M2M功能架构与安全研究

高 同[1],朱佳佳[1],罗圣美[2],孙知信[1]
(1.南京邮电大学,江苏 南京 210003;
2.中兴通讯股份有限公司,江苏 南京 210012)

摘 要:M2M通信被看作是一种不需要人际互动的机器之间的通信形式,通过通信网络传递信息从而实现机器与机器或人与机器的数据交换。M2M作为物联网在现阶段发展的主要存在形式,其功能架构和安全问题值得重视,文中主要围绕M2M功能架构与安全问题展开研究。针对此问题,欧洲电信标准化协会详细说明了M2M系统相关的安全需求,对机密性、完整性、身份认证以及授权批准进行了研究。此外ETSI还对M2M系统的功能架构进行了设计,提出了概要层的架构方案。最后对该功能架构中各部分涉及安全的模块作了进一步分析。

关键词:M2M;物联网;功能架构;安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)01-0250-04

Research on M2M Functional Architecture and Security

GAO Tong[1],ZHU Jia-jia[1],LUO Sheng-mei[2],SUN Zhi-xin[1]
(1. Nanjing University of Posts and Telecommunications,Nanjing 210003,China;
2. ZTE Corporation,Nanjing 210012,China)

Abstract:M2M communication is seen as a form of data communication between entities that may have no human interaction,which is called machine-type communication. M2M is thought to be the main application of Internet of Things at present,the functional architecture and security problem of which is worthy of being stressed. Focused on this problem,European Telecommunications Standards Institute(ETSI) has concluded the requirements on security. Besides,ETSI has designed a functional architecture in high level. The security of each model is further studied at last.

Key words:M2M;Internet of Things;functional architecture;security

0 引 言

物联网应用十分广泛,可以说无处不在。而物联网中的核心部分就是机器之间的互联、互通,也就是M2M[1]。M2M是所有增强机器设备通信和网络能力技术的统称,它将机器之间的通信、机器控制通信、人机交互通信、移动互联通信等多种不同类型的通信技术有机地结合在一起,让机器、设备、应用处理过程与后台信息系统共享信息,并与操作者共享信息[2]。狭义的M2M通信是指机器与机器之间建立的通信,如许多智能化仪器仪表可以通过特定的无线接口与其它仪器或主控电脑之间建立通信连接。M2M是"Machine to Machine"的缩写,用来表示机器之间的联接与通信。比如,机器之间自动地进行数据交换(这里的机器也指虚拟的应用软件),从它的功能和潜在用途看,M2M引起了整个物联网的产生[3],是物联网目前的主要发展形式。文中在分析已有文献的基础上,结合ETSI标准组织的最新研究成果[4],对M2M功能架构[5]和安全的方案作了综述。

1 安全需求

ETSI对典型物联网业务用例进行了分析,例如智能医疗、城市自动化、智能抄表和智能电网的标准(或草稿)的制定。根据对典型用例的分析,首先对物联网业务相关的安全需求进行研究,ETSI关心的安全需求如下:

- 身份认证
- 数据传送的机密性
- 数据的完整性
- 阻止网络的非法链接

收稿日期:2011-06-08;**修回日期**:2011-09-13
基金项目:国家自然科学基金(60973140,61170276);江苏省自然科学资金(BK2009425);江苏省六大高峰;江苏省青蓝工程;中兴委托项目
作者简介:高 同(1987-),男,江苏江都人,硕士,研究方向为计算机软件及其在通信中的应用;孙知信,博士,教授,研究方向为基于网络的计算机软件技术、软件技术及其在通信中的应用。

· 隐私保护
· 多重执行者
· 设备/网关的完整性验证
· 可信的安全环境
· 证书和软件在应用层的安全升级

2　功能架构

ETSI 规定了 M2M 系统的概要层功能架构。M2M 系统是由 M2M 设备域、M2M 网络和应用域构成的[6]。其中,M2M 设备域由 M2M 设备、M2M 区域网和 M2M 网关组成。M2M 设备是一种能够应用 M2M 服务能力和网络区域功能来运行 M2M 应用程序的硬件设备。M2M 可以用两种方式来链接 M2M 核心网:直接链接或通过网关作为网络代理。网络和应用域是由以下几部分组成:接入网、传输网、M2M 核心、M2M 应用、网络管理功能、M2M 管理功能[7](见图 1)。

