技术研究

基于物联网安全的信任机制构建研究

孟 丹

(山西省霍州煤电集团煤炭运销部，山西 霍州 031400)

摘 要： 随着社会经济和科技的不断发展，信息化水平也不断提高，物联网逐渐成为信息技术的重要组成部分，人们对于物联网的关注也越来越重视。与此同时，物联网的安全和对物联网的信任机制建设就显得格外重要，这对于节约能源，实现社会的节能发展意义重大。主要介绍物联网和物联网存在的安全问题，以及基于物联网安全的信任机制的构建，以实现能源节约，促进节约型社会建设。

关键词： 物联网；节能；物联网信任机制

中图分类号： TP393.4 **文献标识码：** A **文章编号：** 2095-0802-(2014)01-0159-02

On the Construction of Trust Mechanism Based on the Security of Internet of Things

MENG Dan

(Coal Transportation and Marketing Department of Huozhou Coal Electricity Group of Shanxi Province, Huozhou 031400, Shanxi, China)

Abstract: With the continuous development of social economy and science and technology, the level of informatization is also rising, and internet of things gradually becomes an important part of information technology, to which people are paying more and more attention. Meanwhile, the security and the construction of trust mechanism of internet of things are particularly important, which is of great significance to realize energy conservation and the social energy-saving development. Mainly introduces the internet of things, the security problems of it, and the construction of trust mechanism based on the security of internet of things to realize energy conservation and promote the construction of conservation-oriented society.

Key words: internet of things；energy conservation；trust mechanism of internet of things

0 引言

随着科技水平的不断提高，物联网的发展非常迅速，在现代化的 21 世纪，物联网受到极大的欢迎，但是在享受便利的同时，也要注意物联网的安全问题，所以加快物联网安全的信任机制的构建刻不容缓。

1 物联网

1.1 物联网的含义

物联网是在互联网的概念上提出来的，从字面的意思来理解就是在物质的基础建立互相连接的信息网络，具体来说，物联网有两层含义：a) 物联网是在互联网基础上建立的，要依靠互联网技术来运行，所以物联网的核心技术仍然是互联网的技术，它是互联网技术的一个延伸；b) 物联网相对于互联网技术有了很大的突破，不再是局限于虚拟的数据进行连接，而是对于物品和物品之间的信息连接与传递，具有真实物体之间的通讯[1]。物联网之间的信息的传递主要通过射频识别 (RFID) 、红外感应器、全球定位系统、激光扫描器等信息传感设备，按照预先制定的要求，将现实中的物品和互联网建立一定的连接，把物品的信息通过仪器输入，然后完成信息的传递与交流，实现物体的智能化识别，还用于一些物体的跟踪定位和监控等，为生活、企业的管理等提供了巨大的方便，可以算是一种新型的网络。

1.2 物联网的特点

物联网终端的多样化，物联网是在互联网基础上开发和延伸得到的，它不仅仅局限在电脑的领域上，还在我们日常生活中处处可见，小到一个锁或杯子，开发物联网的技术就是要把我们生活中各种各样的东西相互联系起来，无论是有生命的东西还是没有生命的东西，都包含在物联网内，物联网这种终端的多样性是互联网远远达不到的。

物联网感知的自动化，物联网感知是在各种各样的物体上安装感应芯片，这样物品就会有感知，举几个例子来说：在我们喝茶时，杯子可以感知水的温度，以便

收稿日期：2013-11-24

作者简介：孟 丹，1982 年生，男，河南许昌人，2007 年毕业于西安电子科技大学通信工程专业，助理工程师。

提示我们水是否可以泡开茶；给婴儿洗澡时，在浴盆里放置微型感应芯片，可以感应水温，以保证婴儿的舒适；在我们出门时，提醒我们锁门；在乘坐公交车时，刷卡系统在我们刷卡时出现提示音等等，其实，物联网就是实现了物体与物体之间的交流，通过一定的设备感知对方的变化，并做出相应反映的网络技术。

