物联网安全挑战：云和区块链、后量子、密码学和进化技术

帕沃尔·加洛，彼得·普洛泽克
（所属机构：索瓦克电气工程与信息技术学院）

摘　要：物联网连接物理世界和控制论世界。因此，物联网设备的安全问题尤其具有破坏性，需要加以解决。在本论文中，我们从未来威胁的角度概述了物联网当前的安全问题。我们确定了需要特别解决的三个主要趋势：物联网与云和区块链集成的安全问题，量子计算导致密码学的快速变化，以及人工智能的兴起和安全范围内的演化方法。关于物联网，我们概述了已识别的威胁，并提出了未来保护物联网的解决方案。

关键词：物联网；云；区块链；后量子；进化；人工智能

IoT Security Challenges: Cloud and Blockchain, Postquantum, Cryptography, and Evolutionary Techniques

Pavol Gallo, Peter Ploszek
(Affiliation: Faculty of Electrical Engineering and Information Technology, Sovakia)

Abstract: Internet of Things connects the physical and cybernetic world. As such, security issues of IoT devices are especially damaging and need to be addressed. In this treatise, we overview current security issues of IoT with the perspective of future threats. We identify three main trends that need to be specifically addressed: security issues of the integration of IoT with cloud and blockchains, the rapid changes in cryptography due to quantum computing, and finally the rise of artificial intelligence and evolution methods in the scope of security of IoT. We give an overview of the identified threats and propose solutions for securing the IoT in the future.

Keywords: Internet of Things; cloud; blockchain; postquantum; evolution; artificial intelligence

引言

每个人的感知现实不仅包括物理维度，还包括网络空间中重要的虚拟存在。然而，网络空间维度并不是独立的：大量连接的传感器将数据从物理世界带到网络空间。这些数据会影响连接到网络空间的人们的行为，以及对物理世界中流程的反馈，尤其是在控制系统中。同样，仅在网络空间中产生的数据可以通过影响人类思维或连接到网络空间的控制系统来影响物理世界。互联的物理和控制论世界面临许多重要问题，例如：如果数据不正确甚至是恶意的怎么办？如果流程被错误地编程或被完全编程以产生有害结果怎么办？有错误意图的人会以意想不到或完全禁止的方式影响我们的控制论系统，并通过它们影响物理世界吗？我们知道答案是肯定的，虚拟世界对人身伤害的可能性是真实存在的。因此，关注控制论现实的安全方面至关重要，尤其是在它与物理世界有强烈互动的领域。

在本次调查中，我们重点关注物联网设备、产品和技术的安全性。物联网设备已成为网络犯罪分子最常见的攻击目标之一。物联网设备数量的迅速增加进一步加剧了这些问题。2019 年至 2030 年间，全球物联网连接设备的数量预计将从 76 亿增长到 241 亿，收入将从 4650 亿美元增长两倍多，达到 1.5 万亿美元以上。其他亮点是，正如预期的那样，WiFi、蓝牙和 802.15.4（例如 Zigbee）等短距离技术在整个预测期内占据主导地位。几乎四分之三的联网设备都使用这些技术。原因很明显：部署它们比广域或园区技术更容易、成本更低，任何物联网部署自然会默认使用这些技术，除非有充分的理由不这样做，最明显的是缺乏可用网络。全球市场平分四份：中国 (26%)、北美 (24%)、欧洲 (23%) 和世界其他地区 (27%)。后者最大的部分是日本，占 6%，拉丁美洲占 5%。

联网设备、传感器、执行器、GPS 和移动设备被集

成以形成基于物联网 (IoT)、智能电网、传感器网络等概念的混合网络。研究人员建议物联网和云计算之间的合作，因为物联网环境中使用的设备具有局限性，例如：低功耗、低容量和有限的性能。 通过将物联网设备与云计算技术相结合，可以创建高效的服务。 例如，电子医疗云计算系统极大地造福于患者获得优质高效的医疗服务，尤其是在资源不对称的环境下。 医疗保健提供者使用的电子医疗云服务器通常被认为具有强大的存储和计算能力。 需要将频繁收集的 PHI 外包到云端进行存储和预处理，然后再交给相应的医生进行医疗诊断。

