协议可以在一定程度上解决这个问题。

由于传感器设备本身的续航及计算能力有限,安全机制缺乏,其安全威胁主要来自于设备劫持或者通信信道泄密,设备被劫持后可重新读写设备的内容,并通过获取标签中的信息访问后台数据库,目前一般采用物理方法 [11]或密码机制的方法确保 RFID 设备的安全。由于物理方法需要硬件支持或需要改变硬件的状态,因此密码机制被认为是解决设备安全的重要途径。有很多轻量级密码方案,如分组密码 PRESENT [24]、Clefia [25]、在 DES 的基础上进行轻量化设计的轻量级密码 [26,27]、基于流密码算法 Trivium 设计的 KATAN&KTANTAN [28]以及 LBlock [29]等。然而这类密码没有经过深入的安全分析和大规模的测试验证,例如 KATAN&KTANTAN 密码在发表后不到两年就被破译。

RFID 安全协议有 Hash Lock 协议、随机化 Hash Lock 协议、Hash 链协议、基于杂凑的 ID 变化协议、分布式 RFID 询问—响应认证协议、LCAP、再次加密机制等 [13]。轻量级的加密方法只能用于物流和零售等环境,而高强度的加密算法例如 DES、3DES,包括公钥加密方法 RSA 和 ECC 等都需要较多的运算能力和资源消耗,因此只适用于金融、军事和安全等领域,由于 Hash Lock 协议、Hash 链协议对资源的消耗在可控范围内,被认为是适用于物联网领域、切实可行的认证手段。然而 Hash Lock 协议和 Hash 链协议要求 RFID 设备的 ID 是固定的,这会带来设备可追踪的安全风险,可能造成用户隐私泄露,可以通过增加伪随机数的方式增加一个动态 ID,通过这个动态 ID 交互信息,提高设备的匿名性。

不同于 RFID 设备,智能终端设备的运行能力和续航能力有极大提高,如果只采用轻量化安全协议,并不能保证其安全性,可以通过预知共享密钥的方式进行,但对于大范围的感知环境如



智慧社区等则并不适用。终端设备在安全启动之后就开始从周围的环境或者输入下接收数据。此时的安全风险主要有接收到错误的数据和接收的数据被窃取破坏。很多时候 WSN 为自组织网络，没有中心化节点，这使得设计安全架构设计变得困难，特别是认证协议、密钥分发等。区块链利用 Merkle Hash 树进行比对以及验证处理，在分布式环境下进行比对或验证时，Merkle 树会大大减少数据的传输量以及计算的复杂度。因此可以在感知层利用 Merkle Hash 树结构存储关键信息，例如将 WSN 节点间的认证和加密信息 Hash 之后作为叶子节点，这样所有的节点都可以相互验证，同时节点的加入和退出机制也更为灵活，在验证了 Hash 值之后只要更改相应分叉的 Hash 值就可以了，不需要重新生成一棵新的 Hash 树。Hash 值存储在终端的可信组件中，因此通过根 Hash 值和其自身的密钥 Hash 值可以实现终端的可信身份识别。可信身份识别和终端的可信行为评估相互合作，确保终端感知数据的可信性。

2.2 可信传输

物联网的网络层主要通过各种网络基础设施和协议，将感知层的数据传输到应用层的数据处理中心或者客户端应用软件，并不是一种全新的网络传输设施，主要由电信网、计算机网络、有线电视网等现有的网络提供支撑。随着三网融合的推进，网络层将向全 IP 化推进。物联网在网络层的安全威胁如同目前 IP 所面临的安全威胁一样，包括传输过程中的数据丢失、数据截取和数据篡改等。在物联网中，数据的产生地点和接收地址、数据的传输时间、吞吐量、传输协议相对稳定甚至有规律可循，因此其面临的安全威胁比 IP 网络更甚，很多传感器网络部署下去之后基本不再移动，即使如车联网，虽然车载单元(on board unit, OBU)会随车辆一直移动，但路边单元(road side unit, RSU)和中心可信机构(trusted authority, TA)却基本固定。

目前传感器网络中的路由协议都相对简单、易受攻击，即使加入容侵策略、安全等级策略，多径路由，设置广播半径等安全策略也不能保证物联网网络层的安全。计算机网络可以采用认证和加密协议来保证传输数据的安全性，特别是一些敏感数据还使用强加密协议，包括一次一密等，然而认证加密协议会带来终端的存储和计算负担，而物联网中很多传感器节点存储容量小，电量低，计算能力有限。物联网传输路径相对稳定，信息发送甚至有规律可循，信息被完全获取的概率增大，其信息被破解的概率也会随之增大。为保证敏感信息的安全性，同时不过分消耗传感器节点的能量，本文提出一种基于网络编码的数据传输方式来发送、接收数据，同感知层中保存关键信息的 Merkle 树类似，节点在收到数据之后进行编码再发往下游节点，只是编码的方式不一定是 Hash 操作。

