1.

2018 届研究生硕士学位论文

分类号：　　　　　　　　　　　　　学校代码：10269

密　级：　　　　　　　　　　　　　学　　号：51151500079

華東師範大學

East China Normal University

硕士学位论文

MASTER’S DISSERTATION

论文题目：

自主移动机器人空间永恒探索算法的符号模型检测方法

院　　系：计算机科学与软件工程学院

专业名称：软件工程

研究方向：高可信计算理论与技术

指导教师：张民 副教授

学位申请人：蔡晓伟

2017 年 11 月

Dissertation for master degree in 2018 University Code: 10269

Student ID: 51151500079

EAST CHINA NORMAL UNIVERSITY

On Symbolic Model Checking of Mobile Robots Perpetual Exploration Algorithm

Department:	School of Computer Science and Software Engineering
Major:	Software Engineering
Research direction:	Trustworthy Computing Theory and Technique
Supervisor:	Assoc Prof. Zhang Min
Candidate:	Cai Xiaowei

2017.11

华东师范大学学位论文原创性声明

郑重声明：本人呈交的学位论文《自主移动机器人空间永恒探索算法的符号模型检测方法》，是在华东师范大学攻读硕士/博士（请勾选）学位期间，在导师的指导下进行的研究工作及取得的研究成果。除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确说明并表示谢意。

作者签名:____________ 日期: 年 月 日

华东师范大学学位论文著作权使用声明

《自主移动机器人空间永恒探索算法的符号模型检测方法》系本人在华东师范大学攻读学位期间在导师指导下完成的硕士/博士（请勾选）学位论文，本论文的研究成果归华东师范大学所有。本人同意华东师范大学根据相关规定保留和使用此学位论文，并向主管部门和相关机构如国家图书馆、中信所和“知网”送交学位论文的印刷版和电子版；允许学位论文进入华东师范大学图书馆及数据库被查阅、借阅；同意学校将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于（请勾选）

（）1. 经华东师范大学相关部门审查核定的“内部”或“涉密”学位论文 *，于年月日解密，解密后适用上述授权。

（）2. 不保密，适用上述授权。

导师签名:________________ 本人签名:________________

年 月 日

* “涉密”学位论文应是已经华东师范大学学位评定委员会办公室或保密委员会审定过的学位论文（需附获批的《华东师范大学研究生申请学位论文“涉密”

蔡晓伟 硕士学位论文答辩委员会成员名单

姓名	职称	单位	备注
朱惠彪	教授	华东师范大学	主席
章玥	副教授	华东师范大学	无
毛宏燕	副教授	华东师范大学	无

摘 要

随着科技的发展，人们对无线宽带技术的需求日益增加。全球无线微波载入技术 WiMAX(Worldwide Interoperability for Microwave Acess) 是基于无线城域网络的新技术，实现了宽带接入技术和移动服务的相互结合。IEEE802.16m 标准是在 IEEE802.16e 基础上的补充标准，定义了新一代 WiMAX 技术规范。由于无线系统使用完全开放和未实施保护的无线通信信道，因此需要在无线通信技术中实施可信和强健的安全加密保护实现通信的机密性，隐私性和完整性。

IEEE802.16m 标准在 MAC 安全子层中定义了密钥管理 PKMv3 协议，实现基站与手机端间的双向认证以及安全密钥分发。在 PKMv3 协议中，基站作为服务端，手机站作为客户端，双方通过 X.509 数字证书实现身份验证，建立授权密钥，并通过安全组件协商，实现安全参数交换，最终通过密钥材料的传输，生成传输密钥以加密后续的通讯消息。PKMv3 是改进后的第三代密钥管理协议，目前已有大量研究指出前两代协议中出现较多安全漏洞，并且针对第三代协议的研究仍然不够完善。因此，分析 PKMv3 协议的具体执行流程以及验证协议的安全特性十分关键。