关于云互联网的概念，传统的物联网方法无法同时满足低成本和简单性的需求——要么事物变得更加昂贵和复杂，要么对其计算资源需求施加限制。 然而，云提供了一种有可能满足这两种需求的解决方案。 因此，云计算提供了另一种解决方案，为物联网提供了几乎无限的计算能力来源，可以通过互联网轻松访问，具有更好的弹性，并且成本更低。有研究已经指出，云和物联网的配对对安全有影响。 物联网采用云服务也带来了新的安全挑战。 更多现有文章讨论了 IoT 和云计算的安全方面，并强调了该领域的一些新的和有趣的挑战。 安全和隐私正在成为物联网基础设施部署中的主要挑战。 虽然云安全是一个有据可查的挑战，但云与物联网之间的配对带来了额外的担忧。 在一项对物联网和云计算的调查中，研究人员重点关注这两种技术的安全问题。 他们还将这些领域与另一种称为移动云计算 (MCC) 的技术联系起来。 移动云计算被定义为云计算技术与移动设备的集成，使移动设备在计算能力、内存、存储、能量和上下文感知方面具有丰富的资源。 根据研究，主要的安全问题是过时的操作系统和弱密码。由于网络设备和其他对象的概念相对较新，因此在产品设计中并不总是考虑安全性。 物联网产品通常与旧的和未打补丁的嵌入式操作系统和软件一起出售。 此外，购买者通常无法更改智能设备上的默认密码——或者即使他们更改了密码，也无法选择足够强的密码。

物联网和云系统的安全性越来越紧密地交织在一起。第一个物联网僵尸网络被发现于 2013 年 12 月，超过 25% 的僵尸网络由计算机以外的设备组成，包括智能电视、婴儿监视器和其他家用电器。 由于物联网中部署了多种不同的技术和平台，因此很难制定统一的安全策略。 一些设备根本没有足够的计算能力和 / 或内存来实施安全预防措施。 物联网设备通常由容量有限的电池供电，必须节约能源。 保护物联网设备免受某些类型的攻击会导致能耗显着增加； 因此，重要的是首先识别可能的威胁，然后针对开发的物联网系统的特定架构实施适当的对策。

物联网、标准和协议的安全模型

安全建模是构建安全系统的重要准备。 在本节中，我们总结了我们使用的物联网基础设施的安全模型。 一般来说，我们可以认为物联网领域会遭受所有标准类别的对手的攻击，这些对手具有基于互联网的攻击者的典型属性。 因此，我们可以对网络应用程序使用攻击者的一般模型。 在考虑物联网时，我们可以指出一些具体差异：特别是对于工业物联网，工业间谍代理可以作为威胁代理发挥更重要的作用。 他们的具体目标包括工业秘密和专有技术以及工业流程的潜在破坏。 网络恐怖分子是一类具有潜在高影响力的危险攻击者。 这些攻击者可能会针对因网络攻击而对物理世界产生影响的特定物联网设备。 因此，他们的目标是对现实世界（物理）产生影响，其中物联网设备代表过渡资产，而不是攻击者的最终目标。

物理攻击

此类别包括针对硬件本身的攻击。

• 节点篡改——要执行此攻击，攻击者必须能够物理访问物联网设备。 他们的目标是获取敏感信息，例如用于与其他节点通信的加密密钥。 根据研究员的说法，可以将这些攻击描述为侵入性和非侵入性。 侵入式攻击需要昂贵的设备，因为攻击者试图通过直接观察半导体芯片来获取处理器内存的内容。 非侵入性方法包括获得对总线的访问权，该总线可用于访问微处理器的内存。 JTAG 总线经常用于这些目的。 这样，就有可能造成很大的破坏，因为有可能，例如，根据攻击者的请求，用处理器的引导加载程序覆盖处理器的引导加载程序，并激活内存中的读写操作。通过检测对设备盒的入侵，可以相对容易地防止这种攻击。 机械开关或附加传感器可用于检测电源电压的波动。 使用此对策的一个问题可能是频繁的误报。

• RF 干扰——干扰是由多个设备同时以相同频率传输造成的。 攻击者不必传输任何数据； 在给定通信信道的载波或副载波频率上传输噪声就足够了。 这种攻击的目标是实现拒绝服务。