传统路由式的传输方式是将收到的原始数据块直接转发给下游节点，与传统的路由相比，网络编码的传输方式是将收到的数据块编码后转发给下游节点，通过网络编码将从上游来的数据信息进行混合，然后再通过不同的路径转发出去，这样下游的节点必须要收集足够的信息才能恢复原始数据，通过多路径转发提高恶意节点获取全部信息的难度，同时编码的数据都是从上游收到的部分数据块的混合，因此也增加了信息破解的难度。利用网络编码，节点不需要确定发送哪个具体的数据块给下游节点，而是将所有数据块进行线性组合再发送给下游，减少了由于调度带来的开销。编码生成的数据块包含该节点所有数据块的信息。当收到足够多编码过的数据块后，节点就可以根据编码矢量恢复原始的数据块。相对于加密认证协议，网络编码方式改变了原先传输路径和吞吐量相对固定的问题，同时通过数据块的线性组合和轻量化的编码方案，实现物联网节点计算负担和安全性的平衡。

在可信传输层,还可以根据用户的可信度来选择路径和编码方式^[30],用户的可信度有用户身份可信和用户行为可信。

2.3 可信用户

物联网应用层的核心功能围绕着数据和应用两个方面来进行。而无论是应用还是数据,都是来源于用户同时都需要面向用户,这也是物联网的目的所在。因此用户的不规范或恶意行为就成为了应用层安全的主要威胁。

2.3.1 节点可信评估

在物联网应用层的可信度量主要有用户行为可信和用户身份可信。用户身份可信是指用户的身份通过认证、鉴别等手段确保访问控制有授权、访问过程有记录、恶意行为可追溯。用户行为可信主要通过节点可信度来衡量,节点的信任度是节点物理信息和行为信息的综合。物理信息包括电池容量、发射信号功率、节点负载、传输效率等,用户的行为信息是指通过用户的历史行为分析获取的,在分析敏感用户或者用户的敏感数据时,根据用户在一段时间内的行为数据,利用行为分析模型、多属性决策模型或者特征匹配模型进行可信评估,得出用户的可信度,并以此可信度来判断用户数据的可信度或者对用户的行为进行授权。在计算用户可信度时,对影响用户可信的多属性一般通过加权模型进行区别对待,同时需要考虑行为的连续性和阶段性。

不同于互联网中的终端用户行为的多样性,物联网当中感知终端主要用于数据的采集和获取,并按照一定的协议将数据传输到云平台,因此不能简单地评估物联网终端的历史行为。本文提出一种基于波动性和一致性的节点数据可信度判决方法来表示终端行为可信度^[31]。将终端收集的数据分为横向和纵向两个维度,横向指的是其他终端和该终端同时采集和接收数据,纵向指的是该终端在某时间段内收集数据。在横向比较时,其他终端例如邻近终端和该终端所采集的数据应

该有相关性或相近性;在纵向比较时,一段时间内该终端所收集的数据应该服从该时间段内整体数据的特性,若该终端收集的数据不符合特性,则该终端收集的数据不可信的程度较大。

通过对节点数据和行为的分析,可以得到终端的可信度。节点的可信度可以直接作用于终端部署,如 sink 节点选取、认证协议等,并可用于感知层数据检验。同时还可以应用于可信传输、可信路由策略选择。在访问控制时,用户行为可信可以作为用户身份可信的重要补充。

2.3.2 隐私保护

在应用层的用户可信还表现在对隐私的保护。由于感知层的存在,物联网会不断收集大量的个体隐私信息,如车联网当中汽车行驶路线、智慧医疗设施中采集的用户健康状况、工业物联网当中的企业产品信息等^[32]。

物联网的隐私保护主要有基于群签名的认证方案、基于假名的认证方案等的密码学技术^[33]以及基于属性加密的安全健康信息共享策略^[34]、基于属性加密的访问控制算法^[35]等的非密码学技术两种。

