DOI:10.3969/j.issn.1009-6868.2017.01.011
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20170103.1429.004.html

NB-IoT 中安全问题的若干思考

Security Issues of NB-IoT

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2017) 01-0047-004

摘要: 分析了窄带物联网(NB-IoT)感知层、传输层和处理层的安全需求和相关安全技术,认为安全性是确保NB-IoT商用推广的前提。同时提出了一种基于NB-IoT的安全架构,并详细阐述了该架构中各层次实现的功能和关键技术。最后指出中国应协调、整合相关资源,促进产业交流合作,力争在世界范围内掌握NB-IoT发展的主动权。

关键词: NB-IoT;安全技术;架构

Abstract: In this paper, security requirements and techniques in sensing layer, transport layer and transaction layer of narrowband Internet of things (NB-IoT) are analyzed. Security is considered as the precondition for NB-IoT commercial use. A security architecture based on NB-IoT is proposed, the functions and key techniques of each module are also illustrated. We suggest that by coordinating and integrating related resources, promoting exchanges and cooperation, China will have the initiative in NB-IoT development.

Key words: NB-IoT; security technology; architecture

孙知信/SUN Zhixin
洪汉舒/HONG Hanshu
(南京邮电大学,江苏 南京 210000)
(Nanjing University of Posts and Telecommunications, Nanjing 210000, China)

- NB-IoT已经成为万物互联网络的重要分支,是可在全球范围内广泛应用的新兴技术
- 信息安全不仅关系着NB-IoT技术的发展,更关系到网络运营商和每个用户的隐私和利益
- 随着NB-IoT系统技术和生态链的逐步成熟,海量物联网应用必将呈现爆发性增长

1 NB-IoT的背景及发展现状

基于蜂窝的窄带物联网(NB-IoT)近期引起了广泛关注[1-2]。NB-IoT构建于蜂窝网络,只消耗大约180 KHz的频段,可直接部署于全球移动通信系统(GSM)网络、通用移动通信系统(UMTS)网络或长期演进(LTE)网络,以降低部署成本,实现平滑升级。NB-IoT支持待机时间短,对网络连接要求较高设备的高效连接,同时能提供非常全面的室内蜂窝数据连接覆盖,已成为万物互联网络的一个重要分支,是一种可在全球范围内广泛应用的新兴技术。NB-IoT具有广覆盖、多连接、低速率、低成本、少功耗、优架构等特点[3],可以广泛应用于多种垂直行业,如远程抄表、资产跟踪、智能停车、智慧农业等。在NB-IoT系统逐步成熟的同时,中国也非常重视整个NB-IoT生态链的打造。2016年4月,工业和信息化部召开NB-IoT工作推进会,大力推进和培育NB-IoT整个产业链,并要求年底建成基于标准NB-IoT的规模外场试验环境。中国电信积极响应产业政策,采取实验室验证、外场测试、商用开通的"三步走"策略,中兴通讯[4-5]也紧跟NB-IoT发展建设规划,启动了基于NB-IoT标准的POC验证和实验室验证。随着NB-IoT芯片和终端在2017年上半年的成熟和规模出货,预计2017年下半年将会实现真正的规模性商用部署。然而,NB-IoT也面临着诸如接入鉴权、隐私保护、无线传感器节点防伪等安全威胁。因此,如何在NB-IoT系统中保证业务信息、物理空间资源使用的安全性,已成为NB-IoT商用部署进程中重要而迫切的问题。

收稿时间:2016-11-19
网络出版时间:2017-01-03
基金项目:国家自然科学基金资助项目(61373135,61672299)

2 NB-IoT的安全需求

NB-IoT的安全需求与传统的物联网有很多相似之处[6-7],同时也存在着若干区别。针对感知层、传输层和处理层这3层架构,对NB-IoT的安全需求提出了如下分析和思考。

(1)感知层

感知层位于NB-IoT的最底层,是所有上层架构及服务的基础。类似于一般的物联网感知层,NB-IoT的感知层容易遭受被动攻击和主动攻击这两种性质的攻击。

被动攻击指攻击者只对信息进行窃取而不做任何修改，其主要手段包括窃听、流量分析等。由于NB-IoT的传输媒介依赖于开放的无线网络，攻击者可以通过窃取链路数据，分析流量特征等各种手法获取NB-IoT终端的信息，从而展开后续的一系列的攻击。

不同于被动攻击，主动攻击包括对信息进行的完整性破坏、伪造，因此对NB-IoT网络带来的危害程度远远大于被动攻击。目前主要的主动攻击手段包括节点复制攻击、节点俘获攻击、消息篡改攻击等。例如在NB-IoT的典型应用“智能电表”中，若攻击者俘获了某个用户的NB-IoT终端，则可以任意修改和伪造该电表的读数，从而直接影响到用户的切身利益。

