物联网通信协议的安全研究综述

杨 伟[1] 何 杰[2] 万亚东[2] 王 沁[2]

(江西师范大学软件学院 南昌 330022)[1] (北京科技大学计算机与通信工程学院 北京 100083)[2]

摘 要 国际标准化组织 IEEE 和 IETF 正携手为物联网制定一套高可靠、低功耗、可接入互联网的无线通信协议栈。IEEE 主要负责制定物联网通信协议的物理层和链路层的标准,如 IEEE802.15.4-2006 标准,其中 IEEE802.15.4e 是最新的链路层的标准。IETF 主要负责制定物联网通信协议的网络层及以上标准,如 6LoWPAN,RPL 和 CoAP 标准,其可以将资源受限的传感器节点接入互联网。网络安全是物联网大规模发展的基础,必须设计一套安全高效的机制保障通信协议的正常运行。文中详细介绍了物联网通信协议栈,重点分析和讨论了其安全方面的最新研究进展。最后总结和展望了物联网安全通信协议的研究方向。

关键词 物联网,安全,IEEE802.15.4e,RPL

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.12.005

Security for Communication Protocols in Internet of Things: A Survey

YANG Wei[1] HE Jie[2] WAN Ya-dong[2] WANG Qin[2]

(School of Software, Jiangxi Normal University, Nanchang 330022, China)[1]

(School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)[2]

Abstract The IEEE and IETF standardization bodies are working together to develop a framework for the communication protocols of the Internet of Things (IoT). The communication protocols can meet the important criteria of reliability, power-efficiency and Internet connectivity. The IEEE defines the physical layer and medium access control (MAC) layer standard such as IEEE802.15.4-2006, and IEEE802.15.4e is the latest MAC layer standards for the IoT. The IETF defines the network layer and above standards, such as 6LoWPAN, RPL and CoAP, which can connect the resource constrained sensor nodes to the Internet. Network security is the fundamental of large-scale development of IoT, so it is necessary to design some secure and efficient mechanisms to protect the communication protocols. This paper reviewed the communication protocols in the IoT, then analyzed and discussed the latest research progress of secure technologies for them. Finally, it summerized and looked ahead some important directions of secure communication protocols for IoT.

Keywords Internet of Things, Secure, IEEE802.15.4e, RPL

国际电信联盟(ITU)于 2005 年发布了一份《物联网》主题报告,该报告首次提出了“物联网将采用条形码、射频识别与传感器等感知设备,通过一套标准的通信协议,来实现任何物品的智能化识别与实时状态监管”[1-3]。当前全球主要发达国家掀起新一轮工业革命,各国正着手将物联网、大数据等新技术应用于工业智能制造过程中[4-5]。美国于 2012 年最先提出“工业物联网”的概念,将物联网新技术应用于高端制造业,从而达到振兴美国先进制造业的目的。德国于 2013 年提出了“工业 4.0”战略规划,通过构建信息物理系统将产品、设备以及人等各个要素关联起来,从而实现由传统制造工厂向智能化工厂的更新换代。我国于 2015 年发布了《中国制造 2025》战略规划,该规划指出“推动物联网、大数据等新一代信息技术和传统制造业深度融合,促进传统制造业向智能制造转型升级”任务。由此可见,将物联网新技术应用于未来工业应用领域是一个必然的发展趋势。

目前,国际标准化组织 IEEE 和 IETF 正携手为工业物联网制定一套高可靠、低功耗、可接入互联网的无线通信协议。通过大量廉价、资源受限的传感器节点实时地采集工业制造过程中的数据(如转速、振动、温度、湿度以及加速度等),然后采用一套标准的无线通信协议进行单跳或多跳传输,最后通过边界路由器将采集的数据发送到远距离服务器。IEEE 工作组主要负责制定链路层以下标准,如 IEEE802.15.4-2006

到稿日期:2018-04-01 返修日期:2018-07-06 本文受国家自然科学基金资助项目(61741125),国家“八六三”高技术研究发展计划基金项目(2014AA041801-2)资助。

杨 伟(1987-),男,博士,讲师,CCF 专业会员,主要研究方向为物联网安全,E-mail:yw@jxnu.edu.cn(通信作者);何 杰(1983-),男,博士,副教授,主要研究方向为物联网安全;万亚东(1982-),男,博士,副教授,主要研究方向为物联网安全;王 沁(1961-),女,博士,教授,主要研究方向为无线传感器网络与嵌入式系统。

标准[6],其中 IEEE802.15.4e[7]是其最新版的链路层的标准。IETF 工作组主要负责制定链路层以上标准,包括适配层 6LoWPAN[8]、网络层 IPv6 RPL[9]与应用层 CoAP[10]标准,其可以实现资源受限的传感器节点与下一代 IPv6 因特网进行互联互通。

由于物联网被广泛应用于石油、石化、煤矿、电网等国家基础设施领域,物联网安全问题将是其发展和应用过程中必须解决的关键问题。2010 年震网病毒(Stuxnet)导致全球范围内的多个工业控制网络无法正常工作(如伊朗核电站事故)。2015 年黑客针对乌克兰的电力系统发起恶意代码 BlackEnergy(黑色能量)攻击,导致长时间、大面积停电等严重后果。2016 年的 Mirai 事件中,攻击者利用网络摄像头等数以十万计的物联网设备向域名服务器发起 DDoS 攻击,导致大量用户无法正常使用网络服务。另外,信息安全界最有影响力的业界盛会 RSA2017 发布的七大致命攻击中就包括对工业物联网的攻击。可见,目前针对物联网的攻击事件层出不穷,并且越来越得到政府界与学术界的高度重视。

然而,目前物联网通信协议仍然存在许多严重的安全问题。文献[11-14]指出了物联网协议栈中链路层存在安全漏洞,攻击者可以发起时间同步攻击、篡改攻击和能量耗尽攻击等。文献[15-17]指出了物联网协议栈中 RPL 协议存在多种安全漏洞,攻击者可以发起女巫攻击、选择前向攻击、HELLO 洪泛攻击以及虫洞攻击等,从而破坏 RPL 协议正常运行。

本文首先介绍物联网协议栈及其安全架构;然后分别讨论物联网通信协议栈中物理层和链路层、6LoWPAN 自适应层、RPL 路由层和 CoAP 应用层的安全标准及机制的最新研究进展;最后总结和展望了物联网安全通信协议的研究方向。

1　物联网协议栈及其安全架构

1.1　物联网通信协议栈

国际标准化组织 IEEE 和 IETF 的工作目标是在资源受限的传感器节点上设计一套高可靠、低功耗、可接入互联网的通信协议栈,使其可以支持成百上千个节点进行自组织多跳通信。

IEEE 工作组于 2006 年公布适用于短距离、低功耗场景的 IEEE802.15.4-2006 标准[6],该标准物理层规定数据最大传输速率为 250kbps,工作在 ISM 频段上,其中在 2.4GHz 频段有 16 个信道。另外,IEEE802.15.4-2006 标准采用可选的时隙保障 GTS 机制和 CSMA-CA 信道访问机制,支持 ACK 机制以保证可靠传输。到目前为止,该标准已成为 ZigBee[18],WirelessHART[19],ISA100.11a[20] 和 WIA-PA[21] 等协议的物理层和链路层基础。但是基于 IEEE802.15.4-2006 标准的无线通信在低功耗和可靠性等方面暴露出很多问题,2008 年,DUST 公司提出了一种 TSMP(Time-Synchronized Mesh Protocol)时间同步技术[22]。TSMP 采用时分多址 TDMA 技术避免了网络中的节点空闲监听,降低了网络能耗,并采用时隙跳频机制解决了多径衰减和外界网络干扰的问题,提高了无线传输可靠性。2012 年,IEEE802.15.4 工作组正式发布 IEEE802.15.4e 标准,其核心技术是时间同步信道跳频(Time Synchronization Channel Hopping,TSCH),其中 TSMP 技术是 TSCH 的基础。在 IEEE802.15.4e 网络中,节点之间通过精确时间同步在预定时间开启或关闭射频,从而节省了节点能耗;另外,节点采用了基于时隙的跳频机制,从而增强了节点抵抗周围环境噪声干扰和多径干扰的鲁棒性[23]。

