基建调试和电网故障移动应急远动系统

周恒俊[1],郭创新[1],范 斗[2],陈 济[1]
(1. 浙江大学 电气工程学院,浙江 杭州 310027;
2. 河南省电力公司 调度通信中心,河南 郑州 450052)

摘要:在分析比较远动系统中有线通信模式和无线通信模式运行特性的基础上,对基于 GPRS & CDMA 的基建调试和电网故障移动应急远动系统进行了研究。该系统融合访问点域名 APN 服务、虚拟专用网技术和 IPSec 安全认证技术对系统进行全方位安全防护,采用双网热备和规约校验重传技术保证通信网络数据传输的可靠性,以创新的智能分包数据传输模式提高系统的实时性。系统在现场进行了测试,在运行过程中保持了极低的误码率和延时,满足基建调试过程中远动通信的要求,验证了远动系统中无线通信模式的可行性。

关键词:GPRS & CDMA;双网热备;访问点域名;IPSec 协议;虚拟专用网;智能分包
中图分类号:TM 734 **文献标识码**:A **文章编号**:1006-6047(2010)03-0085-05

0 引言

远动系统是关系到电网安全稳定运行的重要设备,随着智能电网(Smart Grid)概念的提出,建设快速、灵活、经济的远动系统成为研究热点之一[1-2]。而现有远动系统多采用有线通信模式,一方面安装成本高,在通信量较小时造成巨大的资源浪费,另一方面受到布线的限制,通信网络部署周期长且缺乏一定的扩展性和灵活性[3-12]。

收稿日期:2009-06-28;**修回日期**:2009-09-11
基金项目:国家自然科学基金项目(50677062);新世纪优秀人才支持计划资助项目(NCET-07-0745);浙江省自然科学基金资助项目(R107062);国家 863 计划项目(2008AA05Z210)

本文在对远动系统中有线通信模式和无线通信模式分析比较的基础上,提出基于 GPRS & CDMA 的基建调试和电网故障移动应急远动系统方案,该方案综合采用先进的网络管理技术、信息安全技术、容错技术和新的数据传送机制,克服了远动系统中无线通信模式易受干扰、安全系数低、延时长的问题。

1 远动系统通信模式探讨

新一代基于以太网的远动系统是集计算机技术、网络管理技术、集成通信技术和信息安全技术于一体的数字化通信平台。选择一个合理的通信模式对数字化远动系统的建立显得尤为重要。具备高速率、大容量、抗电磁干扰强等特性的有线通信模式(如光纤通信)能够满足大部分远动通信的需要,但由于

有线通信模式必须铺设通信介质(如光纤)作为通信信道,因此施工时间长、安装成本高,且通信信道一旦遭人为或自然灾害破坏后,故障定位困难,影响到远动系统的安全稳定运行。

无线通信模式(如 GPRS & CDMA)以公共电磁波为通信信道,因其施工维护简单、安装费用低、建设周期短、组网灵活等优点可弥补远动系统中有线通信模式的不足,覆盖有线通信模式无法覆盖的盲点,解决有线通信模式无法解决的问题。无线通信模式的应用场景如图 1 所示。

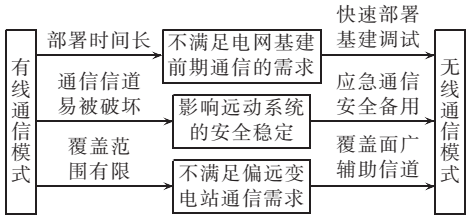


图 1 无线通信模式的应用场景

Fig.1 Applications of wireless communication mode

但是,无线通信模式也存在着安全系数低、易受干扰、通信延时长等缺点,要在远动系统中采用无线通信模式,还必须解决信息传送的安全性,即数据传输满足二次系统安全防护的要求,实现信息的认证和加密。同时,为解决无线数据传输的抗干扰和时延问题,利用冗余通信技术和规约校验与重传技术,优化数据传输机制,保证数据传输的可靠性和实时性。

