Computer Science and Application 计算机科学与应用, 2018, 8(3), 323-327
Published Online March 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.83037

Hans汉斯

An Industrial Internet of Things Security Certification Mechanism and Analysis

Yong Gan[1*], Qunhui Wu[2]

[1]Turkmenistan Branch of China Petroleum Transportation Co., Ltd., Urumqi Xinjiang
[2]Shanghai HEST Environmental Technology Co., Ltd., Shanghai
Email: *ganyong@cnpcca.com, hest2016@126.com

Received: Mar. 10th, 2018; accepted: Mar. 21st, 2018; published: Mar. 28th, 2018

Abstract

At present, the security issue of IoT has become the focus of attention. Especially in the development of industrial IoT security protection and evaluation, there is no systematic security protection system in many countries. There is also a lack of application in various fields of industrial IoT general and specific safety standards and specifications. Therefore, establishing a comprehensive security defense system and developing a series of industrial IoT security products and formulating a series of evaluation standards for networking of industrial networks not only ensure the daily life and safety production activities of the people of the factory, but also provide the basis for social stability. The security of facilities and strategic information is a guarantee of security and is of strategic importance to national security. Therefore, a reliable industrial Internet of Things security certification mechanism is needed and the potential risks of IoT are analyzed to reduce the emergence of problems and the loss of entities.

Keywords

Industrial Internet of Things, Security Certification

一种工业物联网安全认证机制及分析

甘　勇[1*]，邬群辉[2]

[1]中国石油运输有限公司土库曼斯坦分公司，新疆 乌鲁木齐
[2]上海昊长环保科技有限公司，上海
Email: *ganyong@cnpcca.com, hest2016@126.com

收稿日期：2018年3月10日；录用日期：2018年3月21日；发布日期：2018年3月28日

*第一作者。

文章引用: 甘勇, 邬群辉. 一种工业物联网安全认证机制及分析[J]. 计算机科学与应用, 2018, 8(3): 323-327.
DOI: 10.12677/csa.2018.83037

摘　要

目前物联网的安全问题已经成为大家关注的焦点问题，尤其在工业物联网的安全防护和评估的发展方面，很多国家尚无系统化的安全防护体系，也缺乏适用于工业物联网在各领域的通用和专用安全标准和规范。因此建立全面的安全防御体系，并开发一系列的工业物联网安全防护产品，以及制定针对工业物联网的评估系列标准，不仅保证人民的日常生活、安全生产活动，而且为社会的稳定、基础设施和战略信息的安全提供了保障，对国家安全都具有重要战略意义。因此需要一种可靠的工业物联网安全认证机制以及分析潜在的物联网的安全风险来减少问题的出现和实体的损失。

关键词

工业物联网，安全认证

1. 引言

工业物联网的三个特征是全面感知、可靠传输、智能处理，系统通过网络通信协议协调各模块之间的操作时序，从而实现整个系统的自我感知和判断、自我调节和控制等。而本文提出的方法主要是针对于传输层。可靠传输层保证感知数据在异构网络中的可靠传输，其功能相当于 TCP/IP 结构中的网络层和传输层，包括信息传输和识别、数据存储、数据压缩和恢复。构成该层的要素包括网络基础设施、通信协议以及通信协议间的协调机制。可靠传输层的安全主要是传统互联网、移动网、专业网、三网融合通信平台等基础性网络的安全，其可能受到的安全威胁有：垃圾数据传播(垃圾邮件、病毒等)；假冒攻击、中间人攻击等(存在于所有类型的网络)；DDOS 攻击(来源于互联网，可扩展到移动和无线网)；跨异构网络的攻击(互联网、移动网等互联情况下)；新型针对三网融合通信平台的攻击等。

在实际的工业物联网项目应用过程中，通常会采用外部网络与末梢网络裁旬旬的双向认证技术来实现网络与实体之间的互信机制，这部分技术主要在传输层实现，包括安全密码算法(对称和公钥密码)的设休密钥管理、栽点对栽点机密性、端对端机密性、强认证协议、密码算法和密码协议标准化等内容。但是，在现有的技术环境下，双向认证还必须考虑以下两个现实问题：1) 末梢网络资源通常是非常有限的，认证过程中必须充分地认识到这点，因而认证机制所涉及的计算量和通信开销必须尽可能小；2) 对外部网络而言，其连接的末梢网络数量巨大，且结构不尽相同，要在如此复杂的环境下建立一个高效的识别机制，以区分这些网络及其内部栽点，并赋予唯一的身份标识，需要完善的解决方案。