以上攻击方式可以通过数据加密、身份认证、完整性校验等密码算法加以防范[8-9]，常用的密码学机制有随机密钥预分配机制、确定性密钥预分配机制、基于身份的密码机制等。NB-IoT设备电池寿命理论上可以达到10年，由于单个NB-IoT节点感知数据的吞吐率较小，在保证安全的情况下，感知层应当尽可能部署轻量级的密码，例如流密码、分组密码等，以减少终端的运算负荷，延长电池的使用寿命。

与传统物联网感知层不同的是，NB-IoT的组网结构更加明确，感知层节点可以直接与小区内的基站进行数据通信，从而避免了组网过程中潜在的路由安全问题。而另一方面，NB-IoT感知层节点与小区内基站的身份认证应是“双向的”，即基站应对某个NB-IoT感知节点进行接入鉴权，NB-IoT节点也应当对当前小区的基站进行身份认证，防止“伪基站”带来的安全威胁。

（2）传输层

与传统的物联网传输层相比[10]，NB-IoT改变了通过中继网关收集信息再反馈给基站的复杂网络部署，解决了多网络组网、高成本、大容量电池等诸多问题，具有整个城市一张网，便于维护管理，与物业分离更易寻址安装等优势[11-12]，然而也带来了如下所述新的安全威胁。

- 大容量的NB-IoT终端接入。NB-IoT的一个扇区能够支持大约10万个终端连接，如何对这些实时的、海量的大容量连接进行高效身份认证和接入控制，从而避免恶意节点注入虚假信息，这是一个很值得研究的问题。
- 开放的网络环境。NB-IoT的感知层与传输层的通信功能完全借助于无线信道，无线网络固有的脆弱性会给系统带来潜在的风险，攻击者可以通过发射干扰信号造成通信的中断。此外，由于单个扇区的节点数目庞大，攻击者可以利用控制的节点发起拒绝服务攻击，进而影响网络的性能。

解决上述问题的办法是引入高效的端到端身份认证机制、密钥协商机制，为NB-IoT的数据传输提供机密性和完整性保护，同时也能够有效认证消息的合法性。目前计算机网络与LTE移动通信都有相关的传输安全标准，例如IPSEC、SSL、AKA等，但如何通过效率优化，将其部署在NB-IoT系统中还是一个值得研究的问题。

另一方面，应建立完善的入侵检测防护机制，检测恶意节点注入的非法信息。具体来说，首先为某类NB-IoT节点建立和维护一系列的行为轮廓配置，这些配置描述了该类节点正常运转时的行为特征。当一个NB-IoT节点的当前活动与以往活动的差别超出了轮廓配置各项的阈值时，这个当前活动就被认为是异常或一次入侵行为，系统应当及时进行拦截和纠正，避免各类入侵攻击对网络性能造成的负面影响。

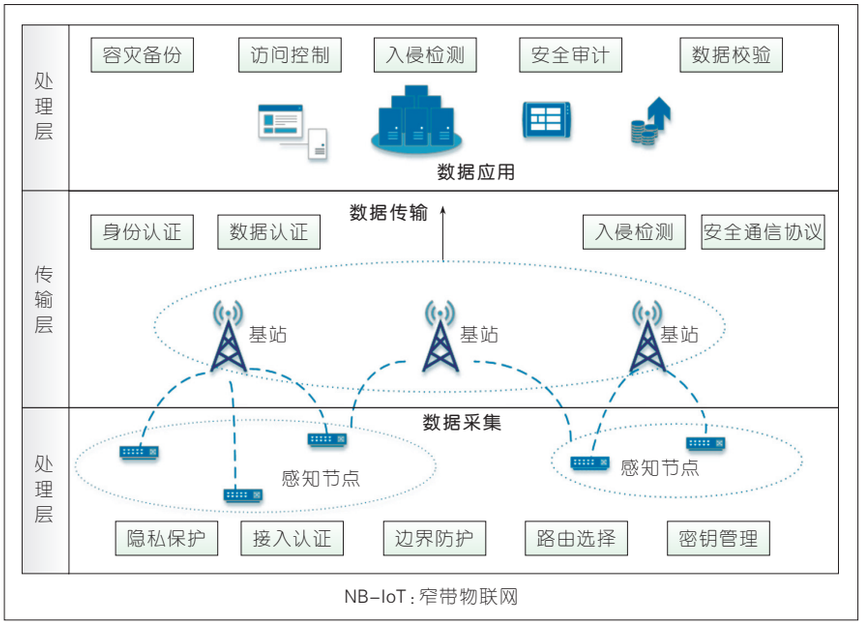
（3）处理层

NB-IoT处理层的核心目标是有效地存储、分析和管理数据。经过感知层、传输层后，大量的数据汇聚在处理层，形成海量的资源，为各类应用提供数据支持。相比于传统的物联网处理层，NB-IoT处理层将承载更大规模的数据量，主要的安全需求集中在以下几个方面：