IETF 工作组主要负责协议栈的应用层、网络层与适应层等高层标准的制定。IETF 先后成立 3 个工作组,分别是 6LoWPAN(IPv6 over Low power Wireless Personal Area Networks)工作组、ROLL(Routing over Lossy and Low-power Networks)工作组和 CoRE(Constrained Restful Environment)工作组。IETF 6LoWPAN 工作组负责制定可以在低功耗个人局域网运行的 IPv6 协议。IETF ROLL 工作组负责制定可以在低功耗和有损网络运行的 IPv6 RPL 路由协议[9]。IETF CoRE 工作组负责制定可以在资源受限节点上运行的轻量级应用层 CoAP 协议[10],使得资源受限节点可以与现有互联网通信。另外,IETF 于 2013 年成立了 6TiSCH(IPv6 over the TSCH mode of IEEE 802.15.4e)标准组[24],负责 IEEE 802.15.4e TSCH 模式下 IPv6 协议的设计,该工作组在安全方面的最新进展包括低开销的安全入网机制和 6TiSCH 安全架构设计。

1.2　安全架构

物联网的安全目标与其他网络的安全目标基本上是一致的,其主要包括机密性、完整性、可用性、不可否认性和数据新鲜性 5 个目标。机密性是指通过采用信息加、解密技术保证机密信息不会泄露给未授权的实体。完整性是指通过采用完整性认证、散列和数字签名等技术保证信息不会被窜改。可用性是指采用容错、入侵检测或网络自愈等技术手段确保在遭受攻击的情况下网络依然能够提供正常服务。不可否认性是指信息源发起者不能否认自己发送的信息,常用技术包括签名、身份认证、访问控制。数据新鲜性是指保证用户在指定时间内得到所需要的信息,常用技术包括网络管理、入侵检测、访问控制。另外,物联网的安全目标还包括隐私、匿名和信任。

图 1 给出了物联网协议栈的安全架构。CoAP 是一种基于 UDP 协议的 REST 架构物联网应用层协议,采用 DTLS(Datagram Transport-Layer Security)[25-26]提供端到端的安全传输。DTLS 是在现存的 TLS 安全协议架构上的扩展,而 TLS 主要用于保证 TCP 上传输数据的安全,不能用来保证 UDP 上传输数据的安全,通过扩展可以使 DTLS 支持 UDP 数据报的安全传输。RPL 协议[9]采用 IPSec 来提供网络层的安全传输。IPSec 提供了网络层的数据包加密、源地址认证以及访问控制等安全服务。约束环境的认证和授权(Authentication and Authorization for Constrained Environments,ACE)工作组正在开发用于访问受限环境中服务器上托管资源的身份验证授权机制,并且最近完成了一个综合用例文档 RFC 7744[27]。受约束环境(DTLS In Constrained Environments,DICE)工作组正在研究用于受限制的物联网设备的 DTLS 协议。另外,轻量级实施指导(Light-Weight Implementation Guidance,LWIG)工作组为资源受限环境提供最小 IP 通信协议栈及相关安全技术,包括非对称加密技术和 IKEv2 认证协议。

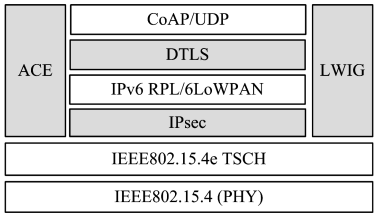

图 1 物联网通信协议栈安全架构图

Fig. 1 Security architecture for communication protocols in IoT

2 物理层和链路层协议安全

IEEE 802.15 工作组成立于 1998 年，该工作组致力于无线个人局域网(WPAN)的物理层(PHY)和链路层(MAC)的标准化工作，以为短距离相互通信的无线通信设备提供通信标准。IEEE 802.15 于 2000 年成立任务组 TG4，专门制定 IEEE 802.15.4 标准，并针对低速率个人局域网(LR-WPAN)制定标准。

2.1 物理层协议——IEEE802.15.4

IEEE802.15.4 物理层定义了 868 MHz，915 MHz 和 2.4 GHz 3 个频段，其中 868MHz 和 915 MHz 提供了 BPSK，ASK 和 O-QPSK 3 种调制方法，2.4GHz 仅提供了 O-QPSK 调制方法，数据传输速率最高可达 250kbps。目前，三大工业无线国际标准 WirelessHART[19]，ISA100.11a[20] 和 WIA-PA[21] 在物理层上均采用了 IEEE802.15.4 标准。另外，为了实现全球互联，大多只使用 IEEE802.15.4 的 2.4GHz 频段。

2.2 低功耗链路层协议——IEEE802.15.4e

许多工业应用场合对无线通信的可靠性、低功耗和实时性等性能要求苛刻，以前的 IEEE802.15.4-2006 标准无法满足以上要求。IEEE 工作组开始制定 IEEE802.15.4e[7] 标准并于 2012 年正式发布，标准的核心是 TSCH 技术。网络中，节点通过精确时间同步在预定时间开启或关闭射频，避免了节点空闲监听，节省了节点的能量；节点通过时隙跳频技术在不同时隙使用不同信道，增强了其抗干扰能力，提高了无线通信的可靠性。研究表明[28-30]，即使在恶劣工业无线环境中，TSCH 技术也可以实现网络丢包率低于 0.01%。

图 2 给出了 IEEE802.15.4e 网络中的节点通信示意图。矩阵横向表示时隙值(ASN)，其随着时间的推移不断递增。槽帧(Slotframe)是多个时隙的组合，可以周期性重复。矩阵纵向表示信道值，其值在 0～15 之间。网络中有 A，B，C 和 D 节点，假设将矩阵中的时隙-信道定义成[时隙值，信道值]，节点 A 和 B 在[1,1]进行通信，节点 A 和 C 在[2,4]进行通信，那么可知节点 A 在不同时隙可以使用不同信道进行通信。

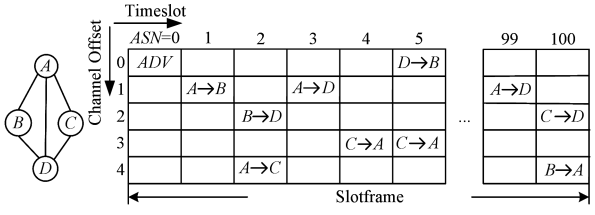

图 2 IEEE802.15.4e 网络中的节点通信示意图

Fig. 2 Communication between nodes in IEEE802.15.4e network

2.3 标准协议中的安全机制

无线通信相比于有线通信更容易遭受监听、中间人以及重放等攻击，IEEE802.15.4 标准在设计时充分考虑了安全问题，其在链路层提供了加密、认证以及重放保护等安全服务。IEEE802.15.4e 的安全部分直接继承了 IEEE802.15.4-2011 标准[31]，下面将从以下 3 个方面来介绍其安全机制。

(1)附加安全域设置

IEEE802.15.4e 帧主要由帧头、帧 PAYLOAD 和帧尾 3 部分组成。帧头由控制域、地址信息、附加安全头和 IE 头组成；帧 PAYLOAD 由 IE PAYLOAD、数据部分和 MIC 组成，其都要参与加密运算；帧尾由 2 个字节的 CRC 校验码组成。附加安全域主要位于帧头部分，具体如图 3 所示。帧控制域包括安全使能位，当安全使能位为 0 时，表示无安全；当安全使能位为 1 时，表示设置安全，则需要在附加安全头字段设置相应安全等级、密钥标识模式以及帧计数器。

