计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
47(Suppl.): 327-332, 2010

一种面向3G接入的物联网安全架构

孙玉砚 刘卓华 李 强 孙利民
(中国科学院软件研究所 北京 100190)
(信息安全国家重点实验室 北京 100049)
(yuyan@is.iscas.ac.cn)

A Security Framework for Internet of Things Based on 3G Access

Sun Yuyan, Liu Zhuohua, Li Qiang, and Sun Limin
(*Institute of Software, Chinese Academy of Sciences, Beijing* 100190)
(*State Key Laboratory of Information Security, Beijing* 100049)

Abstract With the development of Internet of Things, different wireless communication technologies and network infrastructure are continuously integrated, including wireless sensor networks, RFID systems, Mobile vehicle network, 3G technology, wireless metropolitan area network (WIMAX), local area network, etc. As Internet of things network has expanded rapidly and its communication network environment has become more complex, the security issues are more complex than the existing network systems. This paper analyzes the properties of various components of network system security issues in Internet of things, including the mobile communication network security technology, wireless sensor network security technology. Through the analyzing the existing structure and security for Internet of things, this paper discusses the 3G network and wireless sensor network security, then proposes a network security framework that is to adapt to the future Internet of things based on the 3G, and finally gaives details for the achieved Internet of things safety demonstration system based on the 3G.

Key words things network; security framework; 3G communication network; wireless sensor networks

摘 要 物联网正处于全面发展阶段,无线传感器网络、RFID网络、3G通信网络等各种不同网络结构与无线通信技术不断融合,物联网网络规模迅速扩大,物联网环境变得越来越复杂,物联网内实体间的信任关系、安全通信及安全体系等安全问题将比现有网络系统更加复杂和难以解决.简要介绍物联网的系统结构和基本的安全需求,重点介绍了已有的3G接入和前端无线传感器网络安全研究,提出了一种面向3G接入的物联网安全架构,最后详细介绍了已实现的面向3G接入的物联网安全验证系统,包括系统组成和安全协议.

关键词 物联网;安全架构;3G通信网络;无线传感器网络

中图法分类号 TP393

1998年MIT的Ashton首次提及"Internet of things"概念[1],将RFID技术与传感器技术应用于日常物品中将会创建"物联网",这项技术将带来人们对机器理解的新纪元.2005年ITU发表报告

收稿日期:2010-09-08
基金项目:国家"八六三"高技术研究发展计划基金项目(2009AA11Z209);国家科技重大专项基金项目(2009ZX03006-001-01);中国科学院课题(YYYJ-1013);北京市自然科学基金项目(4092011)

"Internet of things"[2],物联网是通过 RFID 和智能计算等技术实现全世界设备互连的网络,从轮胎到牙刷,所有的物品都在物联网的通信范围内,开启了一个新的网络通信时代. 2008 年欧委会的 CERP-IOT 工程给出最新的物联网定义[3],物联网是物理和数字世界融合的网络,每个物理实体都有一个数字的身份;物体具有上下文感知能力—他们可以感知、沟通与互动. 他们对待物理事件进行即时反映,对物理实体的信息进行即时传送,使得实时做出决定成为可能出决定成为可能. 按照 Wikipedia(网络维基百科全书)的定义[4],"物联网"(Internet of things)是把传感器装备到电网、铁路、桥梁、隧道、公路、建筑、供水系统、大坝、油气管道以及家用电器等各种真实物体上,通过互联网联接起来,进而运行特定的程序,达到远程控制或者实现物与物的直接通信.

随着物联网的全面发展,各种不同无线通信技术与网络结构不断融合,包括无线传感器网络[5]、RFID 网络、移动车载网络、手机网络、3G 通信网络、WiMAX 通信网络及有线宽带等,通信网络环境变得越来越复杂,其承载各类业务的基础网络安全性问题将比现有网络系统更加复杂和难以解决. 物联网的安全是一项巨大的系统工程,一方面,网络安全体系是在通信系统架构确立之后产生的,多种复杂异构的通信系统会由于自身特性对整体安全问题带来影响. 因此物联网内实体间的信任关系、前端无线接入的认证和安全通信、安全业务及安全体系的扩展成为重要的研究热点.