- 海量异构数据的识别和处理。由于NB-IoT应用的多样性，汇聚在处理层的数据也具备了异构性的特点，从而导致了处理数据的复杂性增加。如何利用已有计算资源高效地识别和管理这些数据成为NB-IoT处理层的核心问题。此外，应当对应用中包含的海量数据进行实时容灾、容错与备份，在各类极端情况下尽可能的保障NB-IoT业务能够有效开展。
- 数据的完整性和认证性。处理层的数据由NB-IoT的感知层和传输层而来，在采集和传输中一旦某一环节出现异常，都会给数据带来不同程度上的完整性破坏。此外，内部人员对数据的非法操作也会造成数据完整性的缺失，从而影响处理层对数据的应用。解决这类安全问题的关键在于建立高效的数据完整性校验和同步机制，并辅以重复数据删除技术、数据自毁技术、数据流程审计技术等，全方位保证数据在存储和传输过程中的安全性。
- 数据的访问控制。NB-IoT具有大量的用户群，不同的用户对数据的访问及操作权限也不同。需要根据用户的级别设定对应的权限，让用户可以受控的进行信息共享。目前数据的访问控制机制主要有强制访问控制机制、自主访问控制机制、基于角色的访问控制机制、基于属性的访问控制机制等，针对应用场景私密度的区别应当采取不同类型的访问控制措施。

3 NB-IoT的安全架构

基于上述的思考与分析，提出了一个基于NB-IoT的安全架构，如图1所示。



▲图1 一种NB-IoT的安全架构

该安全架构分为感知层、传输层和处理层3个层次。

第1层为NB-IoT感知层的安全体系，目标是实现数据从物理世界的安全采集，以及数据和传输层的安全交换。包括以下几个方面的安全特性：感知节点的隐私保护和边界防护、感知节点对于扇区内基站的身份认证、移动节点越区切换时的安全路由选择、密码系统的建立与管理。所牵涉到的关键技术主要有：接入控制技术、终端边界防护与隐私保护技术、蜂窝通信技术，以及轻量级密码技术等。

第2层为NB-IoT传输层的安全体系，目标是实现数据在感知层和处理层之间的安全可靠传输，具体包括以下几个方面的安全特性：海量节点接入的身份认证，海量数据在传输过程中的认证，传输系统的入侵检测，以及与感知层，处理层的安全通信协议的建立。所牵涉的关键技术主要有：身份认证技术、数据认证与鉴权技术、入侵检测技术，以及安全通信协议等。

第3层为NB-IoT处理层的安全体系，目标是实现数据安全、有效的管理及应用，包括以下几个方面的安全特性：对海量数据的容灾备份、各类应用的用户访问控制、系统防护入侵检测、用户行为的安全审计以及对海量数据交互过程中的校验。所牵涉的关键技术主要有：海量数据实时容灾容错技术、访问控制技术、入侵检测技术、针对数据库的安全审计和数据校验技术。

4 展望

NB-IoT是当下全球范围内最值得期待的技术革命之一，而信息安全不仅关系着NB-IoT技术的发展，更关系到网络运营商和每个用户的隐私和利益。本文从感知层、传输层和应用层3个层面出发，研究了NB-IoT的安全技术需求，并提出了一个NB-IoT的安全架构。如下所述，未来针对NB-IoT的安全工作仍然有很多问题需要解决。

（1）进一步增强NB-IoT系统的可用性和可靠性。

NB-IoT的数据通信依赖于运营商的网络基础设施，一方面，在某些特殊的应用环境中，网络并不能完全覆盖到所有的区域，可能会造成NB-IoT的数据通信中断；另外一个方面，这些网络基础设施所提供的无线信道具有公开性，攻击者可以在一定区域内使用干扰设备对NB-IoT通信进行干扰。上述情况发生时，应当有完备的预案已确保NB-IoT系统的可用性。此外，NB-IoT的普及在为用户带来极大便利的同时，其自身也可能遭受诸如失窃、破坏之类的物理攻击。当NB-IoT终端遭到损坏时，设备中数据和信息的价值可能远大于设备本身的价值，因此如何保护这些数据不丢失、不被窃，也是一个值得研究的问题。