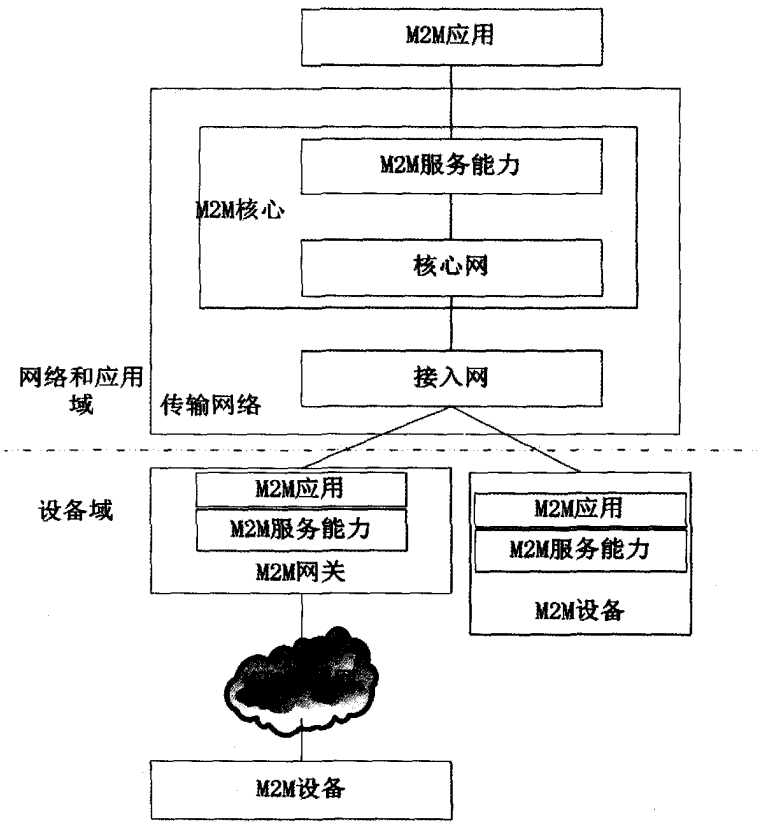

图 1　ETSI 规定的 M2M 功能架构图

ETSI 设计了 M2M 功能架构中 M2M 网关、M2M 设备、M2M 核心上的服务能力(M2M Service Capabilities 简称 SC)。SC 提供了可以被不同 M2M 应用共享的功能。同时,SC 可以通过一些公开的接口使用核心网的功能,同时 SC 也可以调用其它功能。此外,SC 可以接入不止一个核心网。SC 中包含了对安全的考虑,也就是说 M2M 应用可以使用 M2M 服务能力中的安全功能。在 M2M 功能架构中,ETSI 宏观设计了 M2M 系统各元素间的身份认证、密钥管理[8]、服务能力和应用层的注册机制。由此可知,ETSI 考虑的安全主要涉及网络和应用域的安全问题,给出了物联网安全尤其是 M2M 系统有关无线链路和传输网络安全问题,没有涉及 M2M 设备的本地安全,如 M2M 设备的物理安全和签约信息的保护等。

3　网络架构中的安全模块

3.1　网络安全功能模块(NSEC)

NSEC 位于 M2M 网络和应用域的 SC 中,它提供涉及安全的功能包括身份认证、密钥层次和管理、M2M 网关(或设备)的服务层注册以及 M2M 应用注册[9]。

