密钥交换协议在工业物联网的应用研究

网络空间安全　赵正一

摘要

工业物联网（IIOT）的不断发展为工程师们提供了提高机器效率的巨大机会。尽管有了长足的发展，但是由于通信信道的不可信任性，许多行业管理者仍然害怕使用互联网来操作他们的机器。如果对实体进行有效的认证并且确保这一认证是可信任的，那么利用互联网管理工业运营平台就可以被广泛应用。传统的方案由于其固有的安全问题和其他的复杂性质，无法直接部署到资源受限的工业网络设备上，同时，用于学术研究的前沿方法由于效率低等问题也无法直接应用到工业物联网中。因此，本文研究了一个密钥交换协议来解决现有的弱点。本文通过使用各种加密方法，如哈希，以提供安全的相互身份验证和不同实体之间的密钥交换，从而限制未经授权的访问。通过实验验证，这一方法的性能和安全性与传统方法对比都有比较好的效果。

关键字：密钥交换协议；工业物联网

Abstract

The continuous development of the Industrial Internet of Things (IIOT) provides engineers with huge opportunities to improve machine efficiency. Despite the considerable development, many industry managers are still afraid of using the Internet to operate their machines due to the untrustworthy nature of communication channels. If the entity is effectively authenticated and the authentication is ensured to be trustworthy, then the use of the Internet to manage industrial operating platforms can be widely used. Traditional solutions cannot be directly deployed on resource-constrained industrial network equipment due to their inherent security issues and other complex properties. At the same time, cutting-edge methods for academic research cannot be directly applied to the industrial Internet of Things due to problems such as low efficiency. Therefore, this paper studies a

key exchange protocol to solve the existing weaknesses. This article uses various encryption methods, such as hashing, to provide secure mutual authentication and key exchange between different entities, thereby restricting unauthorized access. Through experimental verification, the performance and safety of this method have better results compared with traditional methods.

Keywords：Key Exchange Protocol; Industrial Internet of Things

目录

1 背景介绍

工业物联网（IIOT）又称工业 4.0。是工业革命的新时代，它利用传感器和执行器来提高生产和制造过程。IIOT 是工业发展的第四代。18 世纪第一代工业利用蒸汽发电为其工业生产资源。下一代变革发生在 1870 年的工业大发展，又称工业 2.0。工业领域通过电力和装配线的相互辅助工作，实现了又一次的人类解放双手运动。第二次工业革命的发展引起了工程师们对于工业发展的持续关注，工业发展的第三次进步（工业 3.0）将效率提升到了一个在现在看来是标准水平的地步。工业 3.0 介绍了计算机和可编程逻辑控制（PLC）的概念，这被认为是走向工业自动化的第一步。工业 4.0 的最新发展使用额外的基础设施，将工业过程与互联网连接起来，因此，也允许工程师们远程控制庞大的设备，同时也允许他们通过云连接访问及时信息 [1]。下图描绘了工业几次发展的重要技术和工业互联网的重要应用。

