物联网安全与信任机制研究分析

申林川　翟　壮　刘　芳(黄淮学院，河南　驻马店　463000)

摘　要：物联网是新一代信息技术的重要组成部分。物联网这个概念、在中国早在1999年就提出来了。当时叫传感网。其定义是：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，按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络概念。“物联网概念”是在“互联网概念”的基础上，将其用户端延伸和扩展到任何物品与物品之间，进行信息交换和通信的一种网络概念。

关键词：物联网；物联网安全问题；物联网信任机制

由于物联网是由大量的机器构成，缺少人对设备的有效监控，并且数量庞大，设备集群等相关特点造成的，这些特殊的安全问题主要有以下几个方面：

物联网机器 感知节点的本地安全问题。物联网机器 感知节点多数部署在无人监控的场景中，攻击者可以轻易地接触到这些设备，从而对他们造成破坏。

感知网络的传输与信息安全问题。感知节点通常情况下功能简单(如自动温度计)、携带能量少(使用电池)，使得它们无法拥有复杂的安全保护能力，而感知网络多种多样，从温度测量到水文监控，从道路导航到自动控制，它们的数据传输和消息也没有特定的标准，所以没法提供统一的安全保护体系。

核心网络的传输与信息安全问题。核心网络具有相对完整的安全保护能力，但是由于物联网中节点数量庞大，且以集群方式存在，因此会导致在数据传播时，由于大量机器的数据发送使网络拥塞，产生拒绝服务攻击。此外，现有通信网络的安全架构都是从人通信的角度设计的，并不适用于机器的通信。使用现有安全机制会割裂物联网机器间的逻辑关系。

物联网业务的安全问题。由于物联网设备可能是先部署后连接网络，而物联网节点又无人看守，所以如何对物联网设备进行远程签约信息和业务信息配置就成了难题。另外，庞大且多样化的物联网平台必然需要一个强大而统一的安全管理平台，否则独立的平台会被各式各样的物联网应用所淹没，但如此一来，如何对物联网机器的日志等安全信息进行管理成为新的问题，并且可能割裂网络与业务平台之间的信任关系，导致新一轮安全问题的产生。

1 物联网中的业务认证机制

传统的认证是区分不同层次的，网络层的认证就负责网络层的身份鉴别，业务层的认证就负责业务层的身份鉴别，两者独立存在。但是在物联网中，大多数情况下，机器都是拥有专门的用途，因此其业务应用与网络通信紧紧地绑在一起。由于网络层的认证是不可缺少的，那么其业务层的认证机制就不再是必需的，而是可以根据业务由谁来提供和业务的安全敏感程度来设计。例如，当物联网的业务由运营商提供时，那么就可以充分利用网络层认证的结果而不需要进行业务层的认证；当物联网的业务由第三方提供也无法从网络运营商处获得密钥等安全参数时，它就可以发起独立的业务认证而不用考虑网络层的认证；或者当业务是敏感业务如金融类业务时，一般业务提供者会不信任网络层的安全级别，而使用更高级别的安全保护，那么这个时候就需要做业务层的认证。

2 物联网中的加密机制

传统的网络层加密机制是逐跳加密，即信息在发送过程中，虽然在传输过程中是加密的，但是需要不断地在每个经过的节点上解密和加密，即在每个节点上都是明文的。而传统的业务层加密机制则是端到端的，即信息只在发送端和接收端才是明文，而在传输的过程和转发节点上都是密文。由于物联网中网络连接和业务使用紧密结合，那么就面临到底使用逐跳加密还是端到端加密的选择。

对于逐跳加密来说，它可以只对有必要受保护的链接进行加密，并且由于逐跳加密在网络层进行，所以可以适用于所有业务，即不同的业务可以在统一的物联网业务平台上实施安全管理，从而做到安全机制对业务的透明。这就保证了逐跳加密的低时延、高效率、低成本、可扩展性好的特点。但是，因为逐跳加密需要在各传送节点上对数据进行解密，所以各节点都有可能解读被加密消息的明文，因此逐跳加密对传输路径中的各传送节点的可信任度要求很高。

而对于端到端的加密方式来说，它可以根据业务类型选择不同的安全策略，从而为高安全要求的业务提供高安全等级的保护。不过端到端的加密不能对消息的目的地址进行保护，因为每一个消息所经过的节点都要以此目的地址来确定如何传输消息。这就导致端到端加密方式不能掩盖被传输消息的源点与终点，并容易受到对通信业务进行分析而发起的恶意攻击。另外从国家政策角度来说，端到端的加密也无法满足国家合法监听政策的需求。

由这些分析可知，对一些安全要求不是很高的业务，在网络能够提供逐跳加密保护的前提下，业务层端到端的加密需求就显得并不重要。但是对于高安全需求的业务，端到端的加密仍然是其首选。因而，由于不同物联网业务对安全级别的要求不同，可以将业务层端到端安全作为可选项。未来的物联网安全研究将主要集中在开放的物联网安全体系、物联网个体隐私保护模式、终端安全功能、物联网安全相关法律的制订等几个方面。

[参考文献]

[1]孙其博、刘杰、黎羴、范春晓、孙娟娟.物联网:概念、架构与关键技术研究综述[J].北京邮电大学学报,2010年03期.

[2]聂学武，张永胜.物联网安全问题及其对策研究[J].计算机安全，2010，(11)：4-5.

[3]殷茗、赵嵩正、著.《动态供应链协作信任机制研究》.2009-06-01 .西北工业大学出版社.

[4]任伟、编著.《物联网安全》(普通高校物联网工程专业规划教材).2012-06-01,清华大学出版社.