用户隐私保护分为数据隐私保护和位置隐私保护。在位置隐私保护方面,通过采用部分标识符和 ID 动态更新的方法提出了一种隐私相互认证协议^[36],利用等长度的伪随机函数实现 RFID 系统匿名认证协议^[37]等。安全多方计算 (secure multiparty computation, SMC) 也是物联网隐私保护中重要的安全技术之一。Ien^[38]分析了位置隐私以及 2G/3G 系统的身份隐私问题,提出使用安全多方计算解决蜂窝网中位置隐私的方案。

在数据隐私保护方面。信息隐藏技术的出现和发展,为物联网隐私保护尤其是多媒体数据的保护提供了一种新的思路,目前所采用的信息隐藏技术主要有隐写术、数字水印技术、可视密码技术等,可以通过隐写术隐藏物联网匿名通信系统中用户身份关系的资料^[19]。由于传感器节点计



算能力差,因此可以将存储和计算开销较大的运算放到云平台上执行,然而云平台 and 链路的保密性又带来了新的问题,在充分考虑节点资源受限和数据隐私泄露安全威胁的情况下,参考文献[39]对于大规模数据流提出了一种新的信息隐藏方法。由于用户还需要对物联网数据进行检索,因此物联网搜索引擎导致的数据隐私问题也变得突出。为此提出了加密搜索方案来确保物联网搜索服务提供者无法对后台系统中的数据进行窥探,有基于对称密钥的密文搜索(searchable symmetric encryption, SSE)方案^[40]和基于非对称密钥的密文搜索(public encryption keyword search, PEKS)方案^[41],还有基于属性加密(attribute based encryption, ABE)^[42]的访问控制来确保物联网搜索服务不被滥用以及通过隐藏随机访问模式(oblivious random access machine, ORAM)技术^[43]隐藏用户访问模式来避免深度数据隐私挖掘。

可以利用上文得到的用户可信度来进行访问控制,对不同可信度的用户分别开放不同的权限。用户的可信度可以根据领域、兴趣、知识范围进行划分,再在不同的域内进行细粒度的动态授权。

3 结束语

物联网的发展非常迅速,市场潜力巨大。物联网的信息安全问题是关系物联网产业能否安全可持续发展的核心问题之一,必须引起高度重视。本文从物联网的分层功能出发,提出一种三元两层可信物联网架构模型。从传感器设备开始,通过可信链传递将终端的可信度延伸到网络中,一级验证一级,从而实现数据和终端的全程可信。可信物联网的目的是要达到终端状态可监测、异常数据可评估、恶意行为可控制。全程可信机制能够做到行为可审计、可追溯,更适合于可信物联网架构,只是需要对用户数据保障更加关注,以避免隐私泄露。

在可信控制层,利用 Merkle Hash 树模型存储

感知层重要信息,在无中心化网络中处理节点的认证和加密,在传输层利用这种树型结构对传输的数据进行编码,实现数据的加密。同时在应用层,评估用户和用户数据的可信度,根据用户的可信度开放应用和访问数据的权限给用户。根据用户数据的可信度检验可信感知数据的真实程度,既是对感知层安全策略的补充,也是对底层安全协议的验证。

参考文献:

- [1] STANKOVIC J A. Research directions for the internet of things[J]. *Internet of Things Journal IEEE*, 2014, 1(1): 3-9.
- [2] WEBER R H. Internet of things-new security and privacy challenges[J]. *Computer Law & Security Review*, 2010, 26(1): 23-30.
- [3] VUPPUTURI S, RACHURI K K, MURTHY C S R. Using mobile data collectors to improve network lifetime of wireless sensor networks with reliability constraints[J]. *Journal of Parallel & Distributed Computing*, 2010, 70(7): 767-778.
- [4] ZHANG J, LI X, MA J, et al. Secure and efficient authentication scheme for mobile sink in WSNs based on bilinear pairings[J]. *International Journal of Distributed Sensor Networks*, 2014(1): 84-88.
- [5] 王良民, 姜顺荣, 郭渊博. 物联网中移动 Sensor 节点漫游的组合安全认证协议[J]. *中国科学: 信息科学*, 2012, 42(7): 815-830.
WANG L M, JIANG S R, GUO Y B. Composable-secure authentication protocol for mobile sensors roaming in the internet of things[J]. *Scientia Sinica*, 2012, 42(7): 815-830.
- [6] 周彦伟, 杨波. 物联网移动节点直接匿名漫游认证协议[J]. *软件学报*, 2015, 26(9): 2436-2450.
ZHOU Y W, YANG B. Provable secure authentication protocol with direct anonymity for mobile nodes roaming service in Internet of things[J]. *Journal of Software*, 2015, 26(9): 2436-2450.
- [7] CHEN T H. A robust mutual authentication protocol for wireless sensor networks[J]. *Etri Journal*, 2010, 32(5): 704-712.
- [8] 杨力, 马建峰, 朱建明. 可信的匿名无线认证协议[J]. *通信学报*, 2009, 30(9): 29-35.
YANG L, MA J F, ZHU J M. Trusted and anonymous authentication scheme for wireless networks[J]. *Journal on Communications*, 2009, 30(9): 29-35.
- [9] 周彦伟, 杨波, 张文政. 可证安全的移动互联网可信匿名漫游协议[J]. *计算机学报*, 2015, 38(4): 733-748.
ZHOU Y W, YANG B, ZHANG W Z. Provable secure trusted and anonymous roaming protocol for mobile internet[J]. *Chinese Journal of Computers*, 2015, 38(4): 733-748.