（2）针对NB-IoT应用的多样性制订适合的安全策略。

研究NB-IoT技术的最终目的是为了实现各类行业应用，而安全技术则是确保这些应用能稳定开展的基础。不同的应用场景具有不同的安全需求，例如在“智慧交通”，“智能停车”等隐私级别较低的场景中，对数据的实时性及认证性要求较高，对加密算法的强度要求则可以适当地降低；而在“智能抄表”，“移动医疗”等应用场景中，对于数据的机密性、认证性都有着较高的要求。随着NB-IoT系统技术和生态链的逐步成熟，海量的物联网应用必将呈现爆发性增长，在此过程中各个应用开发商都需要针对应用本身的特点制订透明、健全的安全策略，从而为用户提供更加便捷，更加安全的物联网应用服务。

（3）运营商制订完善的安全接入标准。

由于NB-IoT应用依赖于运营商的网络，因此，想要建立NB-IoT安全体系，运营商必须制订一系列安全接入标准，重点对移动网络的接入许可、实名制登记、NB-IoT终端鉴权与追责机制、设备定位等安全需求做出完善规定。

（4）突破NB-IoT安全的核心技术，力争发展主动权。

目前，国际上NB-IoT生产厂商主

要有高通、英特尔、锐迪科、Sequans等，而中国的生产商主要包括中兴通讯等。在NB-IoT的技术与市场的争夺战中，中国应当协调、整合相关资源，在充分吸收发达国家先进技术的同时，加快研发和突破轻量级密码、入侵检测、高性能数据认证与容灾容错等一系列NB-IoT核心安全技术。此外，还要促进与国际同行开放交流、合作互赢，积极参与国际标准提案工作，力争在世界范围内主导制订NB-IoT的安全标准，掌握产业发展的主动权。

参考文献

[1] 戴国华, 余骏华. NB-IoT的产生背景、标准发展以及特性和业务研究[J]. 移动通信, 2016, 40(7): 31-36. DOI:10.3969/j.issn.1006-1010.2016.07.007
[2] RATASUK R, VEJLGAAD B, MANGALVEDHE N. NB-IoT System for M2M Communication [C]// 2016 IEEE Wireless Communications and Networking Conference. USA: IEEE, 2016:1-5. DOI: 10.1109/WCNC.2016.7564708
[3] 陈博, 甘志辉. NB-IoT网络商业价值及组网方案研究[J]. 移动通信, 2016, 40(13): 42-46. DOI: 10.3969/j.issn.1006-1010.2016.13.009
[4] 中兴通讯. 万物互联——中兴通讯NB-IoT解决方案[J]. 通信世界, 2016, 17(17): 32. DOI: 10.3969/j.issn.1009-1564.2016.17.021
[5] 中兴通讯. 中兴通讯携手产业链引领NB-IoT标准制定[J]. 通信世界, 2016, 17(14): 37. DOI: 10.3969/j.issn.1009-1564.2016.14.025
[6] 沈苏彬, 林闯. 专家前言：物联网研究的机遇与挑战[J]. 软件学报, 2014, 25(8):1621-1624. DOI: 10.13328/j.cnki.jos.004668
[7] KRAIJAK S, TUWANUT P. A Survey on IoT Architectures, Protocols, Applications, Security, Privacy, Real-world Implementation and Future Trends[C]// 11th International Conference on Wireless Communications, Networking and Mobile Computing , USA:IEEE, 2015:1-6. DOI: 10.1049/cp.2015.0714
[8] 武传坤. 物联网安全架构初探[J]. 中国科学院院刊, 2010, 25(4): 411-419. DOI: 10.3969/j.issn.1000-3045.2010.04.007
[9] 武传坤. 物联网安全关键技术与挑战[J]. 密码学报, 2015, 2(1): 40-53. DOI: 10.13686/j.cnki.jcr.000059
[10] 吴振强, 周彦伟, 马建峰. 物联网安全传输模型[J]. 计算机学报, 2011, 34(8): 1351-1364. DOI: 10.3724/SP.J.1016.2011.01351
[11] BARDYN J, MELLY T, SELLER O. IoT: The Era of LPWAN is Starting Now[C]// ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference, USA:IEEE, 2016:25-30. DOI:10.1109/ESSCIRC.2016.7598235
[12] LIN X Q, ADHIKARY A, WANG E. Random Access Preamble Design and Detection for 3GPP Narrowband IoT Systems[J]. IEEE Wireless Communications Letters, 2016, 5 (6): 640-643. DOI:10.1109/LWC.2016.2609914

作者简介

孙知信，南京邮电大学教授、博士生导师、现代邮政学院及现代邮政研究院院长；主要研究方向为计算机网络与安全技术、多媒体物联网、大数据及云计算技术；获评为江苏省“333新世纪科学技术带头人培养工程”培养对象，江苏省“青蓝工程”学术带头人培养对象；已发表论文100余篇。

洪汉舒，南京邮电大学博士；主要研究方向为信息安全与密码学。