2. 基于共享秘密 Hash 函数的 RFID 双向认证协议

在物联网中，RFID 技术是一种通过无线电波远距离识别物体和信息传输的技术。RFID 技术已经在生活中的多个领域得到了普及并充分的突显出了它的强大的实用价值。但是，由于 RFID 系统数据传输标签的独特性，想要设计出安全高效的 RFID 安全认证方案，成为了 RFID 安全协议研究领域的一大挑战。在工业物联网中，RFID 技术引用非常广泛，针对 RFID 系统不停呈现出来的各式各样的安全与隐私问题，通过总结前人提出来的安全协议的设计理念，提出了一种改进的 RFID 系统解决方案，并重点介绍了新

协议的初始化条件、基本原理和认证流程。通过建立安全性分析模型，分析了新协议是如何解决 RFID 系统中普遍存在的安全问题[1] [2] [3]。

在工业物联网中，实体身份识别和认证技术会利用到 RFID 射频识别和双向认证技术。而本文中提出的新协议就是针对于 RFID 技术的安全缺陷和实现实体和网络之间互信机制的双向认证协议。

2.1. 安全认证协议的设计

通过总结前人提出来的安全协议的设计理念，提出了一种改进的 RFID 系统解决方案，并重点介绍了新协议的初始化条件、基本原理和认证流程。通过建立安全性分析模型，分析了新协议是如何解决 RFID 系统中普遍存在的安全问题[4] [5] [6] [7]。

2.1.1. 初始条件与设计原理

数据传输标签存储 ID、S 和 H(ID||S)，认证前数据传输标签状态为锁定状态。后台服务器存储所有数据传输标签数值对(ID, S, H(ID||S))，并且在后台服务器中嵌入随机数生成器。其中 R 是服务器产生的随机数，ID 是数据传输标签的标识，S 是系统运作前预先设置的秘密值，H 是预先定义的哈希函数，Tag 表示标签，Reader 表示读写器，S 和 H(ID||S)会随着随机数的不同而不断更新。不考虑协议中设计的 Hash 函数本身的缺陷[8] [9]。

改进的认证方案设计原理见图 1 所示。

2.1.2. 认证流程

安全协议认证流程如下：

1) 后台数据库将生成的 R 响应给 RFID 读取器。

2) RFID 读取器向数据传输标签发出 Query 认证请求。

3) 数据传输标签依据 H 函数计算 H(ID||R||S)，然后将运算结果和 H(ID||S)通过 RFID 读取器响应给后台服务器。

4) 后端数据库依据接收到的数值，检索系统文档是否存在一组(ID_j, S, $H(ID_j||S)$)数据，其中 $H(ID_j||S)$ 与 H(ID||S)相同，若相同，则依据该组的 ID_j 和 S 计算 $H(ID_j||R||S)$。然后校验 $H(ID_j||R||S) = H(ID||R||S)$，如果相等，则数据传输标签认证通过并进行下一步运作，否则数据传输标签认证失败。

5) 后端数据库计算 $S^{DB} = H(R||S)$、$H(ID||S^{DB})$和 $H(ID_j||R||S^{DB})$，后端数据库使用 S^{DB} 和 $H(ID||S^{DB})$替换相应的 S 和 H(ID||S)，并通过 RFID 读取器将 $H(ID_j||R||S^{DB})$转发给数据传输标签。

6) 数据传输标签计算 $S^T = H(R||S)$、$H(ID||S^T)$和 $H(ID||R||S^T)$，并判断 $H(ID||R||S^T)$与接收到的数据 $H(ID_j||R||S^{DB})$是否相等，若相等，则 RFID 读取器认证成功，系统标签使用 S^T 和 $H(ID||S^T)$替换相应的 S 和 H(ID||S)，否则 RFID 读取器认证失败。