物联网实现虚拟世界与物理世界的互联互通,不仅涉及信息安全,还包括国家安全、公共安全、知识产权保护、个人隐私等. 如果这些安全问题得不到解决,物联网的应用将存在很大的风险,而这些安全问题不能简单地通过网络安全的解决方案予以解决. 在物联网安全的技术方案中,除涉及到网络安全的部分外,还会涉及到许多传统网络安全技术(包括安全程度加强的一些技术)很难解决的问题,如终端安全问题、隐私保护问题、无线传感器网络节点防伪问题等. 如何在物联网通信系统中保证业务信息的安全性和信息空间、物理空间资源使用的安全性,已成为物联网系统中重要而迫切的问题.

1 物联网安全

物联网的体系结构是一个能够兼容各种异构系统和分布式资源的开放式体系结构,可以满足最大化互操作性的需求. 这些分布式资源包括软件、设备、智能物品和人类自身等的信息和服务. 标准的体系结构应该包括明确的抽象数据模型、接口和协议,并与其他的技术进行绑定(如 Web 服务等),共同支持各种操作系统和编程语言. 像互联网一样,物联网的体系结构也应该对物理网络的损坏具有抗毁能力并能够预测节点的移动,允许间歇性的接入,同时还需要满足路由、存贮、事件检索等功能需求,提供有效的缓存、设备预配置、查询请求、软件更新和数据流的同步等机制. 此外,物联网的底层节点应该能够动态自组织的形成 M2M 网络,这需要物联网的体系结构中安全架构支持节点设备间的认证机制和通信安全机制.

按照物联网的各组成元素的功能,欧盟发展框架 7 的 Coordination and Support Action for Global RFID-related Activities and Standardization (CASAGRAS)工作组给出一个四层物联网体系结构,包括了感知层、传输层、处理层和应用层. 图 1 给出了物联网体系结构一般形式的描述物联网中数亿计的设备接入,海量的数据信息、大量异构网络的存在使物联网的安全体系架构面临着更加艰巨的挑战. 物联网的商业安全和个人隐私是值得关注的 2 个主要问题. 因为物联网部署的可扩展性、移动性和复杂性,使得对物品的访问很难有效地控制. 同时物联网中用户也很难保证隐私信息不被泄露. 更具有挑战性的是,许多隐私信息可能是认证过程必须的,比如设备的身份信息、位置信息等,这就给隐私信息的保护带来很大困难. 另外终端的移动性和资源受限特征,使得物联网中时常出现无持续连接的情景,因此需要设计更加灵活的密钥更新机制和高效节能的加密算法,以保障物联网复杂情景下的数据安全性. 因此本文重点考虑 3G 移动通信网络和前端无线接入的安全,为了防止非授权用户对隐私信息的访问和保障授权 3G 用户的合理接入前端无线传感器网络,需要对物联网安全架构展开研究. 目前 3G 接入的物联网安全研究主要分为两方面,一方面是 3G 移动通信网络的接入安全技术,另一方面是前端的无线传感器网络安全技术.

第三代移动通信系统 3G 打破了传统意义上通信网络与互联网之间的物理隔膜,极大地提升了无线接入的能力,实现了多种应用服务. 3GPP 和 3GPP2 专门成立了安全小组制定了对 3G 系统的安全原理和目标、安全威胁和要求、安全体系结构,密

码算法要求以及网络域安全等方面的框架规范.针对第二代移动通信系统 GSM 的安全缺陷,3G 加强了以下安全保护:在身份认证方面,采用双向身份认证,不仅有网络对用户的认证,还有用户对网络的认证;在数据加密方面,加密算法经过公开评估,密钥长度增加,采用高强度的加密算法和完整性算法以及更优的密钥产生分发算法,提高了加密信息的破解难度,增加了信令完整性保护机制,可以抵御攻击者窃听、修改和数据重放攻击等;在核心网安全方面,主要保证核心网络实体间安全交换数据,包括网络实体间身份认证、数据加密、消息认证,以及对欺骗信息的收集.

