电力系统通信中 WWAN 安全研究

黄秀丽,张 涛,王玉斐,华 晔
(中国电力科学研究院 信息网络安全实验室,江苏 南京 210003)

摘 要:目前,电力系统正朝着智能电网的方向发展,在智能电网下通信方式将会呈现多样化,无线通信网络将成为电力系统通信重要的通信方式之一被广泛应用。无线网络以其在网络建设的灵活性、便捷性、扩展性、性能价格比等方面的优势在电力系统通信中得到了应用和普及。同时,随着无线传输在电力监控系统中所占有的地位日显重要,其安全性逐渐成为电力系统通信中的研究热点。文中首先介绍了电力通信的背景,接着对 WWAN 安全及其理论研究趋势进行了分析,最后对电力系统通信中 WWAN 安全进行了思考,并对下一步工作进行了展望。

关键词:电力系统;WWAN;无线传输;安全防护
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)05-0245-05

Research of WWAN Security in Communication of Power System

HUANG Xiu-li, ZHANG Tao, WANG Yu-fei, HUA Ye
(Information & Network Security Laboratory, Electric Power Research Institute of China, Nanjing 210003, China)

Abstract: At present, the power system is moving in the direction of the smart grid, and the communication will be more diversified, the wireless communication network will become an important communication way in power system communications and widely used in smart grid. And wireless communication has been applied and spread in the power system communication because of its merits in the network construction including flexibility, convenience, scalability, cost performance and others. Meanwhile, with the increasing importance of wireless communication in the power monitoring system, its security is becoming a research hotspot in power system communication. It describes the background of power communication, and then makes a detail analysis for WWAN security and its theoretical research trends, and finally research WWAN safety under communication of the power environment, and predict the next step.

Key words: power system; WWAN; wireless communication; security detection

0 引 言

电力通信是电力系统的重要技术之一,有力地支撑了电力系统发电、输电、变电、配电、调度、用电等六大环节的安全性和可靠性。

目前,电力系统主要的通信方式仍为有线通信,无线通信应用较少。随着电力系统向着智能电网的方向发展,无线通信将在端网以及接入网环节得到广泛的应用。其中端网中以无线传感网 WSN 包括 Zigbee 等各种技术为主,接入网以无线广域网 WWAN 包括 3G、4G 等各种技术为主。电力系统终端信息通过无线传感网进行搜集,通过无线广域网进行接入,经过骨干网的传输,到达后台处理系统。

电力系统中应用无线通信的场所多为野外无人值守处,譬如输变电环节的线路状态在线监测系统等,所处环境复杂多变,对通信可靠性、安全性构成了很大的挑战。

无线通信技术目前发展迅速,其各项关键技术均比较成熟,其灵活、便捷的特性已经得到了广泛的认可,能够满足电力系统在智能电网下对通信的要求。此外,无线通信各技术已在其他行业和领域也有很多成功的应用案例。

WWAN 作为无线通信技术中的重要通信技术之一,在电力系统通信中的地位日益重要。但 WWAN 由于其开放性,面临着诸多威胁,譬如针对无线接口和网络接口的攻击,针对终端和用户识别模块(USIM)的攻击等。攻击者利用协议缺陷和系统漏洞对 WWAN 进行窃听、非法访问、干扰,使通信数据泄密、客户盗用、中断或瘫痪网络服务,给通信各方造成各种各样的损失。因此,随着 WWAN 在电力系统的应用和普及,其安全性将成为电力系统无线安全通信面临的重要问题。

1 WWAN 安全机制

截止目前,WWAN 共经历了三代,第一代为模拟

收稿日期:2011-09-29;**修回日期**:2011-12-30
基金项目:国家电网公司 2011 年科技项目(SG11075-1)
作者简介:黄秀丽(1979-),女,工程师,硕士,研究方向为信息安全。