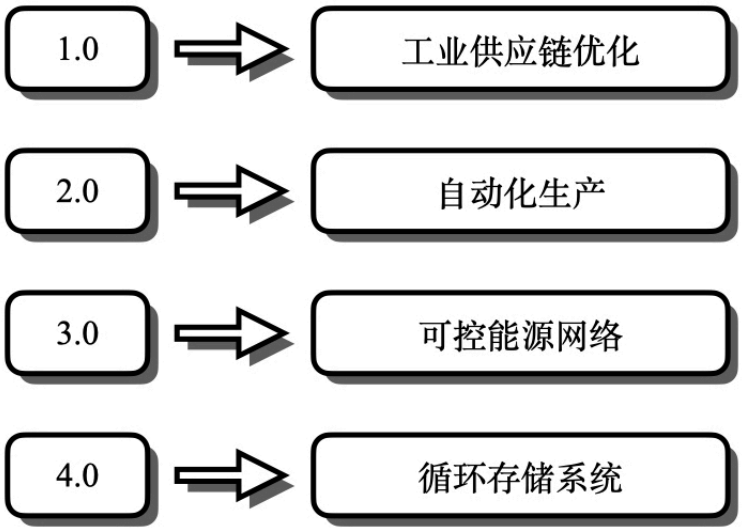

图 1: 工业物联网和重点应用领域的应用示例

但是即便是从常识我们也可以得知，工业物联网将许多传统实践融合到智能化或者是智能化的过程中时，上图的应用其实很少，例如仓库中的供应链优化、工业中的汽车制造、智能电网中的远程发电监控、废品回收和分类等。另一个促使产业主动改造其产业的原因是微电子行业的飞速发展以及信息和通信技术领域的长足进步。工业物联网发展背后的基本目标是无需人工干预的机器对机器（M2M）通信 [2]。M2M 通信利用各种设备，如射频识别（RFID）、传感器、移动设备和无线传感器网络（WSN），实现与其他设备的自动化和无缝连接 [3][4]。物联网使得工业机器能够将数据上传到云端进行快速分析和决策；从而消除了物理输入和分析的需要 [5]。

拥有大型制造单元的行业现在已经广泛采用了 IIOT，并已经开始使他们的机器实

现物联网。Tech Mahindra（TM）正在使用物联网来监控涂装和物流部门（将车辆从生产车间转移到制造车间）。在 TM 中使用物联网使工人能够随时随地查看工厂内设备的状态。此外，物联网加强了设备的工程能力，使得它可以减少从生产到制造的时间总量[6]。IIOT 的发展对整个工业所有者来说都是一个福音，因为他们可以远程可视操作机器，也可以远程监督员工 [7]。通过对机器不同时间的性能分析，可以更好的规划整个工业计划，以及规划现在正在进行的工业项目的进程 [8][9]。

现代物理网络和系统上频受攻击加剧了一种强烈的对物联网安全的焦虑心理，因为这种攻击会给包括使用者、服务提供商、开发人员和制造业人员造成大量损失 [10][11]。系统中未知的漏洞，如进程中断等，为混合攻击铺平了道路。网络攻击可能导致数据隐私和完整性的破坏。IIOT 中不充分或不适当的安全措施甚至会导致整个工业系统的崩溃。例如索契奥运会场馆的灯光、风扇、火灾探测器、供暖、通风和空调网络就是一整套物联网。但在 2008 年的突击检查中，发现 17823 个楼宇自动化控制网络设备和 78000 个监控和数据采集设备在没有进行任何安全保护的情况下直接在互联网上进行信息传输。在调查过程中，发现产生这一问题的主要原因是相互认证和密钥交换协议存在漏洞，导致攻击者利用网络资源进行攻击 [12]。

除此之外，福布斯还曾报道过一起攻击者利用恶意程序和通讯设备非法入侵工业物联网的事件。攻击者从公司的管理者手中非法接管了挖掘机、铲运机和起重机等设备。另一个事件是由一个安全分析公司报道的。根据他们的报道，小米公司生产的物联网电动滑板车甚至可以接受非法用户的控制命令，例如锁定、制动和加速等 [13]。

即便有这样多的安全问题已经被报道，保护 IIOT 免受入侵和网络攻击的方法仍然很少。其中之一是允许入侵发生，然后通过入侵检测系统进行检测 [15]，或者可以使用健壮的相互认证的安全的密钥交换协议来保证 IIOT 不受攻击 [16][17][18]。这里介绍一种新的方法可以应用到工业物联网中，这种方法叫基于相互认证的密钥交换协议。

基于相互认证的密钥交换协议通过安全的相互认证过程来保护对工业网络的未授权访问。、在相互认证和密钥交换过程中，数据的机密性和完整性都得到了保证。与传统的协议相比，这一方法显著优化了计算和通信过程。在这一方案中，身份验证服务器充当了可信工业网络站点和不可信外部世界之间的网关。因此，将用户视为一种潜在的威胁，并相应的验证身份。除了 IIOT，小型的家庭自动化系统也可以使用这一方法来进行验证。

2 相关工作

Esfahani 团队讨论了机器对机器（M2M）通信在 IIOT 网络实现中的作用 [2]。由于 IIOT 中的节点是资源受限的，因此作者只使用了异或和哈希操作来构建认证算法。作者认为，他们的方案提供了相互认证机制和完整的机密性。而且对重放攻击、模拟攻击和修改攻击也具有一定的防范作用。这一方案简单而安全，但通信、消息传输和计算开销比较大，这些消耗往往需要全部占用物联网的信道。因此这种方法是具有敏感资源受限设备网络的障碍。