• 节点干扰——这种攻击主要来自无线传感器网络 (WSN)。 在 WSN 中，节点之间的通信是必不可少的；因此，非常需要快速的攻击检测。 要成功执行攻击，攻击者需要对通信协议有深入的了解。 通过调整路线，可以避开拥塞区域。JAM（干扰区域映射协议）、SAD-SJ（自适应和分散的 MAC 层）或 JAM-BUSTER 协议是合适的。

网络攻击

• 流量分析攻击——实现这种攻击的先决条件是有可能拦截物联网网关和通过互联网与网关通信的用户之间的通信。 被动窃听允许攻击者找出物联网设备的类型以及连接到网关的物联网设备的活动。通信也可以加密。对于这种攻击，通信是否加密并不重要。 流量分析提供了其他危险攻击所需的数据，例如恶意代码注入。目前没有针对这种攻击的完美保护，但可以减轻这种攻击。

• Sinkhole 攻击——攻击的基本思想是破坏恶意节点

周围附近节点的数据通信。有两种主要类型的反措施。第一种方法是实施入侵检测系统。一般来说，这些系统的缺点是准确性高，因此误报的频率相对较高。另一种选择是适当的密钥管理，其中使用基于身份的加密算法保护每个节点的身份。

• 中间人攻击——这种攻击类似于恶意节点注入。在被动攻击中，攻击者窃听通信。如果攻击处于活动状态，则攻击者会控制通信。它们可以延迟数据包、丢弃数据包或更改其内容。不同之处在于攻击者不必是网络的一部分，因为整个攻击完全通过传感器网络的给定网络通信协议进行。针对 MITM 的最常见保护是质量入侵检测系统 (IDS)。在这个解决方案中，在低延迟、高检测率、低 CPU 负载和由此产生的算法低功耗之间寻求折衷。IDS 通常部署在层级更高、功能更强大的设备上，例如 Fog 或 Edge 设备的网关。

物联网安全中的云和区块链

近年来，出现了很多使用区块链技术替代云存储的提议。利用区块链可以提高网络维护的安全性和效率。区块链的关键特征，即不变性，可以防止未经授权的修改。有大量论文关注区块链和物联网集成。在我们的工作中，我们专注于与适用于物联网应用的区块链相关的安全问题。

公共区块链和物联网安全

公有链，我们理解为一种分布式开放的点对点区块链，具有无中心信任的共识机制。在安全意义上，公共区块链是一个安全的公共公告板：仅附加的项目列表，每个人都可以阅读，没有人可以修改。只有在所用技术的安全先决条件成立时，链的历史才是不可变的，例如，在 PoS 类型的协议中存在受信任的大多数节点，或者没有攻击者可以获得比 PoW 协议中的其他节点组合更多的计算能力，而开放的公共区块链不保证法律保护或信任。区块链的主要原则是用对技术（区块链本身和运行区块链的软件）的信任取代对某些法律实体（例如云提供商）的信任。物联网提供商应仅选择满足监管要求的公共区块链。缺乏全球标准是该领域的一个重大问题。虽然区块链技术提供了一定程度的完整性保护，但原则上，公共区块链上的每个操作都是公开的。机密数据在提交到区块链之前必须加密。但是，区块链可以揭示重要的元数据，例如谁在何时发布了哪些数据。隐藏技术涉及额外成本，并且可能不足以满足某些用例。区块链访问的可用性可能是一个重大问题。区块链运营成本高昂；因此，在区块链上发布任何信息比使用标准的分布式数据存储解决方案要昂贵得多。区块链无法解决针对物联网客户端或指挥中心的网络基础设施的拒绝服务攻击问题。

私有区块链和物联网安全

在为物联网设计安全解决方案时，我们可以考虑私有区块链。私有区块链不需要复杂的共识机制，即使某些物联网节点受到损害，各种协议也具有弹性。公共区块链的机制（例如工作证明）不适合私有解决方案，因为它们的高成本反映了对网络缺乏信任。区块链存储不适合临时数据，因为区块链的数据结构是仅追加。为了限制区块链的整体数据存储，需要仔细考虑链中应该存储什么。私有区块链需要类似于标准云解决方案的安全机制，包括访问控制、管理、备份等。与标准数据库解决方案相比，即使是私有区块链数据结构也会产生额外的运营成本。因此，我们建议仅将区块链用作存储永久数据项的部分技术解决方案，其中需要保持不可变的线性排序。