蜂窝移动通信,在模拟蜂窝通信中,没有安全通信措施,信息以明文方式发送,攻击者找到其频段,就很容易窃听信息。同时,也很容易伪造终端进行无线通信网络接入,造成非法访问。第二代数字蜂窝移动通信系统(2G),是第一个采用安全措施的无线广域通信技术,实现了用户信息的认证和加密。第三代移动通信系统(3G)在2G安全措施的技术上,继承其优点改进其缺点,并与2G兼容,有更完善的安全保障措施。

在移动通信三代的通信技术发展历程中,无线接入的安全特征主要体现在五个方面:设备识别、用户身份保密、身份认证、数据保密和和数据完整性。为了实现这些安全特性和目标,主要采取了以下四方面安全措施:

(1)采用唯一的国际移动设备标识符(IMEI)对移动设备识别;

(2)使用临时识别符(TMSI)代替用户永久身份(IMSI),防止IMSI被窃听;

(3)使用认证和密钥协商(AKA)对用户鉴权;

(4)无线链路上对通信信息加密和信令信息完整性保护。

设备识别的作用是保证通信系统中的终端设备的合法性。识别功能通过设备识别寄存器(EIR)完成。每个网络都有EIR,EIR以黑名单、白名单和灰名单对应被偷的或无类型许可的终端、有效的终端和需要单独跟踪的终端。设备识别的程序过程是,交换中心向手机请求IMEI,并将收到的IMEI与白、黑、灰三种表进行比较,通过比较结果判断终端设备是否可以入网。通过合法识别,可以禁止各种非法终端的使用,禁止盗用和非法应用。

用户身份保密措施包括了用户身份保密、用户位置保密和用户位置不可追踪性等3个方面。系统采用用户临时识别码(TMSI)实现用户的身份保密,保护用户的隐私,防止用户位置被跟踪。对进入其访问区的每个用户,网络都会分配一个临时移动台识别号码(TMSI),TMSI和IMSI一起存于数据库中,用户只要使用TMSI和位置区域标识LAI即可标识自己的身份。

身份认证是最重要的网络安全接入措施,通过认证和密钥协商(AKA)协议[1~3]完成。通过身份认证,决定用户是否能够接入移动系统,是否有权限使用网络资源,以保证网络资源的合法使用,防止非法用户的接入。身份认证在用户登记、开机、位置更新和注册等环节进行[4]。

数据保密性主要指加密算法协商、加密密钥协商、用户数据加密、信令数据加密四个方面。加密密钥协商通过AKA环节完成,加密算法协商通过安全模式协商机制完成。

数据完整性包括了完整性算法协商、完整性密钥协商、数据和信令完整性三个方面。完整性密钥协商通过AKA环节完成,完整性算法协商由用户与网络间的安全模式协商机制完成。

2 WWAN安全机制分析

2.1 WWAN安全机制差异

GSM是第一个提供安全机制的移动通信系统,而3G移动通信系统中的安全技术是在GSM的安全机制的基础之上建立起来的,它弥补了GSM安全机制中的缺点,补充了新的安全机制。在用户身份保护、密钥协商、双向认证、数据通信的保密以及数据完整性检测等方面都得到了加强。2G和3G的差异主要体现在下面七个方面:

(1)3G使用了临时身份TMSI和加密的永久身份IMSI用来识别用户身份;

(2)3G的认证和密钥协商(AKA)协议采用了5元组的认证向量AV,实现了用户网络双向认证,并且在鉴权令牌AUTN中包括了序列号SQN,保证鉴权过程的最新性,防止重放攻击;

(3)3G加长了密钥,长度增加为128位,改进了加密算法,补充了算法协商机制;

(4)3G的数据加密延长到无线接入控制器RNC,增加了信令数据的完整性和保密性;

(5)3G通过消息认证机制保护用户和网络间的信令消息完整性,防止被篡改攻击;

(6)3G的安全机制拥有可扩展特性,为将来扩展安全机制提供了支撑;