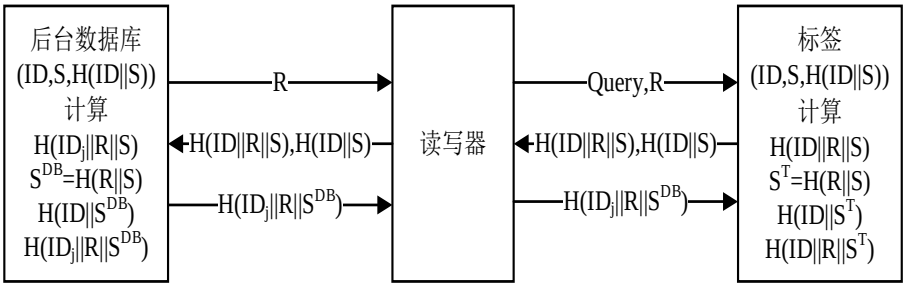

Figure 1. Security authentication protocol design principles
图 1. 安全认证协议的设计原理

2.2. 协议的安全性分析

1) 双向认证。通过后端数据库比较 $H(ID_j||R||S)$和 $H(ID||R||S)$是否相等、数据传输标签比较 $H(ID||R||S^T)$和 $H(ID_j||R||S^{DB})$是否相等，实现了 RFID 系统合法身份的双向认证。

2) 向前安全。由于 R、数据传输标签秘密值 S 的可变性和 H 函数的不可逆性，纵然非法用户取来了 $H(ID||R||S)$和 $H(ID||S)$的值，也无法追溯到系统数据传输标签以前相关的认证响应记录。

3) 防位置跟踪。由于 R、数据传输标签秘密值 S 的可变性、更新的，因此系统 Tag 每次回答 RFID 读取器询问的数值 $H(ID||R||S)$和 $H(ID||S)$也是不同的，可以防止非法使用者依据 RFID 系统 Tag 的特定响应记录而进行的定位追踪。

4) 防重传攻击。每次的秘密数 S 是变化的，攻击者即使窃听了合法 RFID 读取器前一次发送的 $H(ID_j||R||S^{DB})$、合法数据传输标签前一次发送的 $H(ID||S)$和 $H(ID||R||S)$，也无法再次模拟出 $H(ID_j||R||S^{DB})$的值或 $H(ID||S)$和 $H(ID||R||S)$的值，有效的防止了重传攻击。

5) 防窃听与非法读取。数据传输标签 ID 在非安全信道传播时经过 Hash 函数的加密处理，所以非法用户无法窃听标签的真实 ID。

6) 防假冒攻击。由于在每次认证过程完成后，都对数据传输标签共享秘密值 S 和服务器共享秘密值 S 进行了更新，攻击者无法伪造秘密值 S。系统合法 Tag 响应的 $H(ID||S)$和 $H(ID||R||S)$与攻击者伪造的数据传输标签响应不同，因此无法通过系统合法 RFID 读取器认证。系统合法 RFID 读取器响应的 $H(ID_j||R||S^{DB})$与攻击者伪造的 RFID 读取器响应不同，因此无法通过系统 Tag 的合法认证。

7) 不可分辨性。由于认证过程中加入了随机数、秘密值和 Hash 函数这些元素，使得非法使用者无法通过获取多个合法 Tag 的响应辨别出某一个系统 Tag 的响应，也无法通过获取同一个 Tag 的多次响应辨别出该响应 Tag 的某一次响应，达到了不可分辨性的安全目标。

8) 拒绝服务。由于后台数据库和标签中的隐私数据只有通过安全认证后才会进行数据更新，假如合法标签正在进行安全认证，在完成之前被停止了，那么此时后台数据库和系统 Tag 中的数值记录也没有任何更替，可满足下一次或诸多次的认证，达到了抵制拒绝不法服务的安全目标。