(1)身份认证和服务密钥的管理。

M2M 功能架构中身份认证的考虑使 M2M 系统支持 M2M 核心网、M2M 设备或 M2M 网关间相互的身份认证,并且也支持通过 M2M 核心网的 M2M 设备和 M2M 网关单行道的身份认证。同时,每一项服务能够单独地对其它服务进行身份认证。由于 M2M 设备都通过 M2M 网关相连接[10],因此 M2M 设备的身份认证可以直接通过对(与该硬件相连的)M2M 系统或 M2M 网关的身份认证来实现。M2M 设备认证在 NSEC 模块地实现还需要进一步研究。身份认证在 NSEC 中的具体内容如下:

· 通过身份认证和服务密钥协议执行 M2M 服务层注册。

· 在 M2M 设备/网关和 NSEC 之间执行服务密钥管理。

· 在提供服务之前要进行应用的注册。

· 通过接口与 M2M 注册服务器相链接来获取注册数据,而这些注册数据是执行 M2M 设备或 M2M 网关的注册和服务密钥的管理所必需的。此时 NSEC 扮演了注册者的角色。

· 向 NGC(网络普通通信功能)和 NAE(网络应用实现功能)传达协商的应用密钥。

(2)密钥层次设计。

ETSI 描述了现在 M2M 架构中用于不同层级的认证和授权的密钥层次。由根密钥 KR 派生服务密钥 KS,再由 KS 派生应用密钥 KA。上述的数据层次允许密钥间存在密码性的间隔,而这样的结构就允许废除某个 KA 时却不用废除由同一个 KS 派生的其它 KA,或废除某个 KA 时却不用废除派生该 KA 的 KS。ETSI

规定,当网络运营商和M2M服务提供商不存在商业关系时,应该由服务提供商负责KR的产生方案(在这种情况下网络并不产生KR)。

·KR通过M2M设备/网关和位于M2M核心的M2M服务能力模块之间的身份认证和密钥协议得到服务密钥。在M2M核心这边,KR存储在M2M身份认证服务器(M2M Authentication Server简称为MAS)里的一个安全的环境中,这个安全环境能够防止信息被未授权的程序侵入和操纵。根据基础网络,MAS可位于网络层也可位于服务能力层。在M2M设备或网关里,KR也存储在M2M设备/网关里一个安全的环境中。每一组预分配的M2M设备/网关证书有一个根密钥。

·KS是根据KR派生的服务密钥。KS派生应用层的密钥(KA),而KS对于应用层而言是不可见的。在M2M核心,KS由MAS传输并被存储在NSEC中。而在M2M设备/网关,KS由本地存储KS的安全环境中传输并分别存储在DSEC(设备安全模块)和GSEC(网关安全模块)中。

·KA是根据KS派生出的M2M应用层密钥。对于M2M的每一个应用都应相应存在一个KA,且KA在M2M设备/网关和NGC(网络普通通信能力)之间通信。KA在M2M设备/网关用于对M2M应用进行身份认证和授权,KA也用于保护应用数据的传输。

(3)根密钥的配置(KR)。

M2M的体系应支持多种根密钥配置的方案:

① 当移动运营商和M2M服务提供商是同一个运营商或者存在商业关系时,M2M设备用UICC(Universal Integrated Circuit Card)里预备好的密钥进行接入层和服务层注册[11]。M2M设备配备了UICC,而UICC里储存了用于接入层的注册和服务层注册的安全信令,在这个方案里,UICC存储了两个不同的根密钥,一个用于接入层注册,另一个用于服务层注册。

② 当移动运营商和M2M服务提供商不是同一个运营商且不存在商业关系时,M2M设备/网关可将UICC里预备的密钥用于接入层的注册,而当设备第一次尝试在M2M服务层注册时,M2M设备自动产生另一个不同的密钥用于M2M服务层注册。

③ 如果M2M设备和M2M网关是完全分开的实体,那么每一个实体用UICC预存KR或用自动方法产生KR。在这种情景中,M2M网关负责接入层的注册,M2M设备负责M2M服务层的注册。例如:

·M2M网关用UICC里预备好的密钥进行无线网络注册。另一方面,如果M2M网关应用无线网络来接入M2M系统,那么需要使用一个自动程序来引导M2M网关使用的根密钥。

·M2M设备可使用UICC里预备的根密钥,或者通过一个自动程序产生根密钥。

(4)设备完整性确认。

M2M系统能够提供一种机制来验证M2M设备/网关的完整性。M2M设备/网关可能支持也可能不支持完整性的验证。假设M2M设备/网关支持完整性验证并验证失败,那么该设备/网关将不被允许执行设备/网关的身份认证。验证设备/网关完整性的机制可能开始于查询M2M系统,也可能在任何时候在局部由设备/网关自主开始。如果某个M2M设备/网关支持完整性验证,则在此设备/网关中设有缺陷探测器,M2M系统可远程获取探测器中的数据。

NSEC模块中对设备完整性的支持分以下两个方面:

·NSEC模块需要验证支持完整性验证的M2M设备/网关的完整性。

·NSEC应触发后验证措施,例如:接入控制、补救措施(包括启动NREM功能对M2M设备或网关的软件或固件进行升级)。

3.2 网关安全功能模块(GSEC)

M2M设备域的感知信息都要由网关节点与外界联系,M2M网关的安全性极其重要,接入到M2M核心的超大量传感节点的识别、认证和控制问题,都与M2M网关息息相关。一个网关节点实际被敌手控制的可能性很小,因为需要掌握该节点的密钥(与设备域内部节点通信的密钥或与远程服务能力平台共享的密钥),而这是很困难的。如果敌手掌握了一个网关节点与设备域内部节点的共享密钥,那么他就可以控制设备域的网关节点,并由此获得通过该网关节点传出的所有信息。但如果敌手不知道该网关节点与远程服务能力平台的共享密钥,那么他不能篡改发送的信息,只能阻止部分或全部信息的发送,但这样容易被远程服务能力平台觉察到。ETSI中网关的安全功能主要实现对设备域所有设备的安全控制,执行M2M设备服务层和应用的注册、授权和认证,并对可能的非法设备进行处理,比如阻塞它们与M2M核心的连接。GSEC位于M2M系统功能架构中M2M网关的服务能力里,它提供如下涉及安全的功能:

(1)密钥的管理。

·在M2M网关与位于M2M核心中的M2M服务能力进行身份认证时,从M2M网关里的一个安全环境中获取(不是派生)一个服务层密钥(KS),并且防止未授权程序获取服务层密钥(KS)。

·根据KS为M2M网关的每一个应用各派生(不是获取)一个应用层密钥(KA),并且传递应用层密钥。传递应用层密钥主要的作用是保护M2M应用数

据传输和对 M2M 网关应用进行注册和授权。

·获取(派生或者商议)用于对 M2M 设备和 M2M 网关中服务能力之间进行身份认证的密钥资料。密钥资料的形成和存储应该在网关中的一个安全环境里进行。

(2) M2M 网关服务的注册。

·通过与 M2M 核心中的 M2M 服务能力彼此间的身份认证执行服务层的注册。

·可选择支持以下完整性认证和后确认程序:

-执行认证并且(或者)报告 M2M 网关完整程度。

-根据策略,当侦查出 M2M 设备的完整性出错时,控制出错的 M2M 设备和 M2M 核心的接入。

·可选择支持安全时间同步的程序。

(3) M2M 设备服务的注册和管理。

·在 M2M 网关促进 M2M 设备与 M2M 网关中的 M2M 服务能力的服务层注册。

·遵守 M2M 运营商的策略;如果 M2M 设备能够执行完整性验证但是完整性验证失败的话,阻塞 M2M 设备到 M2M 核心的所有接入。

(4) 应用的身份认证。

·在网关应用(Gateway Applications 简称 GA)数据流交换之前,促进 GA 在服务层的身份认证。

·作为 NSEC 执行身份认证功能的代理,促进 M2M 设备应用(Devices Applications 简称 DA)在服务层的身份认证。

3.3 在 M2M 设备的安全功能模块(DSEC)