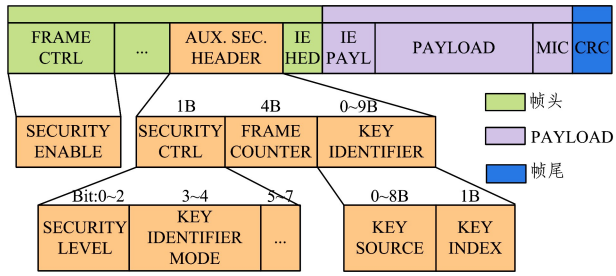

图 3 IEEE802.15.4e 帧格式中的附加安全域

Fig. 3 Security headers in IEEE802.15.4e frame

(2)安全服务的等级与密钥标识模式

表 1 列出了 IEEE802.15.4e 标准定义的 8 个安全等级，包括无安全、仅认证 MIC-32、仅认证 MIC-64、仅认证 MIC-128、仅加密 ENC、加密与认证 ENC-MIC-32、加密与认证 ENC-MIC-64、加密与认证 ENC-MIC-128。认证码的位数可以是 32，64 或 128。当选择安全等级 5 时，其提供数据加密和数据认证服务(M=4 kB)。IEEE802.15.4e 标准定义了 4 种密钥标识模式，当密钥标识模式设置为 0x00 时，表示节点采用预配置的密钥；当密钥标识模式设置为 0x01，0x02 或 0x03 时，则分别表示密钥标识长度为 1，2 或 3 字节。

表 1 IEEE802.15.4e 标准定义的安全等级

Table 1 Security levels defined by IEEE802.15.4e standard

安全模式	数据加密	数据认证(认证码的长度 M)
无	无	无(M=0)
MIC-32	无	有(M=4)
MIC-64	无	有(M=8)
MIC-128	无	有(M=16)
ENC	有	无(M=0)
ENC-MIC-32	有	有(M=4)
ENC-MIC-64	有	有(M=8)
ENC-MIC-128	有	有(M=16)

(3)安全加密与认证基本流程

当节点安全模式设置为 ENC-MIC-32 时，发送方先进行信息完整性认证，然后再进行加密操作；接收方收到数据包后先解密，然后再进行完整性认证。

发送方的信息完整性认证处理流程如图 4 所示。首先将

原始帧分成头部和 PAYLOAD 两部分,然后分别构造 AUTH 数据头部和 PAYLOAD,由于 AES-128 算法要求输入内容是分块,每块长度为 16 字节,因此当内容长度不够时就需要填充;初始向量(INIT VECTOR)由 Flags,NONCE 和 LEN 构成,其中 NONCE 的长度为 5 字节,由源地址和帧计数器构成;当 AUTH 数据头部和初始向量构建完成后,以 16 字节的分块作为 AES-128 算法的输入,以前一轮加密结果作为后一轮的输入,最后输出 16 个字节的数据 X_{t+1},若选用了 ENC-MIC-32 安全属性,则选择 X_{t+1} 的高 4 个字节作为 MIC。

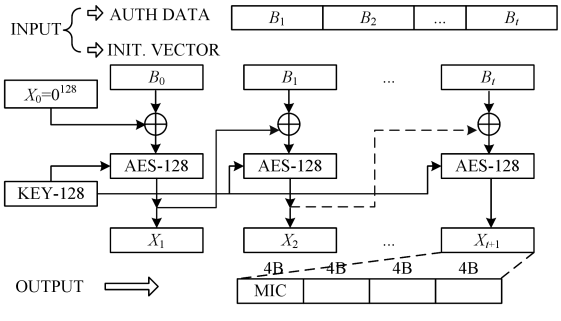

图 4　发送方的信息完整性认证流程

Fig. 4　Procedure of message integrity authentication in sender

IEEE802.15.4e 标准的加密处理流程如图 5 所示。将原始帧分成头部和 PAYLOAD 两部分,其中 PAYLOAD 部分构成加密数据(ENC DATA),不足 16 字节的整数倍则需要填充。原始帧的头部构成 A_0,A_1,A_2 等。当 ENC DATA 和 A_0,A_1,A_2 构建完成后,先将 ENC DATA 按照 16 个字节大小分块,输入信息完整性码 MIC 和预配置密钥 KEY,经过 AES-128 加密机后输出 C_0,C_1,…,C_t,取 C_0 信息块的最左端的 4 个字节作为加密后的 MIC,C_1,C_2,…,C_t 信息块构成 ENC PAYLOAD。因为采用对称加密算法后明文与密文的长度相同,所以取 C_1,C_2,…,C_t 信息块的最左端的 m 个字节,把原始帧头部一起连接起来构成最终的发送加密数据帧。最后射频通过无线方式将其发送出去。

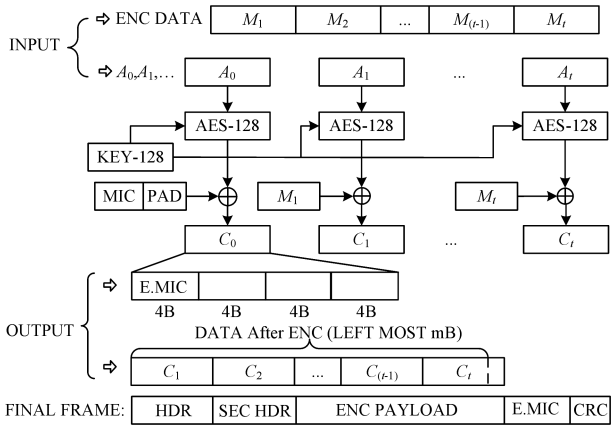

图 5　发送方的信息加密流程

Fig. 5　Procedure of message encryption in sender

接收方成功接收加密数据后,需要对其进行解密。接收方首先将密文拆分成 A_0,A_1,A_2,…信息块、ENC PAYLOAD 信息块和 MIC 3 部分。然后按照信息加密方法进行操作,密钥是预配置,经过 AES-128 加密机后输出 C_1,C_2,…,C_t 信息块,取其最左端的 m 个字节作为解密数据部分,C_0 信息块的最左端的 4 个字节作为解密后的信息完整性的码,记为 D.MIC。接收方的信息完整性认证的流程与发送方信息完整性的认证基本类似,通过信息完整性认证方法得到 MIC,然后与解密后的 D.MIC 进行比较,若相同则说明信息没有被篡改,可以正常接收,并回复 ACK 确认包。

2.4　其他相关安全机制

Sciancalepore 等[32-33]指出 IEEE802.15.4e TSCH 模式下节点需要保持高精度时间同步,攻击者可以通过篡改同步误差发起 DOS 攻击,故需要对同步信息包进行加密与认证,但是安全机制的引入会带来额外的时间开销,其可能对网络的时隙大小(典型值是 10 ms)产生影响。他们采用 OpenMote-CC2538 硬件节点[34]和 OpenWSN 软件平台[35],通过实测来评估 AES 和 CCM* 安全算法对最小时隙的影响,结果表明,采用硬件加速方式实现 ENC-MIC-32 对最小时隙几乎没有影响。

Sajjad 等[36]分析了 IEEE802.15.4 链路层协议的安全性,指出其在超帧的 CFP(Contention Free Period)和 CAP(Contention Access Period)阶段容易遭受攻击,如攻击者在 CAP 阶段监听 GTS 请求信息,然后在预定时间发送干扰信息,将导致协调器无法接收合法节点数据包;在 CFP 阶段通过篡改退避时间方式,可使信道处于忙状态,导致合法节点无法发送合法 GTS 请求。

Yang 等[37-38]挖掘了 IEEE802.15.4e 时间同步协议存在的漏洞,提出了一种基于时钟模型的 TOF 算法和基于信任的多跳时间同步算法,并通过 OpenWSN 平台[35]验证了算法的可行性和有效性。

Raymond 等[39]指出 WSN 中大部分链路层协议(如 S-MAC,T-MAC 和 B-MAC)无法抵御拒绝睡眠的攻击,该攻击将导致节点的电池寿命从几年下降到几天,并且 SPINS[40],TinySec[41],IEEE802.15.4 等安全协议均无法抵御拒绝睡眠。文中提出了一个安全防御框架,该框架包括强认证、重放保护、干扰检测、广播攻击保护和自适应流量限制等安全机制,可以有效地抵御拒绝睡眠攻击。