(7)3G增加了用户安全措施的可视性操作,用户能够查看自己所采用的安全措施、安全模式、安全级别。

表1为2G和3G安全机制差异一览表。

表1 安全机制差异一览表

安全机制	2G	3G
用户身份识别(IMSI)	明文	密文
网络认证用户	有	有
用户认证网络	无	有
数据加密传输	密钥生成:A3 加密算法:A5/GEA	密钥生成:f3 加密算法:f8
	密钥长度:64kit	密钥长度:128kit
	算法:固定/可选	算法:协商
数据完整性传输	无	有
安全配置可见性	无	有

2.2 WWAN安全机制缺陷

●2G系统安全机制的主要缺陷集中在以下六个方面:

(1)2G系统明文发送IMSI,容易造成窃听攻击和仿冒攻击;

(2)用户和网络间认证为单向认证,即网络对用户的认证,用户不对网络的认证;

(3)密码长度只有64 bit,比较短,容易被破解;

(4)密码算法不公开,其安全性不能得到客观的评价,许多潜在的漏洞不易被及时发现、改进,加密算法固定不变,缺乏算法协商和密钥协商过程;

(5)用户信息和信令信息不是端到端加密,而只是在无线信道部分加密,基站和基站之间及固网内无加密;

(6)用户信息和信令信息缺乏完整性认证。

●3G系统的安全机制较GSM系统有所改进,特别是增加了移动台对网络的鉴权,但在3G系统中,仍然遗留下来一些潜在的安全问题,主要有以下六个方面:

(1)IMSI在有些情况下明文传输,可被攻击者截获,用于进一步攻击;

(2)安全模式建立时,移动设备向RNC经由空中接口明文发送安全能力参数;

(3)安全算法自主开发欠缺,算法先进性不足;

(4)Iu接口和Iur接口上数据无保护措施,以明文方式传输安全参数;

(5)缺乏用户数据完整性保护;

(6)缺乏用户对VLR的认证。

2.3 WWAN安全增强建议

目前,主要有以下八个方面的增强建议,通过增强措施加强3G的安全性:

(1)使用智能天线进一步加强物理层安全;

(2)考虑Iu接口和Iur接口的安全性;

(3)考虑使用某个特定的密钥将IMSI加密后传输;

(4)开发自主的加密算法;

(5)采用公钥算法抗抵赖;

(6)采用新密码技术提高抗攻击能力;

(7)对重要数据提供用户数据完整性;

(8)对机密通信业务采用端到端的安全性保护措施。

3 WWAN理论研究趋势

目前对无线WWAN的理论研究主要集中在两方面,一方面是对3G安全机制的增强研究,另一方面是对4G安全机制的研究。

3.1 3G安全的增强研究

用户身份保密、算法、算法协商、AKA身份认证等都是3G安全性研究的热点,针对3G安全机制中存在的缺陷和不足,国内外许多学者对其做了大量研究和改进,解决了存在的一些问题,增强了3G机制的安全性。

在用户身份保密方面,文献[5]提出了3种保护IMSI方法;文献[6]通过在系统中采用匿名标识管理模块对IMSI标识作了保护;文献[7,8]对认证中"永久身份不保密"和"单项认证"等缺陷,提出了改进方案,前者将单项认证机制改进为双向认证,其中假设访问网络与归属网络有共享密钥,后者假设归属网络有公钥,并基于归属网络与访问网络有共享密钥,提出了改进的方案,解决了用户的身份泄露问题和终端对网络的认证问题。

在算法方面,文献[9]针对3GPP中AKA认证协议和无线空中接口的安全算法设计要求,给出了多种实现方案,同时结合《商用密码管理条例》相关规定,讨论了3GPP中保密算法、完整性算法的国内应用问题;文献[10]对基于TD-SCDMA系统的完整性保护算法进行了研究;文献[11]对3GAKA协议中算法进行了研究。

在算法协商、数据保密及数据完整性方面,文献[12,13]分析了UMTS系统中存在的安全缺陷,包括由算法协商导致的拒绝服务攻击,用户数据缺少完整性保护,Iu和Iur接口上传输的数据缺少机密性保护措施。文献[14]对第三代移动通信系统网络接入安全机制进行了分析,并指出了3G的一些主要缺陷,包括未提供用户数据完整性保护。