M2M 设备具有数量庞大和无人值守的特点,且其中的部分所处环境恶劣。DSEC 位于 M2M 系统功能架构中 M2M 设备的服务能力里,它提供涉及安全的功能包括密钥的生成和管理、M2M 服务层的注册、M2M 应用的身份认证和设备完整性验证。但是 ETSI 考虑的设备安全问题主要局限是设备在网络中的合法性和设备域传输信息的机密性,未涉及设备的本身安全问题,如设备敏感信息的泄露、篡改、终端病毒等问题。而常用的解决措施有身份认证、数据访问控制、信道加密、单向数据过滤和强审计等[12]。

DSEC 位于 M2M 系统功能架构中 M2M 设备域的服务能力里,它提供如下涉及安全的功能:

(1) 密钥的管理。

·根据在 M2M 核心中 M2M 设备与 M2M 服务能力彼此间的身份认证,从 M2M 设备里的一个安全环境里获取(不是派生)一把服务层的密钥(KS)[13]。

·根据 KS 为 M2M 设备运行的每一个应用各派生一把应用层的密钥(KA),并将这些密钥传递到 M2M 设备里安全的环境中。这些密钥用于 M2M 应用的身份认证和授权,也用于保护 M2M 设备应用的数据流。

(2) M2M 设备服务的注册。

·通过与 M2M 网关中的 M2M 服务能力之间的相互身份认证,执行服务层的注册。

·认证并且(或)报告 M2M 设备完整性。

·支持安全的时间同步程序。

·协议并运用可行的安全服务类的属性。

4 结束语

文中对 M2M 通信的网络架构进行研究,其目的是支持 M2M 通信的安全。以尽早确定 M2M 通信的功能架构,完善各个功能点,ETSI 提出一种 M2M 功能架构,并对网关、设备、网络三个模块的安全部分做了分析,并未对具体细节做进一步说明。在进一步研究中,将通过构建真实的 M2M 通信环境对所提方案进行完善和细化。

参考文献:

[1] 孙其博,刘 杰,黎 彝,等. 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,2010,33(3):1-9.

[2] 宁焕生,张 瑜,刘芳丽,等. 中国物联网信息系统研究[J]. 电子学报,2006,34(S1):2514-2517.

[3] 刘雯婕. M2M 系统结构及发展[J]. 通信管理与技术,2009(2):40-42.

[4] 曾谁飞,何光宇,闻英友,等. SIP 应用的 DoS 检测与响应研究[J]. 通信学报,2010,31(5):108-112.

[5] 叶袁洪. M2M 设备管理系统的研究与实现[D]. 重庆:重庆大学,2009.

[6] Starsinic M. System architecture challenges in the home M2M network[C]//Applications and Technology Conference. [s. l.]:[s. n.],2010.

[7] 金 爽. M2M 关键协议研究及一致性验证[D]. 北京:北京邮电大学,2010.

[8] 雷震粥. 支持 M2M 通信的无线网络基础的发展[J]. 电信科学,2004,20(11):1-4.

[9] Chen Hongsong, Fu Zhongchuan, Zhang Dongyan. Security and trust research in M2M system[C]//2011 IEEE International Conference on Vehicular Electronics and Safety. [s. l.]:[s. n.],2011:286-290.

[10] Du Jiang, Chao Shiwei. A study of information security for M2M of IOT[C]//2010 3rd International Conference on Advanced Computer Theory and Engineering. [s. l.]:[s. n.], 2010.

[11] 杨 庚,许 健. 物联网安全特征与关键技术[J]. 南京邮电大学学报,2010,30(4):20-29.

[12] 焦文娟,齐旻鹏,朱红雪. M2M 的安全研究[J]. 电信技术,2009(6):76-78.

[13] Cha I, Shah Y, Schmidt A U, et al. Trust in M2M communication[J]. Vehicular Technology Magazine, IEEE, 2009, 4(3): 69-75.