3　6LOWPAN 协议安全

IETF 于 2004 开始成立 6LoWPAN(IPv6 over Low power Wireless Personal Area Networks)协议工作组,负责制定可以运行在低功耗个人局域网的 IPv6 协议。

3.1　自适应层协议—6LoWPAN

当前互联网的协议是基于 IP 技术,物联网是互联网的延伸,将 IP 技术应用于物联网能够带来诸多好处[42-44],比如能够方便与其他 IP 网络进行互操作、使用 IP 网络成熟的安全机制以及负载均衡等。6LoWPAN 在 IEEE802.15.4 链路层之上提供 IPv6 网络访问服务,其通过简化 IPv6 包头来适应低功耗资源受限网络的要求。RFC 4944[45]定义了如何在 IEEE802.15.4 网络中传输 IPv6 数据包。RFC 6282[46]详细描述了 6LoWPAN 自适应层如何进行 UDP 数据包的头部压缩。

IEEE802.15.4 链路层规定数据包的最大长度为 127 字

节，而标准 IPv6 包头达到 40 个字节，留给数据部分的长度很短。如图 6 所示，6LoWPAN 通过对 IPv6 包头进行压缩，将 IPv6 包头缩减为 1 个包头压缩字节和 1 个剩余跳数字节。此外，6LoWPAN 采用分组实现应用层对物理层的透明传输，支持 IPv6 的 1280 字节长数据包，并通过在包头中添加 MESH 路由字段，实现基于 IPv6 的多跳路由转发。

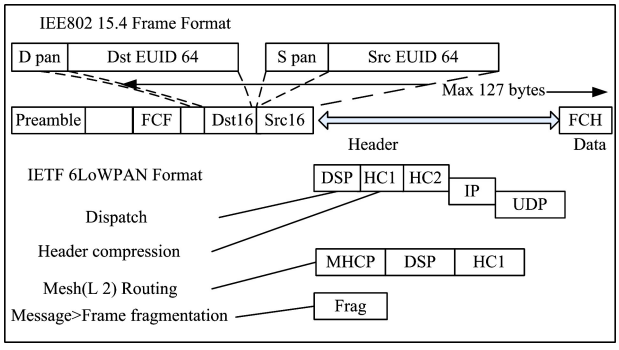

图 6 6LoWPAN 的 IPv6 扩展帧结构

Fig. 6 Structure of IPv6 extended frame in 6LoWPAN

3.2 6LoWPAN 协议中的安全机制

虽然 6LoWPAN 标准中没有定义相关安全机制，但是有相关的 RFC 文档讨论了 6LoWPAN 自适应层的安全问题。IETF 6LoWPAN 工作组从设计之初就非常重视安全，其在 2007 年发布的文档《6LoWPAN: Overview, Assumptions, Problem Statement, and Goals》[47]中描述了安全问题，并将此问题列入设计目标之一。另外，该文档对 6LoWPAN 网络的安全机制进行了可行性分析。

还有一些相关 RFC 文档也讨论了 6LoWPAN 自适应层的安全问题。如 RFC 4944[48]指出了攻击者可能会伪造或复制 EUI-64 MAC 地址，这可能会危及具有全球唯一性的 6LoWPAN 接口标识符。RFC 6606[49]提供了 6LoWPAN 网络中路由算法的指导方针，但并没有详细地描述路由算法。该文档指出了户外部署 6LoWPAN 网络中的节点可能遭受捕获或克隆攻击、洪泛攻击以及重放路由信息攻击。因此，需要在链路层和路由层上增加安全机制，如在 IEEE802.15.4 链路层上使用 AES/CCM 加密算法，在路由层上使用多路径路由算法。

3.3 6LoWPAN 中的其他相关安全技术

Hummen 等[50]详细分析了 6LoWPAN 协议中分片机制的安全性，指出了该机制缺少认证机制，攻击者可以利用该漏洞发起分片复制攻击和缓冲区保留攻击，从而导致接收方无法正常地组装到达数据包。然后提出了一种基于内容链接的认证方法来抵御分片复制攻击和一种分离缓冲器方法来检测缓冲区保留攻击。最后通过 Contiki 平台验证了攻击的破坏性和防御方法的有效性。

Raza 等[51]指出 6LoWPAN 定义了资源受限传感网中运行 IP 协议的机制，IPsec 是传统 Internet 网络中端到端的安全通信协议，文中提出了一种 6LoWPAN/IPsec 扩展机制来保障端到端通信的安全性，并与链路层单跳安全机制进行比较。实验表明在一个较大 IP 包或多跳情况下，6LoWPAN/IPsec 扩展机制比链路层单跳安全机制速度更快且延迟更短。

4 RPL 路由协议安全

RPL 是由 IETF RoLL(Routing over Lossy and Low-power Networks)工作组制定的物联网 IPv6 路由协议[9]，其主要应用于 LLN 网络。下面将详细介绍 RPL 协议及其安全方面的最新研究进展。

4.1 路由层协议——IPv6 RPL

RPL 是一种适用于 LLN 环境的距离矢量路由协议，其使用目标函数 OF(Objective Function)和度量来构建有向无环图(DODAG)。RPL 协议中定义了 DIO(DODAG Information Object)，DAO(DODAG Advertisement Object)和 DIS(DODAG Information Solicitation)3 种类型的控制信息包，其作用是建立和维护网络路由表。由于 DODAG 是有向无环图，IETF 6TiSCH 工作组推荐使用节点的下一跳路由作为其时间同步的父节点，从而不需要额外开销来构建和维护时间同步树。

采用 RPL 协议构建 DODAG 图主要包括两个阶段：建立向上路由和建立向下路由。建立向上路由是指构建一条从叶子节点到根节点的路径；建立向下路由是指构建一条从根节点到叶子节点的路径。图 7 给出了 RPL 协议构建 DODAG 图的具体步骤。

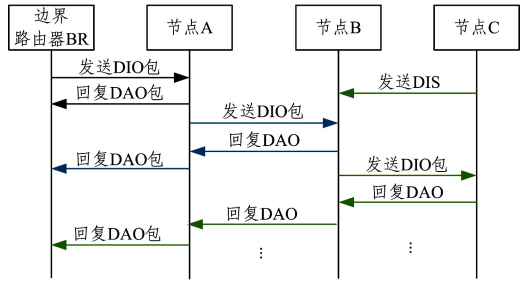

图 7 RPL 路由协议构建有向非循环图的过程

Fig. 7 Process of building DODAG in RPL routing protocol

(1)边界路由器 BR 广播包含 DODAG 图的信息的 DIO 包。

(2)节点 A 收到 BR 广播的 DIO 包后，过滤出 Rank、跳数和链路质量等相关参数，然后通过 OF 函数计算一个评价值，最后决定是否选择 BR 为父节点并加入该 DODAG 图。

(3)当节点 A 加入到 DODAG 图后，其可以广播 DIO 包，节点 B 以同样的方式决定是否选择节点 A 为父节点并加入 DODAG 图，若选择加入，则其发送 DAO 消息给边界路由器，从而建立向下路由。

在 RPL DODAG 图中，节点之间的 *Rank* 值的大小是有规律的，子节点 *Rank* 值在父节点 *Rank* 值的基础上增加 *RankIncrease*(*RankIncrease*>0)。假设节点 A 是节点 B 的父节点，则 $Rank(B)=Rank(A)+RankIncrease$。另外，*RPL* 协议中规定了 *RankIncrease* 的计算方法，具体计算过程如式(1)所示，其主要将发包数量和 ACK 回复数量的比率作为衡量指标。

$$RankIncrease=2*\frac{numTx}{numTxAck}*MINHOPRANKINC \tag{1}$$

4.2 RPL 协议中的安全机制

RFC 6550[9]文档中已经定义了 RPL 路由协议相关的安

全机制,用于保护 DIS,DIO,DAO 和 DAO-ACK 等控制消息。图 8 给出了安全 RPL 控制消息格式,其主要包括 ICMPv6 头部、安全域、DIO 消息格式或 DAO 消息格式部分和可选域。ICMPv6 头部中 Type 表示 RPL 包,默认设置为 155;Code 表示 DIO,Secure DIO,DAO 或 Secure DAO;Checksum 用于校验。RPL 安全域可以设置安全算法、密钥模式和安全等级。安全算法主要包括加密、完整性认证和数字签名算法。目前 RFC 6550[9] 文档中采用了 AES/CCM 作为加密和完整性认证算法,而数字签名算法选用了 SHA-256。