2 物联网存在的安全问题

物联网给我们带来极大方便的同时，也存在一定的安全问题，主要现在以下几个方面。

2.1 感知层面的安全问题

物联网的感知是在物体中植入微型的芯片，这样，物体内植入芯片不仅仅是能被拥有它的主人所识别，也能被其他的人所识别和感知，这样就会造成信息安全的威胁：a) 对个人隐私造成泄漏。射频识别技术在物联网中应用时，是将感知芯片植入到物体内部，人的肉眼是观察不到的，这就会导致使用者并不知道物体里面嵌入了感知芯片，造成所有者的隐私信息被他人读取、监控的情况，严重侵害了个人的隐私权；b) 造成疑似的攻击，因为智能传感器终端，射频识别技术是暴露在攻击者前的，而且传输信息依靠的是无网络线路传输方式，这就会引起极大的疑似攻击，威胁着传感器节点之间的协调工作；c) 计算机病毒和黑客的攻击，物联网技术是建立在互联网技术之上的一种技术，我们都知道互联网很容易感染计算机病毒和遭到黑客的攻击，基于物联网是在无线网络条件下进行的信息传输，给计算机和黑客造成了很大的机会，一旦计算机病毒和黑客入侵物联网成功，它的传播速度也就非常迅速，相对于互联网来说，病毒对于物联网具有更大的威胁性和破坏性[2]；d) 大量的数据请求导致拒绝服务，对于计算机病毒和黑客攻击的入口大多会出现在感知层与核心网络连接部位，根据物联网的特点我们知道，物联网的节点比较多，而且节点的分布相对来说比较集中，这样在数据的传播时，就会集中于节点处，造成节点崩溃，发生节点堵塞，从而不会继续为数据的传输服务；e) 信息的安全。由于在物联网中数据的信息比较多，节点又比较单一，这样处理信息的安全性能就会比较低，并且数据的信息量非常大，对于收到的信息在处理时没有统一的处理标准，所以，物联网不能提供统一的安全保护策略，物联网不仅仅在生活中得到广泛应用，还在国家的公共事务以及一些秘密工作中有所应用，所以，信息的安全影响非常巨大，它的作用不容忽视。

2.2 网络层的安全问题

物联网是建立在互联网基础上的，存在网络层的安全问题，主要体现在以下的几个方面：a) 网络环境的不确定性。物体的分布非常广泛和复杂，所以数据的传输就会非常复杂，由于在传输的过程中，数据之间发生着冲突和交汇，在这种网络环境下，数据之间存在着冗余和互补性，由于网络环境不是固定不变的，造成的安全问题也非常复杂；b) 传输层的安全问题。物联网的应用范围更加广泛，这就要求物联网具有极高的安全保障，拥有更高的可控、可信以及可知的能力，对于现在的物联网传输而言，由于是无线网络的传输，在传输的过程中没有信息的安全保护措施，造成了传输层的安全问题。

2.3 应用层的安全问题

物联网是一种集成应用和解析服务综合的技术，具有非常强大的信息处理功能和信息融合功能，在物流的监控、临床的监控、智能化的交通监控、家居智能化都发挥着巨大的作用，在这些应用层上，存在着很多安全问题，对于物联网的安全性和可靠性提出了巨大的挑战。

3 基于物联网安全的信任机制的构建

物联网的安全是一个值得大家重视和研究的问题，在现在诸多物联网安全问题下，保证物联网的安全是急需解决的问题，建立物联网安全的信任机制是靠几个方面来实现的——物联网的加密机制、物联网中的认证机制以及物联网立法的保护，这几个方面的实现代表着物联网安全的信任机制构建的实现。

3.1 物联网的加密机制

传统的网络层加密机制是逐跳加密，就是在信息的传送过程中，信息的传输是有一定加密的，但是，网络层加密是在整个传输的线路中加密的，要保证物联网的安全的性能，不仅仅要在传输的过程中要加密，还要在数据经过的每个节点上进行加密和解密，也就是说每个节点的密钥都是明文的，这是对于传输层的加密；对于业务层的加密是终端到终端的加密，就是只有在信息传输的终端才是明文的，但是在传输的过程中和在传输过程中的节点上都是密文，是加密的，不进行解密的过程，在物联网中网络与业务之间是有一定联系的，它们有各自的特点，要合理对逐跳加密和端口与端口加密进行选择[3]。

对于逐跳加密来说，它可以针对性地对一些链条进行加密，对于保护性较高的传输进行强化加密，由于逐跳加密是在网络层中应用的，所以，逐跳加密使用的业务更加广泛，可以实现不同物联网业务平台上的安全管理，有利于做到安全机制对业务透明度的提高，提高可信度。

对于端口到端口的加密可以根据不同的业务形式来选择不同的安全策略，对于安全性要求比较高的业务采取高保密性措施，对于低安全性的业务选取低保密性措施，比如上面所列举的茶杯对于水温的检测就不需要高的安全性，而对于政府的业务就需要安全性较高的策略，但是端口与端口加密有缺陷，就是不能根据消息的传输来进行有目的性的保护，因为它在每个节点之间没有加密和解密的保护，很容易受到通讯过程中恶意攻

（下转 165 页）

各矿使用的锚固剂主要有 CK2340 和 Z2388，顶锚杆接近于全长锚固，非常不利于锚杆预应力的扩散，有待改进。同样，帮锚杆和顶锚索都存在锚固长度过长不利于预紧力扩散的问题。

4.2.3　螺母螺纹及预紧力施加

在井下调研发现，锚杆螺母直接压在托板上，螺母和托板之间的摩擦系数较大，不利于锚杆螺母预紧力矩转化为杆体的预紧力，具体摩擦系数即转化关系有待下一步实验室试验来确定。