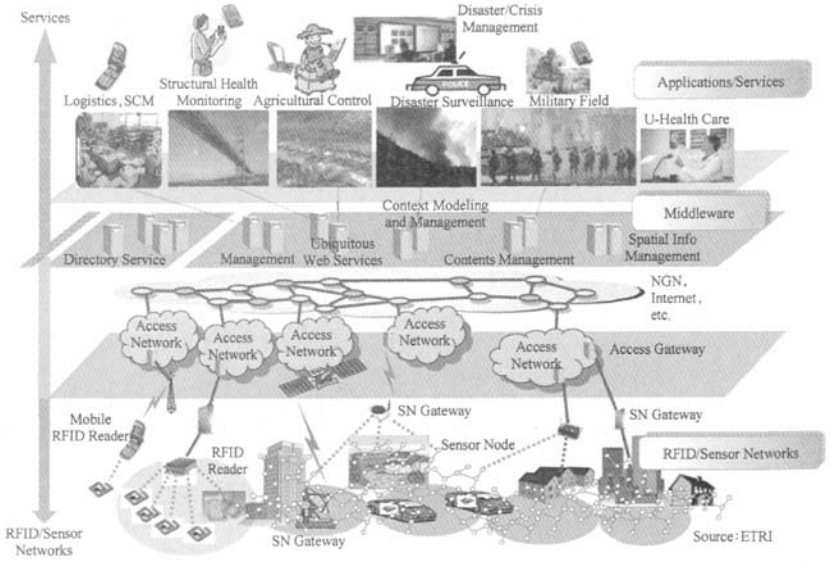

图 1 物联网系统体系结构

负责前端无线接入的无线传感器网络技术是支持物联网以及未来移动通信系统的重要技术基础,由于无线传感器网络具有自组织、拓扑动态变化、资源受限的特点,给网络安全的设计和实现提出了巨大的挑战,对无线传感器网络安全技术的研究已经是计算机网络和通信领域的一个热点.无线传感器网络安全主要关注密钥管理和安全路由.安全路由是无线传感器网络安全的一个重要部分,大部分安全机制都依靠路由提供的网络功能实现,大部分安全路由协议例如 ARAN,SAODV,SLSP[6] 协议,采用公开密钥证书加数字签名的安全机制,虽然完善了安全,但是计算量非常大、非常耗时,对于资源受限的无线传感器网络是沉重的负担.密钥管理涉及到身份识别、文件的加密传输、授权访问控制等活动,如何生成、发放、管理和使用密钥是无线传感器网络的一大问题,由目前有很多密钥管理方案都设计了各种方法代替互联网中常见的集中式认证中心(certification authority, CA),比如采用门限密码理论实现分布式的 CA 进行密钥管理[7],以及使用 PGP 算法通过节点证书交换实现自组织的密钥管理等[8].

目前还没有专门研究针对 3G 接入的物联网安全架构,无线传感器网络与 3G 网络的融合也出于起始研究阶段.3G 通信网络的安全技术与无线传感器网络的安全技术是独立分开的,同时无线传感器网络的认证和密钥管理等安全机制都没有形成国际标准,迫切需要建立物联网安全架构,提出跨网络架构的实体认证技术和隐私保护技术标准,实现物物互联安全通信的基本保障.

2 面向 3G 接入的物联网安全架构

物联网将来要在下一代移动通信网络 3G 系统的基础上发展起来的,因此它的安全架构可以在支持 3G 系统安全特征的基础上,结合无线传感器网络和 RFID 系统的安全有针对性地进行设计,以提