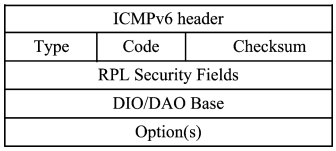

图 8　安全 RPL 控制消息格式

Fig. 8　Structure of secure RPL control message

另外,RFC 6550[9] 文档中定义了 3 种安全模式,分别是非安全、预安装和身份验证。在非安全模式下,DIO,DAO 等控制信息通过明文传输。在预安装安全模式下,RPL 使用安全的消息。为了加入 RPL,有向非循环图中的节点必须拥有预安装密钥,节点使用预安装密钥进行加密和完整性认证操作。在身份验证安全模式下,节点和路由器必须从密钥认证机构获取密钥,并使用非对称加密算法。RFC 7416[52],RFC 6687 [53] 和 RFC 8036[54] 也讨论了 RPL 路由协议的安全漏洞问题。

4.3　路由层中的其他安全机制

在 RPL 路由协议中,*Rank* 值非常重要,其可以用来避免循环、拓扑优化和降低控制开销,因此 *Rank* 值往往成为攻击者的目标。Wallgren 等[55] 指出了 Hello 洪泛攻击能够破坏 RPL DODAG 图,攻击者通过周期性广播一个信号很强但 *Rank* 值较小的 DIO 包,可以吸引很多邻居节点选择其作为路由父节点。Weekly 等[56] 指出了黑洞攻击可以破坏 RPL 路由协议,从而导致网络端到端的数据传输率大大下降。Le 等[57] 指出传感器节点大多没有防篡改保护,攻击者可以很容易地捕获到节点并获取到合法密钥,该内部攻击方式可以严重破坏 RPL 路由协议。文中深入分析了 Rank 攻击可导致网络端到端的数据传输率下降和延时增长。另外,文献[58-59] 也指出了 RPL 路由协议存在严重的安全漏洞,攻击者很容易破坏协议的正常运行。

Dvir 等[60] 指出了内部攻击者可以假冒网关或捕获网络中一个靠近网关的节点,然后通过非法增加有向非循环图的 *Version Number* 值或者伪造很小的 *Rank* 值来破坏 RPL 路由,该攻击将导致网络中大部分信息流向攻击者或消耗正常节点能量。文中提出了一种基于哈希链的 VeRA 算法来认证 *Version Number* 和 *Rank* 值的合法性,最后通过 MICAz 平台验证了该安全方法具有很低的时间开销。

Landsmann 等[61-62] 指出 RPL 路由协议面临拓扑攻击问题,恶意攻击节点可以通过伪造 *Version Number* 值或者 *Rank* 值来非法提高其在有向非循环图中的地位。VeRA 算法提出了一种 *Version Number* 和 *Rank* 值认证方法,但是其仍然存在伪造哈希链和 Rank 重放攻击,文中提出了一种连接 Version Number 和 Rank 的加密链方法和 Rank 请求-响应机制,并通过实际测试验证了该方法的有效性和可行性。

Zhang 等[63] 和 Le 等[64] 提出了一种基于入侵检测的安全 RPL 路由协议。他们通过分析 RPL 自组织特性,发现了一种新的 RPL 内部入侵方式,将该方式命名为路由选择(RC)入侵,然后设计了一套基于 ETX 度量的入侵检测系统(IDSs),最后在 Contiki 平台上验证了该方案可以有效地检测出 RC 入侵。

Djedjig 等[65-66] 提出了一种基于信任模型的安全 RPL 路由协议。文中指出仅使用信任平台模块(TPM)来确保节点之间的信任是不够的,内部攻击仍然可以破坏 RPL 拓扑的构建;采用基于节点行为的信任值方式,将安全方面的计算与处理交给 TPM 模块,节点可以很容易计算出其他节点之间的信任值,从而在 RPL 路由的建立和维护阶段抵御各种攻击。另外,文献[67-69] 也讨论了 RPL 路由相关的安全漏洞问题,并提出了一些轻量级的解决方案。

5　COAP 应用层协议安全

IETF CORE 工作组于 2010 年提出了 CoAP 标准[10],该应用层标准专门针对资源受限的嵌入式设备,比现有互联网应用层标准 HTTP 简单,便于小设备联网。下面详细介绍 CoAP 协议及其安全相关机制。

5.1　应用层协议——CoAP

CoAP 是一种基于 REST 架构的物联网应用层协议,最小数据包长度仅为 4 个字节。CoAP 协议与 HTTP 协议的最大区别是:前者基于 UDP 传输协议,后者基于 TCP 传输协议。主要原因是 TCP 协议非常复杂(包含流量控制和重传机制),不易在资源受限的嵌入式设备中运行,而 UDP 协议相对较简单,并支持多播。

CoAP 协议提供了请求/响应通信模型。CoAP 客户端节点向服务器发送请求信息,由服务器端进行响应。由于 CoAP 采用 UDP 传输协议,CoAP 通信不需要事先建立连接。CoAP 协议也提供了一个轻量级的可靠机制。CoAP 协议分为请求/应答层和会话层两层。会话层只负责控制端到端的报文交互,请求/应答层负责传输资源操作的请求和响应。另外,CoAP 协议已经在 OpenWSN[35] 和 Contiki 平台上得以实现。

CoAP 协议的报文结构如图 9 所示。信息头部主要由版本编号 Ver、报文类型 Type、CoAP 标识符长度 TKL、功能码/响应码 Code 和报文编号组成,长度为 4 字节。Token 长度为 0～8 字节,通过 TKL 指定。Options 为报文选项,通过报文选项可设定 CoAP 主机、CoAP URI、CoAP 请求参数和负载媒体类型等。Payload 为负载信息,该字段必须以 0xFF 起始,后面跟消息内容。

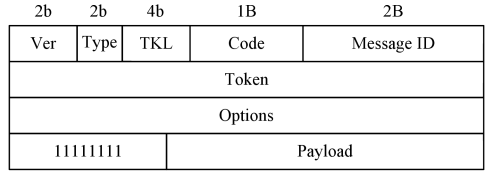

图 9　CoAP 协议的报文结构

Fig. 9　Message structure of CoAP protocol

5.2 CoAP 协议中的安全机制

CoAP 协议建议采用 DTLS(Datagram Transport-Layer Security)[28]来提供端到端的安全传输,采用了该安全机制的 CoAP 协议也被称为 CoAPs。DTLS 是在原有的 TLS 协议[70]架构上进行的扩展,使其能够支持基于 UDP 的应用(如 CoAP 协议)。DTLS 协议可以为应用层通信提供信息加密、完整性认证和身份认证等安全服务。

CoAP 标准中定义了 4 种安全模式:1)NoSec,不带安全机制,但是仍然可以使用低层的安全机制,如 IPSec 协议;2)PreSharedKey,DTLS 开启安全机制,使用预共享对称密钥模式,每对通信节点共享一个密钥,该模式适用于无法使用非对称密钥算法的资源受限环境;3)RawPublicKey,DTLS 开启安全机制,每对通信节点拥有一对非对称密钥,但是无 X.509 证书;4)Certificate,DTLS 开启安全机制,每对通信节点拥有一对非对称密钥,密钥对还拥有 X.509 证书,该证书可以由一些普通的信任根分配。另外,CoAP 协议中的 RawPublicKey 和 Certificate 安全模式建议采用椭圆曲线密码(ECC)算法[71]。

5.3 应用层中的其他安全机制

Keoh 等[72]和 Granjal 等[73]分析了 IETF 工作组制定的物联网标准协议,重点讨论了 CoAP 协议及其安全协议 DTLS。文中详细描述了 CoAP 协议的 RawPublicKey 安全模式,扩展了 DTLS 协议中的安全组通信,并减少了 DTLS 协议的包头长度,最后在 Contiki 平台上对 TinyDTLS 库进行了性能验证。