- [10] SARMA S E, WEIS S A, ENGELS D W. Radio-frequency identification: secure risks and challenges[J]. *RSA Laboratories Cryptography*, 2003, 6(1): 2-9.
- [11] KORKMAZ E, USTUNDAG A. Standards, security & privacy issues about radio frequency identification (RFID)[C]//2007 1st Annual RFID Eurasia, Sept 5-6, 2007, Istanbul, Turkey. New Jersey: IEEE Press, 2007: 1-10.
- [12] CONTI M, PIETRO R D, MANCINI L V, et al. Mobility and cooperation to thwart node capture attacks in MANETs[J]. *EURASIP Journal on Wireless Communications and Networking*, 2009(1): 8.
- [13] SAVRY O, VACHERAND F. Security and privacy protection of contactless devices[M]. Berlin: Springer, 2009.
- [14] WANDER A S, GURA N, EBERLE H, et al. Energy analysis of public-key cryptography for wireless sensor networks[C]//IEEE International Conference on Pervasive Computing and Communications, March 8-12, 2005, Kauai Island, HI, USA. New Jersey: IEEE Press, 2005: 324-328.
- [15] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[C]//ACM Conference on Computer and Communications Security, November 18-22, 2002, Washington, DC, USA. [S.l.:s.n.], 2002: 41-47.
- [16] WANG K, BAO J, WU M, et al. Research on security management for internet of things[C]//International Conference on Computer Application and System Modeling, Oct 22-24, 2010, Taiyuan, China. New Jersey: IEEE Press, 2010.
- [17] MEDAGLIA C M, SERBANATI A. An overview of privacy and security issues in the internet of things[M]. Berlin: Springer, 2010: 389-395.
- [18] DOMINGO-FERRER J. A provably secure additive and multiplicative privacy homomorphism[C]//Information Security, International Conference, ISC 2002, September 30-October 2, 2002, Sao Paulo, Brazil. New York: ACM Press, 2002: 471-483.
- [19] The 12th information hiding conference[EB/OL]. (2010-06-30) [2017-08-20]. <https://ih2010.cpsc.ualgary.ca/>.
- [20] CONTI M, ZHANG L, ROY S, et al. Privacy-preserving robust data aggregation in wireless sensor networks[J]. *Security & Communication Networks*, 2009, 2(2): 195-213.
- [21] Cisco lightweight extensible authentication protocol[EB/OL]. (2015-12-13)[2017-08-20]. http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-series/prod_qas0900aecd801764f1.html.
- [22] WATRO R, KONG D, CUTI S F, et al. TinyPK: securing sensor networks with public key technology[C]//The 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, October 25, 2004, Washington DC, USA. New York: ACM Press, 2004: 59-64.
- [23] HSIEH W B, LEU J S. A robust user authentication scheme using dynamic identity in wireless sensor networks[J]. *Wireless Personal Communications*, 2014, 77(2): 979-989.
- [24] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: an ultra-lightweight block cipher[J]. *Lecture Notes in Computer Science*, 2007(4727): 450-466.
- [25] SHIRAI T, SHIBUTANI K, AKISHITA T, et al. The 128-bit blockcipher CLEFIA[C]//The 14th International Conference on Fast Software Encryption, March 26-28, 2007, Luxembourg. New York: ACM Press, 2007: 181-195.
- [26] ISO. Information technology-security techniques-lightweight cryptography-part 2: block ciphers[S/OL]. (2012-01-31)[2017-08-20]. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552.
- [27] LEANDER G, PAAR C, POSCHMANN A, et al. New lightweight DES variants[C]//14th International Conference on Fast Software Encryption, March 26-28, 2007, Luxembourg. New York: ACM Press, 2007: 196-210.
- [28] CANNIÈRE C D, DUNKELMAN O, KNEŽEVIĆ M. KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers[M]. Berlin: Springer Berlin Heidelberg, 2009: 272-288.
- [29] BELLOVIN S M, GENNARO R, KEROMYTIS A, et al. Applied cryptography and network security[M]. Berlin: Springer Berlin Heidelberg, 2012.
- [30] 殷安生, 张顺颐. 基于终端可信度的路由策略设计与实现[J]. *电信科学*, 2016, 32(4): 1-8.
YIN A S, ZHANG S Y. Design and implementation of routing strategy based on terminal trust[J]. *Telecommunications Science*, 2016, 32(4): 1-8.
- [31] 殷安生, 张顺颐. 基于可信群划分及评估值波动性和一致性的可信评估模型[J]. *南京邮电大学学报: 自然科学版*, 2014, 34(3): 101-105.
YIN A S, ZHANG S Y. A trust model based on volatility and consistency in trusted groups[J]. *Journal of Nanjing University of Posts and Telecommunications*, 2014, 34(3): 101-105.
- [32] SATHISHKUMAR J, R. PATEL D. A survey on internet of things: security and privacy issues[J]. *International Journal of Computer Applications*, 2014, 90(11): 20-26.
- [33] 丁洁, 吴汉炜, 林志阳, 等. 增强型匿名 RFID 双向认证协议 eARAP 的设计与分析[J]. *广西大学学报: 自然科学版*, 2015, 40(6): 1494-1500.
DING J, WU H W, LIN Z Y, et al. Design and analysis of an enhanced anonymous mutual RFID authentication protocol eARAP[J]. *Journal of Guangxi University(Nat Sci Ed)*, 2015, 40(6): 1494-1500.
- [34] HAO Y, CHENG Y, REN K. Distributed key management with protection against rsu compromise in group signature based VANETs[C]//2008 Global Telecommunications Conference, Nov 30-Dec 4, New Orleans, LO, USA. New Jersey: IEEE Press, 2009: 1-5.
- [35] HE D, ZEADALLY S, XU B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehi-