后量子密码学应用

网络安全现在正处于一个新时代的边缘。量子计算机发展的新成果导致了严重的后果。对手拥有更多的计算能力，并且出现了新的威胁。目前用于物联网设备安全的算法，尤其是密钥交换和数字签名，很容易受到量子计算机发展产生的新型攻击。与传统计算机（台式机和笔记本电脑）相比，我们还有另一个因素需要考虑。攻击者的计算能力正在增加，但我们在物联网设备上的资源非常有限。

物联网安全中使用的算法

有许多协议用于保护物联网通信。然而，随着我们深入了解它们使用的特定加密算法，我们可以看到这些协议中使用的密码数量有限。关于物联网中使用的最重要的协议，对于每一层，我们展示了协议并使用了有趣的加密算法：

• 物理层——大多数物理层协议（DASH7、LoRa）使用 AES-128 来提供数据的机密性。

• 数据链路层——安全由 IEEE 802.15.4 提供，它指定了几个加密选项，但都基于 AES (AES-32 - AES-128)。

• 网络层——IPsec 协议是 IPv6 的要求，允许 Diffie - Hellman、ECDH、RSA、AES。网络层的另一个协议，6LoWPAN 协议，只依赖于传输层的安全性。

• 传输层——在传输层，我们主要可以使用两种类型的协议，TCP 或 UDP。对于 TCP，安全性由 TLS 提供，在版本 1.3 中允许 AES 和临时 Diffie - Hellman。UDP 由 DTLS 或 QUIC 保护。这些协议允许使用短暂的 Diffie - Hellman 进行密钥交换，使用 AES 进行数据保密。

• Application Layer——CoAP 协议提出使用 DTLS 提供安全性，AMQP 协议使用 TLS。因此，使用与传输层相同的算法。

威胁我们密码学的量子算法

当我们谈论量子计算机对现代密码学的威胁时，我们主要谈论两种算法：（一）Shor 算法是一种量子计算机算法，用于在多项式中寻找给定数的质因数（整数因式分解）时间。这足以破解现代非对称密码学，

因为它基于整数分解或类似问题。（二）1996 年，Lov Grover 发表了数据库搜索算法。一个有趣的结果是 Grover 的算法能够找到时间复杂度为 $\sqrt{n}$ 的 n 位密钥。由于 Grover 算法或多或少可以暴力破解任何黑盒函数，我们需要重新考虑物联网中使用的对称密码学的安全性。

安全技术进化算法

为了解决优化问题，解决方案搜索空间对于简单的蛮力方法来说太大了。他们从生物学中汲取灵感，在生物学中，一组生物体（代表解决方案）是通过各种技术进化而来的，而进化法则（例如自然选择）适用。目标是找到评估解决方案质量的适应度函数的全局最优值。最流行的进化算法是遗传编程，主要是因为它不难实现并且可以为复杂问题提供良好的结果。进化算法可能并不总能找到最佳的全局解决方案。起始种群和进化操作（例如交叉和变异）的定义可以极大地影响算法找到全局最优值的能力。人工智能和机器学习是物联网安全的有前途的解决方案。它们可以检测网络上的异常活动、入侵和各种恶意软件活动。但是，必须对这些算法进行训练才能成功检测到攻击。这就是 GA 的用武之地。