在AKA认证方面,文献[15]鉴于序列号操作困难的问题,提出了一种新的改进协议AP-AKA,其基于移动终端和归属网络共享同一个认证密钥、两个消息认证函数、一个密钥生成函数;文献[16,17]鉴于AKA存在VLR/SGSN与HE/HLR之间交互信息流量大、VLR/SGSN存储负担重和序列数SQN同步3个问题,并借鉴了文献[18]的思想提出了基于临时密钥机制的X-AKA协议;文献[19]针对AKA存在数据流重定向攻击、故障网络中的主动攻击和序列数SQN操作困难等安全问题,提出了增强型AP-AKA协议;文献[20]指出文献[19]提出的AP-AKA协议存在IMSI标识暴露、VLR/SGSN与HE/HLR之间交互信息流量大和VLR/SGSN存储负担重等问题,采用临时密钥体制提出了新的AKA协议;文献[21]对UMTS安全框架进行了全面的评估,分析AKA协议如何抵抗各种类型攻击;文献[22]提出了基于Difie-Hellman协议的增强型AKA协议;文献[23,24]基于VLR/SGSN与HE/HLR之间共享对称密钥K,提出了各自的改进型3G认证与密钥协商协议。

3.2 4G安全的研究

目前无线通信已经发展到第四代4G,4G传输技术在安全性优于3G,主要体现在两个方面:一是频段

更宽,更难以被监听;二是与其配套制定的加解密算法更优。国外在智能电网方面关注基于4G无线网的试点建设,德国则已经开始正式发放4G牌照,并且在提供高无线通信带宽的同时探讨其安全性。

4G的标准还未正式制定,很多研究机构和学者都提出了自己的观点见解。目前,国际上提交的4G标准一共有6个技术提案包括3GPP(LTE-A)(欧洲标准化组织)、IEEE的802.16m(北美标准化组织)、基于LTE-A(日本)和802.16m(日本)、LTE-A(3GPP)、TD-LTE-Advanced(中国)、基于802.16m(韩国)。

第四代移动通信系统4G是基于宽带接入技术和分布式技术的全IP网络。4G网络将不同网络连接在一起,形成一致性、无缝的移动计算环境,达到高速移动环境下数据传输2-100Mb/s能力,支撑高质量传输语音、数据、图像。对于4G的研究,在理论界主要有两种思路:一种思路是把4G网络看做一个全IP移动网,以研究移动IP的安全[25~28]为主题进行研究;另一种研究思路是以现有无线广域网为重点,以研究与其他各种无线通信网络的互联互通为主题[29~32]。

4 电力通信中WWAN安全防护

电力系统在朝着智能电网的方向快速的建设和发展,在此期间,新通信设施的建设和安全问题是工作的重点之一。接入网是智能电网网络层的重要环节,WWAN作为无线接入网的重要通信方式,其安全性直接影响着电力物联网的整体安全。

通过对WWAN的安全分析,可以深刻地了解无线接入网中WWAN的安全现状,指导电力无线接入网的安全建设和智能电网应用层的安全建设,达到WWAN网络层安全和智能电网应用层安全紧密合作、优势互补、高效防护的整体效果。

电力系统通信中WWAN建设工作中的研究点和关注点应该包括:

(1)是否进行WWAN接入网建设,建设什么安全等级的无线接入网;

(2)租用什么安全等级的WWAN,在应用层进行哪些安全增强,如何实现安全增强。

以前,对有线网络的安全研究居多,对无线通信网络的研究较少,且只关注于其可用性及可靠性。国家电监会5号令《电力二次系统安全防护规定》等文件对电力系统通信速率、安全性等方面有着详细的规定和要求,无线通信一旦作为电力通信的一部分,其各项指标也要满足电力系统的相关安全防护要求。目前电力系统在无线通信安全防护手段上正进行进一步的深入的研究。