Raza 等[74]指出 DTLS 可以为 CoAP 协议提供加密和认证服务,但是存在开销过大的问题。文中提出了一种轻量级解决方案 Lithe,通过对 DTLS 包头进行压缩,可以有效缩短包的长度,其可以降低通信开销和避免 6LoWPAN 分片(降低分片攻击概率),最后在 Contiki 平台上验证了该方案的可行性和有效性。

Capossele 等[75]针对标准的 DTLS 协议存在开销过大的问题,提出了一种优化的 DTLS 协议。该优化协议充分利用了 CoAP 协议的特点,优化了椭圆曲线密码算法,从而使其达到良好的性能。在 MagoNode 硬件平台[76]上的实测结果表明,优化后的 DTLS 比标准版的 DTLS 网络寿命提高了 6.5 倍。另外,文献[77-78]也讨论了 CoAP 协议相关的安全漏洞问题,并提出了一些安全的解决方案。

总之,物联网通信协议还是存在大量的安全漏洞问题,需要不断地加强安全方面的研究。表 2 对当前物联网通信协议中典型的安全机制进行了小结,可以为物联网协议的安全设计提供必要参考。

表 2 物联网通信协议中典型的安全机制

Table 2 Summary of typical security mechanisms for communication protocols in IoT

文献	协议层	安全技术	抵御攻击	描述
文献[33]	IEEE802.15.4e MAC	AES-128 and CCM*	Forge,ACK frames attack	Hardware accelerations for link-layer security
文献[38]	IEEE802.15.4e MAC	Sec_ASN and TOF Algorithm	Forge,Replay,Pulse-delay	Secure ASN synchronization and secure single-hop Device-to-Device synchronization
文献[50]	6LoWPAN Adaptation	Content chaining scheme	Fragmentation atttack	Adds an authentication token to each fragment
文献[51]	6LoWPAN Adaptation	IPsec	Manipulate,Forge	Evaluation of the 6LoWPAN/IPsec extension
文献[60]	RPL Route	Hash chain	Rank atttack	Version Number and Rank Authentication
文献[65]	RPL Route	Trust-based	Internal and external attacks	New trust metric based on nodes' behaviors
文献[74]	CoAP Application	DTLS header compression scheme	Manipulate,Forge Fragmentation atttack	6LoWPAN header compression for DTLS
文献[75]	CoAP Application	DTLS optimizations	Manipulate,Forge	Security associations as CoAP resources

6 展望

安全性是物联网大规模发展的前提和基础,本文深入讨论了物联网通信协议中安全性相关机制的最新研究进展,该研究成果可以为安全物联网协议的发展及应用提供重要的参考价值。但是还存在许多未解决的问题,需要开展进一步的研究工作,主要的工作内容和研究思路如下。

(1)在物理层和链路层协议的安全方面,由于大部分传感器节点在计算和存储方面的性能受限,通常采用基于对称的 AES-128 算法进行信息的加解密,但是该方案存在密钥如何被安全分发的问题。有研究者建议采用非对称加密算法(如 TinyECC 或 NanoECC 算法)进行密钥分发,该方法一方面可以增大网络密钥被破解的难度,增强系统的安全性;另一方面降低了单纯使用非对称加密算法进行网络信息加解密带来的巨大开销。因此,基于混合机制进行物理层和链路层加解密算法的设计与实现是一个重要的研究方向。

(2)在 6LoWPAN 安全方面,建议采用 IPsec 安全协议对 IP 数据包进行认证和加密,从而为网络层提供一个端到端的安全保障。但是如何在资源受限的节点上运行 IPsec 安全协议和 IKE 密钥管理是一个巨大的挑战,目前还没有在工程中实现。有些研究者建议采用压缩 6LoWPAN 安全头部方法和精简版 IKEv2 密钥管理机制,使得其可以适用于资源受限环境。另外,6LoWPAN 协议缺乏认证机制,容易遭受包分片攻击,此攻击可破坏正常网络流,因此需要进一步提出安全解决方案。

(3)在 RPL 路由协议安全方面,RPL 路由协议主要面临路由信息重放、拜占庭攻击、选择前向攻击、黑洞攻击、女巫攻击、虫洞攻击以及捕获攻击等,目前 IETF RoLL 工作组虽然讨论了 RPL 路由协议的通用安全需求和目标,但是没有给出其具体的安全模型,仍然需要进一步研究安全威胁模型并开发一套实际系统来保护 RPL 协议。另外,基于信任模型的安全路由协议也是一个重要的研究方向,其可以有效抵御多种路由攻击。

(4)在 CoAP 应用层协议安全方面,标准版的 DTLS 协议可以提供端到端的安全传输,但其需要双向认证,存在开销过大的问题,下一步需要研究优化的 DTLS 协议。另外,CoAP

协议中的 RawPublicKey 和 Certificate 安全模式采用了椭圆曲线密码算法,该算法的安全性是建立在基于有限域椭圆曲线离散对数问题的困难性上的。在相同密钥长度下,椭圆曲线密码算法的安全性高于 RSA 公钥算法。但是椭圆曲线上的群操作需要大量运算,如何优化该算法使其适用于资源受限的传感器节点也是当前面临的一个重要挑战。

(5)由于无线通信信道的开放广播特性,其容易受到干扰攻击,IEEE 和 IETF 制定的物联网通信协议也不例外。为了有效应对干扰攻击,可以使用复杂的物理层技术,如直接序列扩频和跳频序列扩频技术。但是基于 IEEE 802.15.4 的无线网络在计算能力、频宽以及能耗方面的受限性,通常不采用复杂的物理层技术,而是在链路层上设计干扰检测与防御机制。干扰通常可以分为持续性干扰和选择性干扰,持续性干扰比较容易被检测出来,而选择性干扰非常隐蔽,一般在信道空闲时它不会发起攻击,而是在信道忙碌时发起攻击。IEEE802.15.4e 链路层采用了时间同步信道跳频方式,网络中的节点会周期性地采用相同的时隙和信道进行通信,攻击者可以通过监听网络信号的特征发现节点之间通信的规律,然后发起选择性干扰,从而破坏节点的正常通信。因此,如何有效检测与抵御选择性干扰对 IEEE802.15.4e 网络的攻击是一个重要的研究方向。

(6)物联网是一个开放、全球化的网络,其可能遭受各种各样的攻击(如跨层攻击、DDoS 攻击等)。传统的安全防御策略通常针对某种特定攻击,无法应对不断变化的攻击方式。机器学习是人工智能领域的一项重要支撑技术,其可以很好地解决一些语音识别、计算机视觉等分类问题,以及数据分析等预测问题。机器学习使用大量的经验数据,通过某种特定的算法来训练模型,从而可以对未来数据进行分类与识别。因此,将机器学习应用于物联网的攻击检测也是一个重要的研究方向。

结束语　目前,国际标准化组织 IEEE 和 IETF 正携手为物联网制定一套高可靠、低功耗、可接入互联网的无线通信协议栈,但是该通信协议存在大量的安全漏洞问题。本文首先介绍物联网通信协议以及安全架构;然后分别深入讨论该协议栈中物理层和链路层 IEEE802.15.4e 协议、自适应层 6LoWPAN 协议、路由层 RPL 协议和应用层 CoAP 协议的安全相关机制的最新研究进展,并对当前物联网通信协议中典型的安全机制进行小结;最后指出了物联网安全通信协议的发展方向,其中低开销椭圆曲线密码、选择性干扰攻击的防御、机器学习应用于物联网的攻击检测等都是未来重要的研究方向,该研究成果可以为物联网协议的安全发展及应用提供重要的参考价值。下一步主要从最新 IEEE802.15.4e 协议中低开销的安全机制和基于信任模型的安全 RPL 路由协议两个方面开展工作。

参 考 文 献

[1] DA XU L,HE W,LI S. Internet of things in industries:A survey[J]. IEEE Transactions on Industrial Informatics,2014,10(4):2233-2243.