2.3. 基于共享秘密 Hash 函数的 RFID 双向认证协议的工业物联网

本文提出的新协议，是在典型的安全认证机制基础之上设计出来的，新协议有效地解决了 RFID 系统的双向认证问题，并且在新协议中加入了 Hash 函数[10]、共享秘密值和随机数这 3 个元素，加强了新协议的防位置、跟踪、重放攻击、假冒攻击、窃听的抵抗能力。基于前面第三节提出的安全性分析，总体上来说，本文设计的新协议基本上解决了典型的 RFID 隐私保护机制存在的各种各样的安全问题，具有较好的安全性能[11]。针对于工业物联网，新协议主要解决了两个问题。第一个就是双向认证的问题，新协议不但要认证服务器端而且还要认证标签端。第二个就是 RFID 技术的安全问题，新协议通过利用变化的共享秘密值以及变化的随机数保证了用户每次在识别身份时确保了用户身份唯一性。从而保证了用户的数据安全和隐私。此外其次就是数据在网络传输的安全性，为了解决互联网中通信数据隐私问题，我们需要对传输的数据进行加密，本文采用采用 MD5 算法[12]进行数据加密。

3. 小结

本文介绍了工业物联网的安全风险分析和关键防护技术，并通过总结前人提出来的安全协议的设计理念，提出了一种改进的工业物联网 RFID 系统解决方案，并重点介绍了新协议的初始化条件、基本原理和认证流程。通过建立安全性分析模型，分析了新协议是如何解决 RFID 系统中普遍存在的安全问题。在工业物联网中，RFID 技术安全与隐私和 RFID 技术的应用领域是紧密相关的，不同的应用领域关联了

不同的 RFID 安全等级。对于有些领域如工业安全生产管理，控制安全要求较高，那么需要将协议的安全性放在第一位。所以在充分考虑系统设计成本的基础之上，设计出机制简单、安全高效的加密认证算法成为了研究的热点。

参考文献

[1] Khattab, A., Jeddi, Z., Amini, E., *et al.* (2017) RFID Security Threats and Basic Solutions. RFID Security. Springer International Publishing, Berlin, 27-41.

[2] Khattab, A., Jeddi, Z., Amini, E., *et al.* (2017) Introduction to RFID. RFID Security. Springer International Publishing, Berlin, 3-26.

[3] 张兴, 韩冬, 曹光辉, 贾旭. 基于 PRESENT 算法的 RFID 安全认证协议[J]. 通信学报, 2015(S1): 65-74.

[4] Ha, J.C., Ha, J.H., Moon, S.J., *et al.* (2007) LRMAP: Lightweight and Resynchronous Mutual Authentication Protocol for RFID System. Ubiquitous Convergence Technology. Springer, Berlin Heidelberg, 80-89.

[5] Wang, S., Liu, S. and Chen, D. (2015) Security Analysis and Improvement on Two RFID Authentication Protocols. *Wireless Personal Communications*, **82**, 21-33. https://doi.org/10.1007/s11277-014-2189-x

[6] Abughazalah, S., Markantonakis, K. and Mayes, K. (2015) Secure Improved Cloud-Based RFID Authentication Protocol. Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Springer International Publishing, Berlin, 147-164.

[7] Desai, N. and Das, M.L. (2015) On the Security of RFID Authentication Protocols. *IEEE International Conference on Electronics, Computing and Communication Technologies* (*CONECCT*), Bangalore, 10-11 July 2015, 1-5. https://doi.org/10.1109/CONECCT.2015.7383895

[8] Sarma, S.E., Weis, S.A. and Engels, D. (2003) Radio-Frequency-Identification Security Risks and Challenges. *Cryptobytes*, **6**, 93-98.

[9] Sarma, S.E., Weis, S.A. and Engels, D.W. (2002) RFID Systems and Security and Privacy Implications. International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin Heidelberg, 454-469.

[10] Henrici, D. and Muller, P. (2004) Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers. *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, Orlando, FL, 14-17 March 2004, 149-153.

[11] 谢磊, 殷亚凤, 陈曦, 陆桑璐, 陈道蓄. RFID 数据管理: 算法、协议与性能评测[J]. 计算机学报, 2013, 36(3): 457-470.

[12] Kuznetsov, A.A. (2015) Parallel Algorithm for MD5 Collision Attack. *Program Systems Theory & Applications*, **61**, 61-72.