Li 团队强调了物联网安全的需求和挑战 [3]。因为不安全的无线通信信道的开启和设备的资源限制，作者提出了一个三因素的用户认证协议来对抗合法性威胁。提出的协议具有效率高，抗重放攻击、模拟攻击等优点。Xu 团队 [19] 还公开了一种基于三因素机制的物联网多网关无线传感器网络认证方案。利用 ProVerif 机制进行形式化分析，证明该方案能抵抗多种潜在攻击。然而，这两种协议在实现三因素安全性的同时消耗了太多的能源。此外这些协议也消耗了大量的通信开销和计算开销。

Li 团队 [20] 讨论了无线传感器网络（WSN）和 iOtal 集成在一起执行某种任务的各种应用。作者提出一种新的安全协议的动机是传感器节点被非法用户访问，这种访问会对整个系统产生威胁。针对 IIOT 网络中存在的用户匿名性不足和其他安全漏洞，作者提出了一种基于椭圆去吸纳密码（ECC）的认证协议。他们提出的算法使用生物计量学和模糊提取器，在单向散列和异或方法上来实现了身份验证的目的，作者认为这种方法是安全的。经过分析，在 S3 网络模拟器中对该方案仿真分析，了解了这一方法在 WSN 物联网环境中的行为。尽管有这些优点，该方案仍然没有针对可能证明协议有效的潜在攻击进行测试（如中间人攻击）。由于不存在 nonce 机制和加密机制，这一方案在保证所有共享信息的信息及时性上也存在不足。

在物联网领域,有一些标准化工作为受限的设备提供认证的密钥交换 [21], 如 Diffie-Hellman 协议、Diffie-Hellman Over-COSE 协议 [22]。但可以发现，这些协议都存在一些错误，这些错误使得网络容易受到类似缓存的攻击从而限制了敏感网络（比如本文讨论的工业互联网）的应用。此外，工业物联网中的制造执行系统生成的时间敏感信息需要超低延迟的信息交换。因此，工业物联网网络寻求一种比 TCP/IP 层更好的框架 [23]。此外，研究人员认为 TCP/IP 最初是为了连接主机和有线网络而开发的；因此，最初设计的 TCP/IP 协议栈不足以满足物联网架构的需要 [24]。互联网工程任务组（IETF）和研究人员正在努力开发更好的替代方案。

递归的网络体系结构也是 TCP/IP 的一个很好的替代方案，因为它可以灵活地管理分层操作，而且不会中断实时通信。此外 RINA 声称比 TCP/IP 体系结构更安全，因为

它是一个保护层而不是一个协议。对现有体系结构的回顾解释了 IIOT 网络的 TCP/IP 的不完整性以及工业应用的开放标准的影戏那个。显然，TCP/IP 协议栈中简易的安全协议可能与开放体系结构不兼容，从而会产生漏洞，并对网络安全构成威胁。

最后，基于开放体系结构的 IIOT 网络安全协议的研究仍然在研究中，可以在有限的资源利用率下提供完整的安全解决方案。本文介绍的方法是专门针对基于开放体系结构的专用 IIOT 网络设计的。

3 模型介绍

3.1 模型概览

3.1.1 用户设计

在这里，用户可以是行业的管理者、所有者、经营者等。他们有权控制机器、从 IIOT 节点获取数据。用户可以使用任何数字设备（如计算机、笔记本电脑和移动终端设备）访问网络，这些设备能够与通信单元一起计算加密操作。所以，用户需要根据某种密钥交换协议来获得密钥，之后，用户再利用获得的密钥来进行对物联网设备的管理控制以及通信交流。

3.1.2 网关设计

网关为用户提供了连接 IIOT 网络的接口，网管不一定是通过同一个电源进行供电，而是取决于 IIOT 的使用情况。例如，部署在火山附近的工业网络，用于监测喷发和提取火山矿物，以此类推，网关从控制终端接受用户的部分安全密钥，再利用这些密钥验证请求的合法性。由于 IIOT 网络的所有节点都可以通过网关进行通信，因此任何漏洞都会破坏整个网络。