表2是文中对电力系统通信中WWAN自建、租用两种场景下,给出的安全增强建议。

5 结束语

寻求更好的通信方案,使通信系统不再成为电力系统通信发展的瓶颈,一直以来都是电力领域的重要研究方向,移动通信网络以其信号覆盖面广、网络质量高,在行业应用中得到了广泛的应用。而移动通信网络由于其无线传播的开放性,安全问题是WWAN通信系统的重要问题之一。

表2 电力物联网下WWAN增强建议一览表

增强建议	租用(应用层增强)	自建(网络层增强)
物理层安全		√
Iu和Iur接口安全		√
用户身份IMSI加密		√
开发自主加密算法	√	√
采用公钥算法	√	√
应用新密码技术	√	√
用户数据完整性	√	√
端到端加密	√	√

鉴于无线终端在存储能力、计算能力和电源供电时间等方面的局限性,使得原来有线网络的安全技术及方案不适用于无线环境。无线通信安全是一个包含范围广、影响深远的研究课题,有必要在未来的研究对其进行充分的分析,进行更加深入的研究。

参考文献:

[1] 张方舟,叶润国,冯彦君,等.3G接入技术中认证鉴权的安全性研究[J].微电子学与计算机,2004,21(9):33-37.

[2] 刘 锋.第三代移动通信系统中认证与密钥协商协议应用研究[D].重庆:重庆大学,2005.

[3] 张 鹏.第三代移动通信接入认证研究[D].重庆:西南交通大学,2004.

[4] 和 晨,杨 涛,诸鸿文.GSM移动通信用户鉴权算法的分析与实现[J].数据采集与处理,1999(4):38-42.

[5] Barbeau M, Robert J M. Perfect identity concealment in UMTS over radio access links[C]//Proc. of the IEEE Int'l Conf. on Wireless and Mobile Computing, Networking and Communications. Washington: IEEE Computer Society Press, 2005: 72-77.

[6] SaRarzadeh B, Asadpour M, Jalili R. Improved user identity confidentiality for UMTS mobile networks[C]//Proc. of the 4th European Cone on Universal Multiservice Networks. Washington: IEEE Computer Society Press, 2007: 401-409.

[7] 刘东苏,韦宝典,王新梅.改进的3G认证与密钥分析协议[J].通信学报,2002,23(5):119-122.

[8] 袁亚飞,廉玉忠.3G认证与密钥分发协议逻辑化分析[J].信息工程大学学报,2004,5(4):15-17.

[9] 林德敬,林柏钢,林德清.3GPP系统全系列信息安全及其算法设计与应用[J].重庆邮电学院学报,2003,15(4):18-23.

[10] 王　冉,李小文.基于TD-SCDMA系统的完整性保护算法的研究[J].信息技术,2005(10):66-69.

[11] 姚惠明,隋爱芬,杨义先.3GPP网络AKA协议中若干算法的设计[J].北京邮电大学学报,2002,25(3):98-102.

[12] 万仁福,李方伟,马剑光,等.GPRS与UMTS系统网络接入安全机制的比较与研究[J].电讯技术,2004(4):42-46.

[13] 万仁福,李方伟.GPRS与UMTS系统网络接入安全机制的比较与研究[J].重庆邮电学院学报,2004,17(1):42-45.

[14] 戴沁芸.第三代移动通信系统网络接入安全机制分析[J].现代电信技术,2010(4):12-17.

[15] Zhang Muxiang, Fang Yuguang. Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol[J]. IEEE Transactions on Wireless Communication, 2005,4(2):734-742.

[16] Huang C M,Li J W. Authentication and key agreement protocol for UMTS with low bandwidth consumption[C]//Proc. of the 19th Int'l Conf. on Advanced Information Networking and Applications. Washington:IEEE Computer Society Press, 2005:392-397.

