附表3

**河北北方学院**

**毕业论文（设计）开题报告**

题 目：物联网网关轻量级认证和加密技术研究

姓 名：郑智聪

院 系：信息科学与工程学院

专 业：电子信息科学与技术

年 级：2016级

学 号：201642030

指导教师：郭本振

开题时间： 2019年11月15日

**河北北方学院教务处制**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **论文题目** | | **物联网网关轻量级认证和加密技术研究** | | |
| **课题来源** | | **师生共同拟定课题** | | |
| **研究方向** | |  | | |
| 报告内容：（以下项目仅供参考，各学院可根据专业特点修订）  一、立题依据（研究的目的与意义）  物联网是以互联网为基础,延伸到物与物之间的通信,使设备之间的通信不需要通过人而直接交换信息的技术。物联网的发展和广泛应用,使人们越来越深刻体会到物联网所带来的便利,但这种不需要人参与的技术也引入了新的安全隐患。物联网设备往往是一些受限的设备,它们因为计算能力有限,资源空间有限，无人值守等特点而对诸如加密算法、密钥管理协议等安全机制要求较高,除此以外,通信内容较为单一、数据长度有限、业务通信流程异于原有互联网业务。导致在物联网设备上的安全问题很难照搬互联网上成熟的安全解决方案,而需要为此专门设计一套轻量级的安全解决方案。  二、研究内容(内容、结构框架或研究提纲以及要突破的难点)：  1. 学习并研究物联网通信方式及通信架构, 对物联网网络结构有清晰的认识, 熟练掌握物联网的主要特点及通信模式  2. 依据物联网的架构特征以及机器通信的特点, 深入分析基于移动通信网传输信息的物 联网存在的安全问题, 提出相应的安全需求。  3. 结合物联网安全需求分析以及现有通信网络安全机制设计情况, 提出基于移动通信网络传输物联网信息的物联网安全架构及适用于物联网的认证机制, 包括用户接入认证和 设备认证机制。  三、研究方法与技术路线  首先分析物联网的产生及研究现状,基于移动通信网络承载物联网通信的物联网架构,总结归纳物联网不同于现有通讯网络的特点。然后根据物联网的架构及物联网的特点,分别从终端设备、传感器网络、通信网络、物联网应用、控制管理等角度详细分析物联网中可能出现的安全问题, 并针对物联网中的特殊安全问题 , 提出物联网中的安全需求, 结合现有通信网络安全技术及物联网架构研究分析物联网中适用的安全关键技术, 包括接入认证、业务认证的分析、加密方式的选择、密钥管理方式、用户隐私的保护等安全关键技术。  在对物联网中认证问题详细分析的基础上, 研究提出适用于物联网的组认证机制和 设备认证机制以及基于认证的物联网密钥管理，其中组认证机制解决较大数量物联网终端短时间内同时接入网络带来的信令拥塞问题, 设备认证机制可以防上非法的设备接入网络 从而对网络造成危害, 基于物联网认证技术的密钥管理机制将传感器网络与通信网络结合起来使得运营商通信网络可以安全控制传感器网络的密钥及信息传递。  四、研究过程安排  (1) 2019.11.15-2019.12.15 进一步查阅资料，了解选题方向上国内外的研究现状。  (2) 2019.12.16-2020.02.29 整理相关资料，系统学习和分析用到的技术点。  (3) 2020.03.01-2020.04.15 确定整体软件框架，实现基本的认证和加密功能。  (4) 2020.04.16-2020.05.30 对完成的程序进行测试、优化、分析并得出结论；  (5) 2020.05.30-2020.06.01 进行毕业答辩。  五、预期研究结果  设计出一套适用于物联网网关的轻量级的安全解决方案，实现优化后的算法,同时改进密钥扩展算法以提升其安全性。基本上实现大量具有组特性的物联网终端设备同时接入网络的安全认证。  六、参考文献：   1. 基于物联网安全认证技术的研究与实现[J]. 吴召平.电子科技大学 2. 物联网安全—认证技术研究[J]. 焦文娟 .北京邮电大学 3. 物联网环境下统一认证安全机制的研究[J].居庆祎.湖南工业大学 4. 物联网环境下的控制安全关键技术研究.杨金翠.北京邮电大学 | | | | |
| 指导教师意见：  指导教师（签名） 2019年11月20日 | | | | |
| 专 家 组 成 员  （不得少于三人） | 姓名 | | 职称 | 所在教研室 |
| 刘建军 | | 副教授 | 电子信息教研室 |
| 张雪姣 | | 讲师 | 电子信息教研室 |
| 刘泉 | | 讲师 | 电子信息教研室 |
|  | |  |  |
|  | |  |  |
| 院 系 专 家 组 论 证 意 见 | 同意开题。  专家组组长签名：  专家组委员签名：  2017年11月22日 | | | |
| 备注 |  | | | |