3.1.3 认证设计

认证服务器是一个受到管理者信任的实体单位，它的主要职责是验证网络的用户和其他设备。假设用户 id 离线存储在认证服务器中。用户从认证服务器请求安全验证。在验证后，该服务器向用户提供一个随机的秘密数字，用户根据这个数字再生成密钥。从而保证数据的完整性。

3.1.4 工业物联网节点设计

工业机器继承了传感器（运动、接近、真空和压力等）和低功耗收发器模块（如蓝牙、无线局域网等），以便提供即时访问来控制和监控工业基础设施。合法的用户，如工程师，工程所有者等通过网关与 IIOT 各节点进行通信。值得注意的是，这些协议往往是为了保护网络免受外部威胁。因此，只考虑了用户和网关之间的安全信息交互。

3.2 密钥交换协议

通过上述分析，可以看出：IIOT 的长足发展离不开先进的密钥交换协议。传统的密钥交换协议往往存在各种安全性风险，最前沿的密钥交换理论往往也因为性能效率无法保障而很难落地实用。下文将介绍一种基于神经网络的密钥交换理论，这一理论有高效快捷的特点，可以作为 IIOT 密钥交换协议发展的新思路。

3.2.1 传统的密钥交换协议

传统的密钥交换协议都是从 Diffie-Hellman 协议发展来的。双方都以私钥开始，并使用公共协议传输其加密的私钥，经过一些转换之后，这些私钥会生成一个公共密钥。Diffie-Hellman 密钥交换协议适用于生成公共密钥的典型协议。

所有已知的安全密钥交换协议都是用单向功能，这一功能通常是基于数论的，尤其是基于难以分解大质数的乘积。通常，N 位长度的密钥在两个通信方之间传输，并通过某种函数转换位公共密钥。密码学理论的基本问题之一就是：是否有可能建立一个不依赖于数论的安全密码系统；是否可以传输少于 N 比特长度的密钥；是否可以生成很长的密钥，可以直接用于一次性的流密码。

3.2.2 基于神经密码学的密钥交换协议

人工神经网络的诞生源自于真实的神经网络。人们通过研究神经元的特性发现，学习可以被看作是在神经元之间建立新的连接或者是对已经有的类似于连接的物质进行修改的过程。所以对于人工神经网络来说，就要建立起权重与输入相乘最终得到某个结果的等式。其中 W 是权重矩阵，X 是输入矩阵，o 是对应的输出。

神经网络是有多层神经元群组成的，由泰勒展开公式可知，一个特定的函数可以分解为多个非线性函数的加和，也可以说多个非线性函数加和的时候，可以模拟出某一个特定的函数。

$$f(x)=\frac{f(x_0)}{0!}+\frac{f^{'}(x_0)}{1!}(x-x_0)+...+\frac{f^{(n)}(x_0)}{n!}(x-x_0)^n+R_n(x) \tag{1}$$

基于这个想法，我们将输入的 x，匹配某个权重 w，再增添某个偏置 b，就可以得到对于输入 x 的线性函数。再将结果输入某个激活函数中，得到最终结果。

$$f(x) = sign(wx + b) \tag{2}$$

我们将由输入空间到输出空间的到的函数称为感知机。多个神经元以全连接形式层次相连，形成的网络称为前馈神经网络，也称为多层感知机（MLP），由泰勒展开可以得知，MLP 理论上可以模拟所有函数。其中模型为 $y = F(x)$，训练数据为 $D = x_i, y_i^n{}_{i=1}$，预测数据为 $\hat{y_i} = F(x_i)$，训练目标为 $\min(|\hat{y_i} - y_i|)$

神经密码学是通过通信双方构建相同的神经网络，并将这种固定的神经网络拓印至某种特殊的电路中。通过相互学习机制，连续进行沟通数据，通过多轮学习，最终达到双方的神经网络权重相等的结果。由于这种学习方式的黑盒特征，攻击者很难找到一种攻击方式来对神经密码学进行有效的攻击。通信双方可以将权重矩阵作为沟通的会话密钥，用于后续的信息交流。