当前的研究主要集中在使用 GA 优化神经网络参数或特征选择。张等人使用经过特殊修改的 GA 来设置深度信念网络的参数。Alqahtani 等人提出了另一个使用 GA 优化分类算法性能的例子。他们使用优化的极端梯度提升 (GXBoost) 创建了一个僵尸网络攻击分类器。GA 用于优化 GXBoost 模型的参数。当前使用 GA 的解决方案取得了非常好的结果。GA 使分类器更加高效和有效。但是，GA 对初始种群仍然很敏感，可能并不总能找到全局最优值。未来的研究可能会展示如何选择初始种群以及如何对其进行进化，以便以非常高的概率找到全局最优值。IoT 设备会生成包含大量数据点的大量数据。即使对于专家来说，也很难确定哪些参数对于检测有害活动很重要。GA 可用于从该数据中选择稍后可在分类器中使用的特征。张等人将普通 GA 与 GWO 算法相结合，从而消除了两种算法的缺点，所选特征用于训练 SVM 模型。使用该模型的入侵检测性能优于以前可用的方法。未来，我们可以期待机器学习在恶意软件和入侵检测中发挥重要作用。因此，提高这些算法的准确性很重要。由于将 GA 与 GWO 相结合提供了更好的性能，因此必须研究各种进化算法的其他组合，以找出哪个提供最好的结果。5G 网络的出现将进一步扩大新物联网设备的使用范围。如此大量的设备需要仔细管理频谱资源，以便它们能够保持良好的连接水平。其中一种管理技术是协作频谱感知，其中设备共享感知信息，一个控制节点决定频谱分配。在此配置中，发送虚假信息的恶意设备可能会导致网络性能严重下降。汗等人提出使用基于 GA 的软决策融合来缓解这些攻击。与传统方案相比，该方案实现了更好的性能和更低的错误概率。

结论

物联网应用程序的安全性正成为一个关键因素。由于物联网的广泛采用，控制论领域的攻击现在可以对现实世界产生重大影响。物联网设备，尤其是那些连接到云供应商的设备，也可能会带来隐私问题，泄露真实世界的私人数据。在物联网安全的未来趋势中，我们可以考虑许多安全选项。物联网设备与云之间的交互存在重大挑战，新兴的与区块链技术的集成增加了一个额外的层，因此需要对机密性、完整性和可用性等基本安全属性进行仔细的设计和考虑。但是，我们必须牢记跨越网络和物理边界的新兴威胁。潜在威胁评估中的一种新的不对称性来自量子计算领域。随着量子计算的快速发展，一些最常用的密码算法，如 RSA，将变得过时。在考虑应在更长的生命周期内保持安全的物理物联网设备时，我们应该考虑一种方法来准备迁移到量子安全算法。

我们将物联网的安全性视为控制论进化的范围：攻击者进化出新技术，然后通过新的防御机制进行缓解。进化技术和机器学习有很多安全应用，特别是在处理物联网设备产生的大量网络流量和日志方面。这是一个有趣的问题，这种类似于自然猎物 – 捕食者关系的控制论进化是否会导致新的人工智能技术的出现。

参考文献

[1] Iakovidis, Towards Personal Health Record: Current Situation, Obstacles and Trends in Inplementation of Electronic Healthcare Records in Europe, International Journal of Medical Informatics, 1998;52(1):105-115.

[2] E. Villalba, M.T. Arredondo, S. Guillen and E. Hoyo-Barbolla, A New Solution for A Heart Failure Monitoring System based on Wearable and Information Technologies, In International Workshop on Wearable and Implantable Body Sensor Networks 2006-BSN 2006.

[3] J. Zhou, X. Lin, X. Dong and Z. Cao, PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System, IEEE Transactions on Parallel and Distributed Systems, to appear.

[4] M. Li, S. Yu, K. Ren and W. Lou, Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings, SecureComm 2010, LNICST 2010;50:89-106.

[5] S. Yu, K. Ren and W. Lou, FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks, In IEEE Infocom 2009.

[6] F.W. Dillema and S. Lupetti, Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment, In HealthNet 2007.

[7] J. Zhou, Z. Cao, X. Dong, X. Lin and A. V. Vasilakos, Securing mHealthcare Social Networks: Challenges,

Countermeasures and Future Directions, IEEE Wireless Communications, 2013;20(4):12-21.

[8] J. Sun, X. Zhu, C. Zhang and Y. Fang, HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare, ICDCS 2011.

[9] Z. Liu, Z. Cao, Q. Huang, D.S. Wong and T.H. Yuen, Fully Secure Multiauthority Ciphertext-policy Attribute-based Encryption without Random Oracles, ESORICS 2011;278-297.

[10] A. Sahai, H. Seyalioglu and B. Waters, Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption, CRYPTO 2012;199-217.

[11] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, SAGE: A Strong Privacy-preserving Scheme against Global Eavesdropping for E-health Systems, IEEE Journal on Selected Areas in Communications, 2009;27(4):365-378.