供完善的安全保障体系.基于以上考虑,本文专门针对无线传感器网络与3G网络的融合应用背景,提出面向3G接人的未来物联网的安全架构应该具有如图2所示的四层安全L

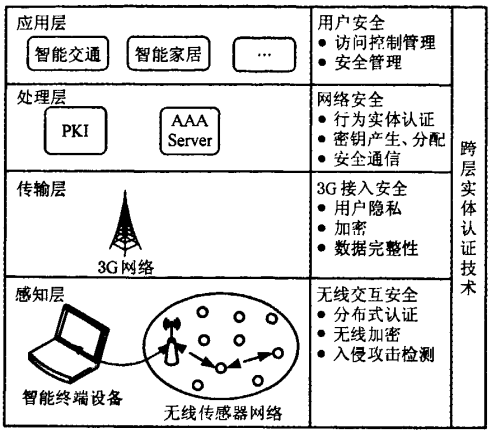

图2 面向3G接人的物联网安全架构

第1层是物联网感知层的无线交互安全,即无线传感器网络的分布式认证、无线加密和人侵攻击检测.分布式认证提供无线传感器节点设备和网关节点之间的简单的认证功能;无线加密包括无线传感器网络内所有设备相互之间无线通信加密算法协商、加密密钥协商、数据加密;人侵攻击检测主要检测拒绝式服务攻击、Sybil攻击、Wormhole虫洞攻击和Node Replication冒充攻击等,防范无线传感器网络节点设备被偷窃、攻击截获或者被恶意破坏后发起的内部攻击.

第2层是物联网传输层的3G接人安全,主要指为用户和无线传感器网络的网关节点提供安全3G移动通信网络服务.接人安全包括以下3个方面的安全特性:1)用户信息的保密性,包括用户标识的保密、用户位置的保密以及用户的不可追踪;2)加密,包括加密算法协商、加密密钥协商、数据加密和信令数据加密;3)完整性,包括完整性算法协商,完整性密钥协商、数据完整性,数据源认证及数据不可否认性.

第3层是物联网处理层的网络安全,包括提供行为实体认证服务和在3G通信网络运营商节点间安全传输数据,主要分为3个方面:1)密钥产生和分配,密钥管理中心产生并存储非对称密钥对,保存其他网络的公开密钥,为用户智能终端设备和无线传感器网络网关节点产生、存储并分配用于生产会话密钥的密钥材料,接收并分配来自其他网络的用于加密信息的对称会话密钥;2)安全通信,使用对称密钥实现数据加密、数据源认证和数据完整性保护.3)行为实体认证,包括用户对网络的认证、网络对用户的认证、异构网络间的认证.

第4层是物联网应用层安全,主要包括访问控制和安全管理.访问控制主要管理哪些物联网的资源可以被合法地访问,资源包括无线传感器网络的信息资源、处理资源、通信资源和物理资源.用户在要求无线传感器网络资源服务之前,必须要确认拥有访问资源的身份权限,同时确保为其服务的资源是完全可信的.安全管理包括配置管理、积累安全审计追踪和安全预警报告,确保物联网网络和系统的可用性,为政府管理部门的管理工作提供帮助.

在上述的面向3G接人的物联网安全框架中还有跨层的实体认证机制.感知层的智能终端与无线传感器网络的汇聚网关节点Sink,通过从下到上的认证机制借助第三方CA进行三向交互认证.认证通过后,用户通过智能终端设备就能够访问身边的无线传感器网络和RFID系统.未来智能设备具备与汇聚网关节点Sink之间的直接无线通信功能,相互认证之后通过协商密钥实现安全通信,在物理空间和信息空间保持互连.

3 面向3G接入的物联网安全架构验证系统

我们针对智能家居应用,按照上述的安全架构实现了一个面向3G接人的物联网安全验证系统,包括多种无线传感器节点和3G无线传感器网关节点构成的无线传感器网络,AAA认证服务器Web服务器.3G智能终端设备可以是3G上网卡的笔记本电脑,也可以是3G手机.3G智能终端设备直接访问Web服务器在通过用户身份认证之后,在数据库中查询历史感知数据,允许智能终端接人访问无线传感器网络,监视无线传感器网络的实时感知数据和无线传感器网络的运行状况,并且发送针对传感节点的查询、控制、管理、配置等控制命令.

验证系统的无线传感器网络中包括了温湿度传感器节点设备、被动红外传感器节点设备和图像传感器节点设备.无线传感器网络中的节点都是Telosb平台节点,采用MSP430处理器和2.4 GHz频段的CC2420无线通信模块,支持多种传感器模块,目前节点设备上的温湿度传感器能感知环境的温度、湿度;被动红外传感器能感应人体移动所发出的红外波,发出人员入侵警告;图像传感器能拍摄现场图

片,并生成 JPG 格式文件.