天地公司对锚杆螺母预紧力矩与杆体的预紧力的转化关系进行了深入研究，开发了专门装置，进行了大量实验，最终得到锚杆杆尾的合理结构为带球窝的拱形托板、调心球垫、减摩垫圈和螺母。调心球垫为 1010 尼龙减摩效果最好，能最大限度地将预紧扭矩转化为杆体预紧力。

4.2.4　锚杆施工角度

a) 当顶板角锚杆垂直布置时，角锚杆与中部锚杆形成的有效压应力区相互连接与叠加，在顶板形成厚度较大、分布比较均匀的压应力区，覆盖了锚固区的大多数面积，锚杆预应力扩散与叠加效果最好；b) 随着顶板角锚杆角度增加，角锚杆形成的有效压应力区与中部锚杆形成的有效压应力区逐步分离，叠加区域越来越小。当顶板角锚杆角度达到 15°，两个压应力区明显分离。继续加大角锚杆角度，角锚杆与中部锚杆的压应力区分开得更远，成为彼此独立的支护单元，锚杆支护的整体作用受到严重影响；c) 顶板角锚杆角度越大，锚杆预应力形成的有效压应力区越小。

由此可见，在考虑锚杆预应力的条件下，在近水平煤层巷道中，顶板角锚杆最好垂直布置。如考虑施工需要一定的角度，最大角度不应超过 10°。

5　结语

以上问题仅仅是通过初期调研发现的，更多更深层次的巷道支护问题，有待随着对调研矿井资料的深入分析再得出，对于已经发现及后续探索得出的问题，需要进行重点研究和攻关，逐步解决现在的弊端和不足，以提升涧河煤矿巷道支护技术。

参考文献：

[1] 梁连峰.浅谈煤巷锚杆支护技术理论[J].内蒙古煤炭经济,2011(01):44-45.
[2] 陶志伦.对煤巷锚杆支护技术理论的探讨[J].中小企业管理与科技(下旬刊),2011(04):154-155.
[3] 杨百顺,张　农,李桂臣,等.制约我国煤矿锚杆支护发展的问题浅析[J].煤矿安全,2012(04):135-136.

(责任编辑：赵春梅)

(上接 160 页)

击，另外，相对于国家合法监听的政策无法满足其要求。对于一些安全性不高的业务来说，逐跳加密已经足够了，不需设置端与端的加密，但是，在一些高安全性要求的业务类型中，端与端的加密是第一选择，所以要根据不同的业务类型和安全性的不同要求选择不同的加密方法，加强物联网安全的信任机制。

3.2　物联网中的认证机制

物联网中的认证机制是区分层次的，网络层的认证主要是针对网络层的身份鉴别，而业务层的认证主要负责业务层的身份鉴别，在物联网中，各种机器分工明确，但是在工作上又紧密相连，在一般情况下，网络层的认证必须要设置，所以业务层就可以根据实际情况设置[4]；还有一种情况，物联网的业务不能通过网络运营商保证数据安全性时，就需要设置独立的业务层的认证机制，这时可以只设置业务层的认证而不必设置网络层的认证。对于安全性较高的业务要设置业务层的认证，而对于安全性较低的业务只设置网络层的认证就足够了，所以，要根据不同的情况合理选择。从而加强物联网安全的信任机制的构建。

3.3　物联网的立法保护

物联网是时代进步的产物，极大地便利了人们的生活，对于社会有很高的应用价值，同时，它也有一定的危害，必须利用立法的制度来加强物联网安全信任机制的构建。在有关的法律中规定：“智能物体”行为的责任认定：“对于物联网是一个智能化的技术，人们在使用过程中，要对使用的工具和物体负法律责任，以保证人们的生命财产安全，提高人们对于物联网安全的信任度；物联网个人信息采集、存储、利用的法律规定：在使用物联网技术采集信息和处理信息时，不得侵犯个人隐私，如果侵犯要负相关的法律责任，详细的法律要求见《关于个人隐私保护与个人数据越境流动的指南：理事会建议》；打击一切的物联网犯罪行为。法律的建立使得物联网安全的信任机制更加可靠。

4　结语

高科技可以带给我们极大的方便，同时也会带来一系列问题，要加强物联网安全的信任机制的建立和完善，使物联网更好地为人们服务，而通过充分应用物联网技术，构建完善的物联网信任机制，能够减少资源浪费，节约能源，满足社会的节能发展。

参考文献：

[1] 王有为.企业战略联盟信任机制构建研究[D].成都:西华大学,2010.
[2] 申林川,翟壮,刘芳.物联网安全与信任机制研究分析[J].无线互联科技,2013(21):99-100.
[3] 殷　茗,赵篙正.动态供应链协作信任机制研究[M].西安:西北工业大学出版社,2013(12):52-53.
[4] 任　伟.物联网安全(普通高校物联网工程专业规划教材)[M].北京:清华大学出版社,2012(08):24-25.

(责任编辑：高志凤)