[2] MIORANDI D,SICARI S,DE PELLEGRINI F,et al. Internet of things:vision,applications and research challenges[J]. Ad Hoc Networks,2012,10(7):1497-1516.

[3] BOTTA A,DE DONATO W,PERSICO V,et al. Integration of cloud computing and internet of things:a survey[J]. Future Generation Computer Systems,2016,56(C):684-700.

[4] BELLO O,ZEADALLY S. Intelligent device-to-device communication in the internet of things[J]. IEEE Systems Journal,2016,10(3):1172-1182.

[5] CHI Q,YAN H,ZHANG C,et al. A reconfigurable smart sensor interface for industrial WSN in IoT environment[J]. IEEE Transactions on Industrial Informatics,2014,10(2):1417-1425.

[6] ROBERT F,JAMES D,PATRICK W,et al. IEEE Standard for Local and Metropolitan Area Networks-Part 15.4:Low-Rate Wireless Personal Area Networks (LR-WPANs) [S]. New York:LAN/MAN Standards Committee,2006.

[7] ROBERT F,RICK A,PATRICK W,et al. 802.15.4e-2012:IEEE Standard for Local and Metropolitan Area Networks—Part 15.4:Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1 [S]. New York:LAN/MAN Standards Committee,2012.

[8] KUSHALNAGAR N,MONTENEGRO G,SCHUMACHER C. IPv6 over low-power wireless personal area networks (6LoWPANs):Overview,assumptions,problem statement,and goals,RFC 4919 [R]. New York:Internet Engineering Task Force,2007.

[9] THUBERT P,WINTER T,BRANDT A,et al. RPL:IPv6 routing protocol for low power and lossy networks [R]. New York:Internet Engineering Task Force,2012.

[10] BORMANN C,CASTELLANI A P,SHELBY Z. Coap:An application protocol for billions of tiny internet nodes[J]. IEEE Internet Computing,2012,16(2):62-67.

[11] SAJJAD S M,YOUSAF M. Security analysis of IEEE 802.15.4 MAC in the context of Internet of Things (IoT)[C]// Information Assurance and Cyber Security. IEEE,2014:9-14.

[12] YANG W,WANG Q,QI Y,et al. Time Synchronization Attacks in IEEE802.15.4e Networks[C]// International Conference on Identification,Information and Knowledge in the Internet of Things. IEEE,2014:166-169.

[13] SALEEM S,ULLAH S,KWAK K S. A study of IEEE 802.15.4 security framework for wireless body area networks[J]. Sensors,2011,11(2):1383-1395.

[14] JO M,HAN L,TAN N D,et al. A survey:energy exhausting attacks in MAC protocols in WBANs[J]. Telecommunication Systems,2015,58(2):153-164.

[15] LE A,LOO J,LASEBAE A,et al. The impact of rank attack on network topology of routing protocol for low-power and lossy networks[J]. IEEE Sensors Journal,2013,13(10):3685-3692.

[16] WALLGREN L,RAZA S,VOIGT T. Routing Attacks and Countermeasures in the RPL-Based Internet of Things[J]. International Journal of Distributed Sensor Networks,2013,2013(2):167-174.

[17] LE A,LOO J,LUO Y,et al. The impacts of internal threats towards Routing Protocol for Low power and lossy network performance[C]// Computers and Communications. IEEE,2013:789-794.

[18] KIM T,KIM S H,YANG J,et al. Neighbor table based shortcut tree routing in ZigBee wireless networks[J]. IEEE Transactions

on Parallel and Distributed Systems,2014,25(3):706-716.

[19] HART Communication Foundation. wirelessHART7.1 Specification [EB/OL]. [2009-04-02]. http://www.hartcomm2.org/hart_protocol/protocol/protocol_specs_popup.html.

[20] MONTERO S,GOZALVEZ J,SEPULCRE M,et al. ISA-100.11a-2011:Wireless Systems for Industrial Automation:Process Control and Related Applications [S]. New York:International Society of Automation (ISA) Standards Committee,2011.

[21] IEC/PAS 62601. Industrial communication network-fieldbus specifications WIA-PA communication network and communication profile[EB/OL]. http://www.iec.ch.

[22] PISTER K S J,DOHERTY L. TSMP:Time Synchronized Mesh Protocol[C]// Proceedings of the IASTED International Symposium on Distributed Sensor Networks (DSN08). IEEE,2008:391-398.

[23] WATTEYNE T,LANZISERA S,MEHTA A,et al. Mitigating Multipath Fading through Channel Hopping in Wireless Sensor Networks[C]// IEEE International Conference on Communications (ICC). 2010:1-5.

[24] DUJOVNE D,WATTEYNE T,VILAJOSANA X,et al. 6TiSCH:deterministic IP-enabled industrial internet (of things) [J]. IEEE Communications Magazine,2014,52(12):36-41.

[25] RAZA S,TRABALZA D,VOIGT T. 6LoWPAN compressed DTLS for CoAP[C]// 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS). IEEE,2012:287-289.

[26] KOTHMAYR T,SCHMITT C,HU W,et al. DTLS based security and two-way authentication for the Internet of Things[J]. Ad Hoc Networks,2013,11(8):2710-2723.

[27] SEITZ L,GERDES S,SELANDER G,et al. Use Cases for Authentication and Authorization in Constrained Environments [R]. New York:Internet Engineering Task Force,2016.

[28] STANISLOWSKI D,VILAJOSANA X,WANG Q,et al. Adaptive synchronization in IEEE802.15.4e networks [J]. IEEE Transactions on Industrial Informatics,2014,10(1):795-802.

[29] WATTEYNE T,WEISS J,DOHERTY L,et al. Industrial IEEE802.15.4e networks:Performance and trade-offs [C]// 2015 IEEE International Conference on Communications (ICC). IEEE,2015:604-609.

[30] VILAJOSANA X,WANG Q,CHRAIM F,et al. A realistic energy consumption model for TSCH networks[J]. IEEE Sensors Journal,2014,14(2):482-489.

[31] ROBERT F,RICK A,PATRICK W,et al. 802.15.4-2011:IEEE Standard for Local and Metropolitan Area Networks-Part 15.4:Low-Rate Wireless Personal Area Networks (LR-WPANs) [S]. New York:LAN/MAN Standards Committee,2011.

[32] SCIANCALEPORE S,PIRO G,VOGLI E,et al. LICITUS:A lightweight and standard compatible framework for securing layer-2 communications in the IoT [J]. Computer Networks,2016,108(1):66-77.

[33] SCIANCALEPORE S,VUČINIĆ M,PIRO G,et al. Link-layer security in TSCH networks:effect on slot duration[J]. Transactions on Emerging Telecommunications Technologies,2017,28(1):80-92.

[34] VILAJOSANA X,TUSET P,WATTEYNE T,et al. OpenMote:Open-Source Prototyping Platform for the Industrial IoT [C]// Eai International Conference on Ad Hoc Networks. 2015:211-222.

[35] WATTEYNE T,VILAJOSANA X,KERKEZ B,et al. OpenWSN:a standards-based low-power wireless development environment [J]. Transactions on Emerging Telecommunications Technologies,2012,23(5):480-493.

[36] SAJJAD S M,YOUSAF M. Security analysis of IEEE 802.15.4 MAC in the context of Internet of Things (IoT) [C]// 2014 Conference on Information Assurance and Cyber Security (CIACS). IEEE,2014:9-14.

[37] YANG W,WANG Q,WAN Y,et al. Security Vulnerabilities and Countermeasures for Time Synchronization in IEEE802.15.4e Networks[C]// 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE,2016:102-107.

[38] YANG W,HE J,WAN Y D,et al. Security Countermeasures for Time Synchronization in IEEE802.15.4e-Based Industrial IoT [J]. Journal of Computer Research and Development,2017,54(9):2032-2043. (in Chinese)
杨伟,何杰,万亚东,等. 基于 IEEE802.15.4e 标准的工业物联网安全时间同步策略[J]. 计算机研究与发展,2017,54(9):2032-2043.