用户的 3G 智能终端设备在通过用户身份认证之后,不仅可以命令图像传感器拍照,设置温湿度感知采样周期和预警阈值等,还可以设置一些智能处理策略.智能处理策略很多是应用相关的,例如智能家居应用中可以设置被动红外传感器报警之后图像传感器节点立刻拍摄现场图片,并将图片以手机彩信或邮件的形式发送到用户的 3G 智能终端设备报警.

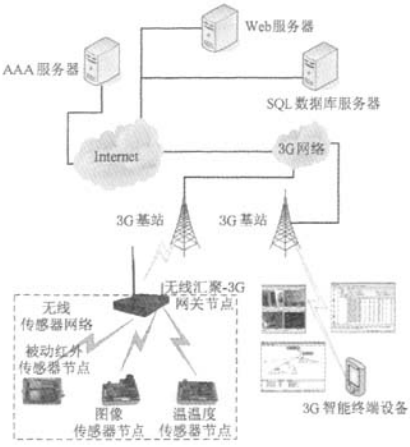

图 3 面向 3G 接入的物联网验证系统组成

无线汇聚-3G 网关节点内置了与无线传感器网络节点设备相同的无线通信模块,同时还内置了 3G 模块,既是无线传感器网络的汇聚节点,同时也是无线传感器网络与 3G 网络之间的网关节点.无线汇聚-3G 网关节点硬件和普通节点相似,使用 MSP430 处理器和 2.4 GHz 频段的 CC2 420 无线通信模块,另外还有 TD-SCDMA 模块和用户智能卡(USIM)和支持 3G 接入.无线传感器网络中的节点设备感知信息通过无线自组织网络传输到无线汇聚-3G 网关节点处.无线汇聚-3G 网关节点负责将无线传感器网络节点设备的感知数据使发送到后端服务器,同时将上针对传感节点的查询、控制、管理等命令转发到无线传感器网络中.

应用本文提出的面向 3G 接入的物联网安全结构,验证系统的安全架构实现也分为 4 层,第 1 层是物联网感知层的无线交互安全,无线传感器网络内节点和接入网关之间不使用认证机制,只对无线通信数据进行加密操作.无线加密操作采用 AES-128 加密算法,每个传感器网络使用不同的加密密钥,在每个传感器网络内部使用同一个加密密钥 K,节点生产的时候固化在每个节点内,省去了密钥分发的机制.

传输层的 3G 接入安全主要涉及到用户智能卡(USIM)和 TD-SCDMA 模块接入安全,包括以下 4 个安全机制:认证与密钥协商 AKA 机制用于用户智能卡(USIM)、访问位置寄存器(VLR)、用户位置寄存器(HLR)间的双向认证及密钥协商;用户身份保密(UIC)机制用于在空中接口保护用户的永久身份;用户及信令数据保密(DC)机制用于 TD-SCDMA 模块与服务网络无线接入控制器 RNC 间信息的加密;消息完整性保护(DI)机制用于 TD-SCDMA 模块和 RNC 之间信令消息的完整性进行保护.

第 3 层是物联网处理层的网络安全,包括提供行为实体认证服务和安全传输数据.在实验室环境下无线汇聚-3G 网关节点总是被认为是可信任的,Web 服务器上和无线汇聚-3G 网关节点之间目前没有实现认证功能.Web 服务器和无线汇聚-3G 网关节点共享一个对称密钥,3G 智服务器周期性向无线汇聚-3G 网关节点发送 Session ID,也就是随机数 R_1,分别使用共享对称密钥 K_1 和 MD5 Hash 算法生产该周期的会话加密密钥.