[17] Saraireh J A,Yousef S. Extension of authentication and key agreement protocol (AKA) for universal mobile telecommunication system(UMTS)[J]. Int'l Journal of Theoretical and Applied Computer Sciences,2006,1(1):109-118.

[18] Lee C C,Hwang M S,Yang W P. Extension of authentication protocol for GSM[J]. IEEE Proc. of Communications,2003, 150(2):91-95.

[19] Zhang M X,Fang Y G. Security analysis and enhancements of 3GPP authentication and key agreement protocol[J]. IEEE Trans. on Wireless Communications,2005,4(2):734-742.

[20] Juang W S,Wu J L. Efficient 3GPP authentication and key agreement with robust user privacy protection[C]//Proc. of the IEEE Wireless Communications and Networking Conf.[s. l.]:[s. n.],2007:2722-2727.

[21] Bais A,Penzhorn W T,Palensky P. Evaluation of UMTS security architecture and services[C]//Proc. of the IEEE Int'l Conf on Industrial Informatics. Washington: IEEE Computer Society Press,2006:570-575.

[22] Jiang R,Li J H,Pan L. Formal analysis of 3GPP authentication and key agreement based on the strand space model[J]. Journal of Shanghai Jiaotong University,2006,40(5):791-795.

[23] Yuan Y F,Lian Y Z. Logic analysis of authentication key agreement protocol of 3G mobile communication[J]. Journal of Information Engineering University,2004,5(4):15-17.

[24] Liu F,Li D X. Amelioration of authentication and key agreement protocol in 3G[J]. Computer Engineering and Design, 2006,27(14):2705-2707.

[25] Marques V,Aguiar R L,Garcia C,et al. An IP-based QoS architecture for 4G operator scenarios[J]. IEEE Wireless Communications,2003,10(3):54-62.

[26] Bravo A M,Moreno J I,Soto I. Advanced positioning and location based services in 4G mobile-IP radio access networks [C]//Proc. of Int. Symposium on Personal,Indoor and Mobile Radio Communicaitons. Lisbon, Portugal: IEEE, 2004: 1085-1089.

[27] Dell'Uomo L,Scarrone E. An all-IP solution for QoS mobility management and AAA in the 4G mobile network[C]//Proc. of Int. Symposium on Wireless Personal Multimedia Communication. Hawaii,USA:IEEE,2002:591-595.

[28] Santhi K R,Kumaran G. S. Migration to 4G:Mobile IP Based Solutions[C]//Proc. of Int. Conf. on Internet and Web Applications and Services. Guadeloupe, French: IEEE Computer Society,2006:76-76.

[29] Kojen G M,Haslestad T. Security Aspects of 3G-WLAN Interworking[J]. IEEE Communication Magazine,2003,41(5):82-88.

[30] Salkintzis A K. Interworking Techniques and Architecture for WLAN/3G Intergration Torward 4G Mobile Data Networks [J]. IEEE Wireless Communication,2004,11(3):50-61.

[31] Salkintzis A K,Fors C,Pazhyannur R. WLAN-GPRS Integration for Next-Generation Mobile Data Networks[J]. IEEE Wireless Communication,2002,9(5):112-124.

[32] Kambourakis G,Rouskas A,Kormentzas G,et al. Advanced SSL/TLS Communication[J]. IEEE Proceedings,2004,151 (5):501-506.

(上接第244页)

李成法,陈贵海.一种基于非均匀分簇的无线传感器网络路由协议[J].计算机学报,2007,30(1):88-91.

[10] 杨菊英,吕光宏.无线传感器网络分层路由协议研究[J].计算机技术与发展,2008,18(6):115-118.

[11] 周贤伟,覃伯平.基于能量优化的无线传感器网络安全路由算法[J].电子学报,2007,35(1):54-57.

[12] Imamoto K,Sakurai K. A Design of Diffie-Hellman Based Key Exchange Using One-time ID in Pre-shared Key Model [C]//The 18th International Conference on Advanced Information Networking and Applications.[s. l.]:[s. n.],2004: 327-333.