本文对安全协议的研究采用形式化建模的方式。安全协议的形式化方法采用数学模型，实现对协议结构以及通信过程的模拟，并通过有效的程序分析验证系统所满足的性质条件。Maude 是基于重写逻辑的形式化建模语言，它定义了简洁且无二义性的语法，并且提供多种检测方法，适合作为编程语言，算法的分析工具以及系统建模工具。本文通过 Maude 定义的可执行形式化规范，实现对 PKMv3 协议中各执行阶段的建模。不同于现有的研究工作，本文考虑到协议执行过程中密钥的周期性质，在协议模型中加入时间机制模拟密钥重认证的过程，同时引入攻击者模型，模拟入侵者在网络中窃取，重放以及伪造消息的过程。

基于编写完成的 PKMv3 协议可执行规范，本文通过 LTL 模型检测工具实现对协议连续性，密钥活性，认证密钥以及传输密钥生命周期等时间相关性质的检测；并通过穷尽空间状态查找指令实现对协议中机密性，认证性，完整性以及可用性等安全性质的验证。验证结果表明，PKMv3 协议模型能够满足协议标准中的各项时间特性，但可能会遭遇到入侵者攻击，从而无法保证协议的完整性以及可用性。针对协议中的安全漏洞，本文在协议各阶段提出相应的解决方案，进而重

新改写协议模型，证明改进后协议所满足的安全特性。

关键词: IEEE802.16m 标准，PKMv3 协议，密钥管理，重写逻辑，Maude 语言，形式化验证

ABSTRACT

With the development of information technology, people's demand for wireless broadband technology is increasing. Worldwide Interoperability for Microwave Access is a new technology based on Wireless Metropolitan Area Network (WLAN), which enables the combination of broadband access technology and mobile services. IEEE802.16m is a supplement standard based on the IEEE802.16e, it defines a new generation of WiMAX technical specifications. Since the wireless system uses completely open and unprotected wireless communication channels, it is necessary to implement trusted and robust encryption protection in wireless communication technology to achieve the confidentiality, privacy and integrity of communications.

IEEE802.16m standard defines the key management PKMv3 protocol in the MAC security sub-layer. It aims to implement mutual authentication and security key distribution between the base station and the subscriber station. In PKMv3 protocol, the base station acts as the server while the subscriber station as the client. They implement mutual authentication by means of X.509 digital certificate to establish the authorization key, and exchange security parameters by means of security association negotiation, and finally generate a traffic key to encrypt subsequent messages. PKMv3 is the third-generation key management protocol. At present, a large number of studies have pointed out security vulnerabilities that exits in the previous two generations of protocols, and the researches on the third generation protocol are still not sufficient. Therefore, it is very important to analyze the specific process of PKMv3 protocol and verify the security property of the protocol.

This paper uses formal modeling method to study the security protocols. The formal analysis of security protocol adopts the mathematical model to realize the simulation of the protocol structure and the communication process, and then validates the condition that the system can satisfy. Maude is a formal modeling language based on rewriting logic. It defines a simple and unambiguous grammar, and provides a variety of verification methods, which is suitable as a programming language, algorithmic analysis tools and system modeling tools. This paper will implement the modeling of each execution phase of PKMv3 protocol through the executable formalization specification defined by Maude. Different from the existing research work, this paper takes consider of the lifetime of secret keys in PKMv3 protocol, adding time mechanism in the protocol model to simulate the key re-authentication process, and introduces the intruder model to simulate the intruder's behavior of eavesdropping, replaying and faking messages in the network.

Based on the executable specification of PKMv3 protocol, this paper can realize the verification of the time-related properties such as succession, key freshness, period of AK and TEK by means of LTL model checker, and realize the verification of security properties such as confidentiality, authentication, integrity and availability by means of search command. The verification results show that PKMv3 protocol model can meet the time characteristics of the protocol standard. However it may encounter intruder attacks, so it can not guarantee the integrity and availability. In view of the security vulnerabilities in PKMv3 protocol, this paper proposes corresponding solutions in each phase of the protocol, and then adapts the formal specification to prove that the improved protocol can meet safety requirements.

Keywords: *IEEE802.16 Standard, PKMv3 Protocol, Key Management, Rewriting Logic, Maude, Formal Verification*