树奇偶校验机（Tree Parity Machine, TPM）由 K 个隐藏层单元组成，其输入向量是 X，初始权重是 W，输出单元是 σ_k。

$$X \subset x_{ij} \in \{-L, \cdots, 0, \cdots, +L\}$$
$$W \subset w_{ij} \in \{-L, \cdots, 0, \cdots, +L\}$$

$$\sigma_k = \text{sign}(\sum_{j=1}^{N} w_{ij} x_{ij}) \tag{3}$$

其中，sign(·) 函数代表取自变量的数学符号，用来表示自变量的正负形，所以有：

$$\text{sign}(\cdot) \in \{-1, 0, +1\}$$

TPM 最终的输出为 τ：

$$\tau^{A/B} = \prod_{k=1}^{K} \sigma_k^{A/B} \tag{4}$$

TPM 的构建是一个动态的过程，通过多轮对比最终构建并同步好彼此的神经网络。其构建流程如下

Algorithm 1 TPM 双方同步按照以下流程执行

1: 随机初始化权重矩阵 $w_{ij}^{A/B}$;
2: **while** $w_{ij}^{A} \neq w_{ij}^{B}$ **do**
3: 随机生成相同的输入矩阵 x_{ij};
4: 计算 $\sigma_i^{A/B}$ 和 $\tau^{A/B}$ 的结果;
5: **for all** τ^A 和 τ^B，比较他们的结果，并按照如下结果继续执行 **do**
6: $\tau^A = \tau^B$: 更新彼此的权重;
7: $\tau^A \neq \tau^B$: 回到第三步;
8: **end for**
9: **end while**

TPM 的学习规则如上述流程图所示，在进行到第六步的时候，需要按照特定的规则来更新神经网络的权重，通常我们会使用以下三种更新方法

1. Hebbian 算法

$$w_i^+ = g(w_i + \sigma_i x_i \theta(\sigma_i, \tau^A)\theta(\tau^A, \tau^B)) \tag{5}$$

2. Anti-Hebbian 算法

$$w_i^+ = g(w_i - \sigma_i x_i \theta(\sigma_i, \tau^A)\theta(\tau^A, \tau^B)) \tag{6}$$

3. Random walk 算法

$$w_i^+ = g(w_i + x_i \theta(\sigma_i, \tau^A)\theta(\tau^A, \tau^B)) \tag{7}$$

其中，$\theta(x, y)$ 代表了 x 和 y 的相等关系，g 函数表示某种运算法则使得运算后的结果仍然保持在原运算空间内:

$$\theta(x, y) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases} \tag{8}$$

4 总结和展望

本文分析了工业物联网在密钥交换协议这一痛点上发展的现状以及主流的研究思路。通过几个案例说明了工业物联网面临的几点问题，以及如何考虑设计一个完备的工业物联网密钥交换协议。同时，本文给出了一个高效快捷的工业物联网密钥交换协议新思路——神经密码学。通过神经网络和相互学习方法的引入，通信双方能够更快的构建神经网络，协商会话密钥。但是这一技术仍然有很多问题需要研究。一是如何将其拓印

至电路板上以供后续使用；二是如何保证会话交流过程的效率。但是神经密码学在密钥交换协议领域的探索仍然值得肯定，在 IIOT 上的应用也因为局域网内交流变得更加广泛。

参考文献

[1] Ozturk H M. Technological Developments: Industry 4.0 and Its Effect on the Tourism Sector[M]//Research Anthology on Cross-Industry Challenges of Industry 4.0. IGI Global, 2021: 1464-1487.

[2] Esfahani, A.; Mantas, G.; Matischek, R.; Saghezchi, F.B.; Rodriguez, J.; Bicaku, A.; Maksuti, S.; Tauber, M.;Schmittner, C.; Bastos, J. A lightweight authentication mechanism, for M2M communication in industrialIoT environment.IEEE Internet Things J.2017,6, 288–296.

[3] Li, X.; Peng, J.; Niu, J.; Liao, J.; Choo, K.K.R. A robust and energy efficient authentication protocol forindustrial internet of things.IEEE Internet Things J.2018,5, 1606–1615

[4] Xu, L.D.; He, W.; Li, S. Internet of things in industry: A survey.IEEE Trans. Ind. Inform.2014,10, 2233–2243.