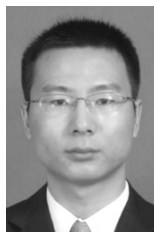


- cular Ad Hoc networks[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(12): 2681-2691.
- [36] IBRAIMI L, ASIM M, PETKOVIC M. Secure management of personal health records by applying attribute-based encryption[C]//International Workshop on Wearable MICRO and Nano Technologies for Personalized Health, June 24-26, 2009, Oslo, Norway. New Jersey: IEEE Press, 2009: 71-74.
- [37] SAHAI A, WATERS B. Fuzzy identity-based encryption[M]. Berlin: Springer, 2005: 457-473.
- [38] IEN G M, OLESHCHUK V A. Location privacy for cellular systems; analysis and solution[C]//5th International Conference on Privacy Enhancing Technologies, May 30-June 1, 2005, Cavtat, Croatia. New York: ACM Press, 2005: 40-58.
- [39] XIAO X, SUN X, YANG L, et al. Secure data transmission of wireless sensor network based on information hiding[C]//International Conference on Mobile and Ubiquitous Systems: Networking & Services, Aug 6-10, 2007, Philadelphia, PA, USA. New Jersey: IEEE Press, 2007: 1-6.
- [40] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable symmetric encryption: Improved definitions and efficient constructions[C]//The 13th ACM Conference on Computer and Communications Security (CCS 2006), October 30-November 3, 2006, Alexandria, Virginia, USA. New York: ACM Press, 2006: 79-88.
- [41] KERSCHBAUM F, SORNIOTTI A. Searchable encryption for outsourced data analytics[C]//The 7th European Conference on Public Key Infrastructures, Services and Applications (EuroPKI'10), September 23-24, 2010, Athens, Greece. New York: ACM Press, 2010: 61-76.
- [42] SAHAI A, WATERS B. Fuzzy identity based encryption[C]//24th Annual International Conference on Theory and Applications of Cryptographic Techniques, May 22-26, 2005, Aarhus, Denmark. New York: ACM Press, 2005: 674-651.
- [43] GOLDBREICH O, OSTROVSKY R. Software protection and simulation on oblivious RAMs[J]. Journal of the ACM (JACM), 1996, 43(3): 431-473.

[作者简介]



殷安生（1982-），男，博士，南京邮电大学副研究员，主要研究方向为网络安全与评估。



张世君（1980-），男，中国电信股份有限公司连云港分公司网络操作维护中心主任、工程师，主要研究方向为电信大数据挖掘与应用。