[39] RAYMOND D R,MARCHANY R C,BROWNFIELD M I,et al. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols[J]. IEEE Transactions on Vehicular Technology,2009,58(1):367-380.

[40] PERRIG A,SZEWCZYK R,TYGAR J D,et al. SPINS:Security protocols for sensor networks [J]. Wireless Networks,2002,8(5):521-534.

[41] KARLOF C,SASTRY N,WAGNER D. TinySec:a link layer security architecture for wireless sensor networks [C]// Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems. ACM,2004:162-175.

[42] GUNGOR V C,HANCKE G P. Industrial wireless sensor networks:Challenges,design principles,and technical approaches [J]. IEEE Transactions on Industrial Electronics,2009,56(10):4258-4265.

[43] QUANG P T A,KIM D S. Enhancing real-time delivery of gradient routing for industrial wireless sensor networks[J]. IEEE Transactions on Industrial Informatics,2012,8(1):61-68.

[44] SALVADORI F,DE CAMPOS M,SAUSEN P S,et al. Monitoring in industrial systems using wireless sensor network with dynamic power management[J]. IEEE Transactions on Instrumentation and Measurement,2009,58(9):3104-3111.

[45] MONTENEGRO G,KUSHALNAGAR N,HUI J,et al. Transmission of IPv6 Packets over IEEE 802.15.4 Networks[C]// 2012 6th International Conference on Signal Processing and Communication Systems (ICSPCS). IEEE,2007:1-6.

[46] THUBERT P,HUI J,SELANDER G,et al. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks [R]. New York:Internet Engineering Task Force,2011.

[47] KUSHALNAGAR N,MONTENEGRO G,SCHUMACHER C,et al. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs):Overview,Assumptions,Problem Statement,

Goals [R]. New York:Internet Engineering Task Force,2007.

[48] MONTENEGRO G,KUSHALNAGAR N,HUI J,et al. Transmission of IPv6 Packets Over IEEE 802.15.4 Networks [R]. New York:Internet Engineering Task Force,2007.

[49] KIM E,KASPAR D,GOMEZ C,et al. Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network(6LoWPAN) Routing[R]. New York:Internet Engineering Task Force,2012.

[50] HUMMEN R,HILLER J,WIRTZ H,et al. 6LoWPAN fragmentation attacks and mitigation mechanisms[C]// ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM,2013:55-66.

[51] RAZA S,DUQUENNOY S,HÖGLUND J,et al. Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN[J]. Security & Communication Networks,2014,7(12):2654-2668.

[52] ALEXANDER R,TSAO T,DAZA V,et al. A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)[R]. New York:Internet Engineering Task Force,2015.

[53] TRIPATHI J,OLIVEIRA J,VASSEUR P,et al. Performance evaluation of the routing protocol for low-power and lossy networks (RPL) [R]. New York:Internet Engineering Task Force,2012.

[54] WINGET N,HUI J,POPA D,et al. Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks [R]. New York:Internet Engineering Task Force,2017.

[55] WALLGREN L,RAZA S,VOIGT T. Routing Attacks and Countermeasures in the RPL-based Internet of Things[J]. International Journal of Distributed Sensor Networks,2013,2013(2):167-174.

[56] WEEKLY K,PISTER K. Evaluating sinkhole defense techniques in RPL networks[C]// 2012 20th IEEE International Conference on Network Protocols (ICNP). IEEE,2012:1-6.

[57] LE A,LOO J,LUO Y,et al. The impacts of internal threats towards Routing Protocol for Low power and lossy network performance[C]// 2013 IEEE Symposium on Computers and Communications (ISCC). IEEE,2013:789-794.

[58] MAYZAUD A,BADONNEL R,CHRISMENT I. A Taxonomy of Attacks in RPL-based Internet of Things[J]. International Journal of Network Security,2016,18(3):459-473.

[59] MEDJEK F,TANDJAOUI D,ABDMEZIEM M R,et al. Analytical evaluation of the impacts of Sybil attacks against RPL under mobility[C]// 2015 12th International Symposium on Programming and Systems (ISPS). IEEE,2015:1-9.

[60] DVIR A,BUTTYAN L. VeRA-version number and rank authentication in rpl[C]// 2011 IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS). IEEE,2011:709-714.

[61] LANDSMANN M,WAHLISCH M,SCHMIDT T. Topology Authentication in RPL[C]// Computer Communications Workshops. IEEE,2013:73-74.

[62] PERREY H,LANDSMANN M,UGUS O,et al. TRAIL:Topology Authentication in RPL[C]// International Conference on Embedded Wireless Systems and Networks. Junction Publishing,2015:59-64.

[63] ZHANG L,FENG G,QIN S. Intrusion detection system for RPL from routing choice intrusion[C]// 2015 IEEE International Conference on Communication Workshop (ICCW). IEEE,2015:2652-2658.

[64] LE A,LOO J,LASEBAE A,et al. The impact of rank attack on network topology of routing protocol for low-power and lossy networks[J]. IEEE Sensors Journal,2013,13(10):3685-3692.

[65] DJEDJIG N,TANDJAOUI D,MEDJEK F. Trust-based RPL for the Internet of Things[C]// 2015 IEEE Symposium on Computers and Communication (ISCC). IEEE,2015:962-967.

[66] DJEDJIG N,TANDJAOUI D,MEDJEK F,et al. New trust metric for the RPL routing protocol[C]// 2017 8th International Conference on Information and Communication Systems (ICICS). IEEE,2017:328-335.

[67] JIANG N,LIU J,XIAO W,et al. Routing attacks prevention mechanism for RPL based on micropayment scheme[C]// International Conference on Wireless Communications,Signal Processing and Networking (WiSPNET). IEEE,2016:835-841.

[68] CHZE P L R,LEONG K S. A secure multi-hop routing for IoT communication[C]// 2014 IEEE World Forum on Internet of Things (WF-IoT). IEEE,2014:428-432.

[69] HUMMEN R,WIRTZ H,ZIEGELDORF J H,et al. Tailoring end-to-end IP security protocols to the Internet of Things[C]// 2013 21st IEEE International Conference on Network Protocols (ICNP). IEEE,2013:1-10.

[70] BLAKE-WILSON S,NYSTROM M,HOPWOOD D,et al. Transport layer security (TLS) extensions [R]. New York:Internet Engineering Task Force,2006.

[71] SEO H,SHIM K A,KIM H. Performance enhancement of TinyECC based on multiplication optimizations[J]. Security and Communication Networks,2013,6(2):151-160.

[72] KEOH S L,KUMAR S S,TSCHOFENIG H. Securing the internet of things:A standardization perspective[J]. IEEE Internet of Things Journal,2014,1(3):265-275.

[73] GRANJAL J,MONTEIRO E,SILVA J S. Security in the integration of low-power Wireless Sensor Networks with the Internet:A survey[J]. Ad Hoc Networks,2015,24:264-287.

[74] RAZA S,SHAFAGH H,HEWAGE K,et al. Lithe:Lightweight secure CoAP for the internet of things[J]. IEEE Sensors Journal,2013,13(10):3711-3720.

[75] CAPOSSELE A,CERVO V,DE CICCO G,et al. Security as a CoAP resource:an optimized DTLS implementation for the IoT [C]// 2015 IEEE International Conference on Communications (ICC). IEEE,2015:549-554.

[76] COLESANTI U M,LO RUSSO A,PAOLI M,et al. Introducing the magonode platform[C]// Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems. ACM,2013.

[77] AL-FUQAHA A,GUIZANI M,MOHAMMADI M,et al. Internet of things:A survey on enabling technologies,protocols,and applications[J]. IEEE Communications Surveys & Tutorials,2015,17(4):2347-2376.

[78] KARAGIANNIS V,CHATZIMISIOS P,VAZQUEZ-GALLEGO F,et al. A survey on application layer protocols for the internet of things[J]. Transaction on IoT and Cloud Computing,2015,3(1):11-17.