[5] Xiong, H.; Mei, Q.; Zhao, Y. Efficient and provably secure certificateless parallel key-insulated signaturewithout pairing for IIoT environments.IEEE Syst. J.2019,5, 310–320.

[6] IoT for Manufacturing.Available online.

[7] Humphreys, D. Mining productivity and the fourth industrial revolution.Miner. Econ.2020,33, 115–125.

[8] Chi, P.W.; Wang. M.H. A lightweight compound defence framework against injection attacks on IIoT.In Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung,Taiwan, 10–13 December 2018; pp. 1–8.

[9] Mumtaz, S.; Alsohaily, A.; Pang, Z.; Rayes, A.; Tsang, K.F.; Rodriguez, J. Massive internet of things forindustrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation.IEEE Ind. Electron. Mag.2017,11, 28–33.

[10] Nakamura, E.T.; Ribeiro, S.L. A privacy, security, safety, resilience and reliability focused risk assessmentmethodology for IIoT system. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao,Spain, 4–7 June 2018; pp. 1–6.

[11] Panchal, A.C.; Khadse, V.M.; Mahalle, P.N. Security issues in IIoT: A comprehensive survey of attacks onIIoT and its countermeasures. In Proceedings of the 2018 IEEE Global

Conference on Wireless Computingand Networking (GCWCN), Lonavala, India, 23–24 November 2018; pp. 124–130.

[12] Zheng, Z.; Reddy, A.L.N. Safeguarding building automation networks: THE-driven anomaly detector basedon traffic analysis. In Proceedings of the 26th International Conference on Computer Communication andNetworks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017; pp. 1–11.

[13] Sureshkanth, N.V.; Wijewickrama, R.; Maiti, A.; Jadliwala, M. Security and privacy challenges in upcomingintelligent urban micromobility transportation systems. In Proceedings of the AutoSec ’20: Proceedings of theSecond ACM Workshop on Automotive and Aerial Vehicle Security, New Orleans, LA, USA, 18 March 2020;pp. 31–35.

[14] Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things:Vulnerabilities, attacks,and countermeasures.IEEE Commun. Surv. Tutor.2019,22, 616–644.

[15] Butun, I.; Österberg, P. Detecting intrusions in cyber-physical systems of smart cities: Challenges anddirections. InSecure Cyber-Physical Systems for Smart Cities; IGI Global: Hershey, PA, USA, 2019; pp. 74–102.

[16] Aydogan, E.; Yilmaz, S.; Sen, S.; Butun, I.; Forsström, S.; Gidlund, M. A central intrusion detection system forRPL-based Industrial Internet of Things. In Proceedings of the 2019 15th IEEE International Workshop onFactory Communication Systems (WFCS), Sundsvall, Sweden, 27–29 May 2019; pp. 1–5.

[17] Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges,opportunities, and directions.IEEE Trans. Ind. Electron.2018,14, 4724–4734.

[18] Taher, B.H.; Jiang, S.; Yassin, A.A.; Lu, H. Low-overhead remote user authentication protocol for IoT basedon a fuzzy extractor and feature extraction.IEEE Access2019,7, 148950–148966.

[19] Xu, L.; Wu, F. A lightweight authentication scheme for multi gateway wireless sensor network under IoTconception.Arab. J. Sci. Eng.2019,44, 3977–3993.

[20] Li, X.; Niu, J.; Bhuiyan, M.Z.A.; Wu, F.; Karuppiah, M.; Kumari, S. A robust ecc-based provable secureauthentication protocol with privacy preserving for industrial internet of things.IEEE Trans. Ind. Electron.2018,14, 3599–3609

[21] Vucinic, M.; Selander, G.; Mattsson, J.; Garcia, D. Requirements for a Lightweight AKE for OSCORE.

[22] Selander, G.; Mattsson, J.; Palombini, F. Ephemeral Diffie-Hellman Over COSE (EDHOC).

[23] Wireless IoT Protocols: Breaking Down the Network Stack|BehrTech Blog

[24] Challenges in IoT Networking via TCP/IP Architecture