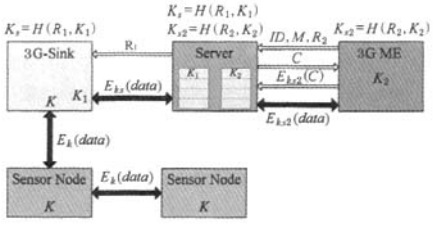

图 4 认证和密钥分发协议

Web 服务器上存储了经过授权访问无线传感器网络的用户名和相应密码,3G 智能客户端与 Web 服务器之间使用 challenge-response 三次握手协议进行认证.

1) 3G 智能客户端先向 Web 服务器发送 ID,请求信息 M 和随机数 R_2;

2) Web 服务器向 3G 智能客户端发送 challenge 消息,包含了随机数 C;

3) 3G 智能客户端使用 MD5 Hash 算法生成会

话加密密钥 K_{s2}，并对 challenge 消息的随机数 C 进行加密，向 Web 服务器返回 response 消息；

Web 服务器确认认证成功后，3G 智能客户端可以对无线传感器网络的资源进行合法访问和控制. 3G 智能客户端与 Web 服务器之间的数据通信采用会话密钥加密保障安全性.

4 结 语

对于物联网安全来说，各种不同无线通信技术与网络结构不断融合使得物联网不仅要面临既有的互联网安全威胁，还因为开放的无所不在的无线接入具备新的安全特性，需要重新考虑物联网的安全架构. 目前还没有专门研究针对 3G 接入的物联网安全架构，无线传感器网络与 3G 网络的融合也出于起始研究阶段. 3G 通信网络的安全技术与无线传感器网络的安全技术是独立分开的，同时无线传感器网络的认证和密钥管理等安全机制都没有形成国际标准，迫切需要建立物联网安全架构，提出跨网络架构的实体认证技术和隐私保护技术标准，实现物物互联安全通信的基本保障.

本文提出了面向 3G 接入的未来物联网的安全架构，并且在实验室实现了一个面向 3G 接入的物联网安全验证系统. 使用本文提出的面向 3G 接入的安全框架，融合其他物联网技术如 2G 网络、有线宽带网络、移动车载网络、RFID 系统和全球定位系统等，在此基础上研究面向物联网的无线网络认证机制、物联网的端到端认证机制、密钥管理方案和隐私保护机制等安全机制等，形成较为完善的物联网安全技术体系将是本文的后续工作.

参 考 文 献

[1] Ashton K. That 'Internet of Things' Thing. RFID Journal, 2009 [2010-04-20]. http://www.rfidjournal.com/article/print/4986

[2] Int Telecommunication Union. The internet of things. ITU Internet Reports, Executive Summary. Washington: ITU, 2005

[3] Vermesan O, Harrison M, Vogt H. Internet of things strategic research roadmap. CERP-IoT Report. Brussels: European Comission-Information Society and Media DG, 2009

[4] Wiki 维基百科. 物联网. (2010-04-16) [2010-04-20]. http://zh.wikipedia.org/zh-cn/物联网

[5] 孙利民，李建中. 无线传感器网络. 北京：清华大学出版社，2005

[6] Papadimitratos P, Haas Z J: Secure link state routing for mobile AD hoc networks //Proc of IEEE Workshop on Security and Assurance in Ad-Hoc Networks, in Conjunction With the 2003 Int Symposium on Applications and the Internet. Washington: IEEE Computer Society, 2003: 27-31

[7] Khalili A, Katz J, Arbaugh W. Towards security solutions for truly ad hoc networks //IEEE Workshop on Security and Assurance in Ad Hoc Networks, in Conjunction with the 2003 Int Symp on Applications and the Internet. Washington: IEEE Computer Society, 2003: 342-346

[8] Capkun S, Nuttya L, Hubaux J P. Jea-Pierre: Self-organized public-key management for mobile ad hoc networks. IEEE Trans on Mobile Computing, 2003, 2(1): 52-64

孙玉砚 男，1982 年生，博士研究生，助理研究员，主要研究方向为物联网安全.

刘卓华 男，1987 年生，硕士研究生，主要研究方向为物联网安全.

李 强 男，1986 年生，博士研究生，主要研究方向为物联网安全.

孙利民 男，1966 年生，研究员，博士生导师，主要研究方向为无线网络、物联网.