2 应急远动通信系统实现策略

通过对远动系统通信模式的探讨,提出基于 GPRS & CDMA 的基建调试和电网故障移动应急远动系统方案。

2.1 通信系统结构

图 2 中变电站和调度中心都通过串口和远动安全网关 RSG(Remote Security Gateway)相连,避免公网的非法信息侵害变电站和调度中心自动化运行设备。变电站侧 RSG 将报文数据打成 IP 包,并经过

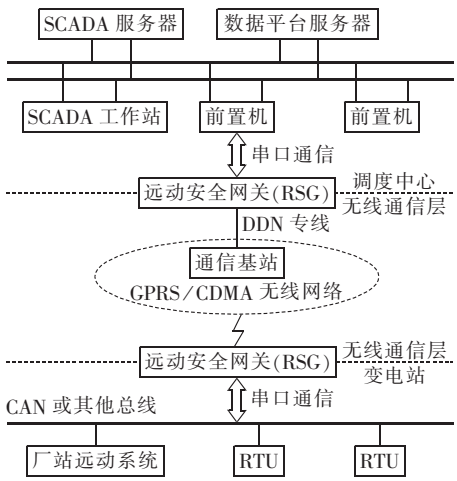


图 2 应急远动系统体系结构

Fig.2 Architecture of emergency tele-control system

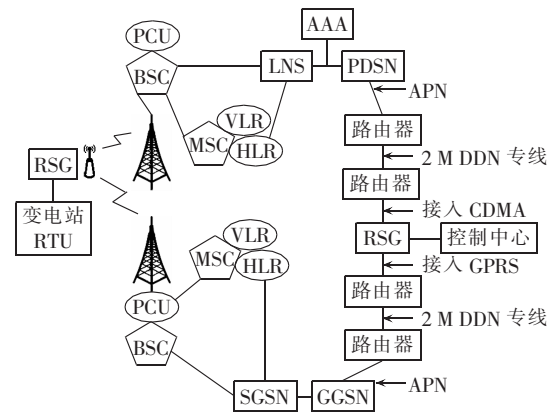
IPSec 协议二次加密,再通过无线发射终端传入到 GPRS & CDMA 网,最后通过调度中心侧 RSG 解密到达系统 SCADA 中心。应急远动系统体系结构如图 2 所示。

2.2 无线通信组网方式

无线通信模式的组网方式主要包括 GPRS 和 CDMA 2 种方式,2 种方式在控制中心侧均采用内网 APN 专线方式进行连接,即从电信公司后台服务器牵出一根 2 M 的 DDN 专线与调度中心远动安全网关连接,由电信公司提供固定 IP 地址;在变电站侧采用固定 IP 地址的 SIM 卡通过远动安全网关的无线发射终端接入 GPRS(或 CDMA)。

GPRS 和 CDMA 2 种组网方式只在电信公司网络运行中心 NOC(Network Operation Center)部分有些不同,通用无线分组业务 GPRS(General Packet Radio Service)组网方式是在原有 GSM 网络结构中增添 3 种新的网络节点(分组控制单元 PCU、GPRS 业务支持节点(SGSN)和 GPRS 网关支持节点(GGSN))以及对 GSM 的相关部件进行软件升级来实现。码分多址分组数据传输技术 CDMA(Code Division Multiple Access)采用分组数据服务节点 PDSN(Packet Data Service Node)作为接入网关,AAA 对用户实现鉴权、授权和计费功能。

GPRS 和 CDMA 2 种组网方式均支持 TCP/IP 协议和 X2.5 协议。在GPRS & CDMA上可开发基于 IPSec 协议的虚拟专用网 VPN(Virtual Private Network)和访问点域名 APN(Access Point Name)业务。其详细网络结构如图 3 所示。采用这种组网方式的数据安全性好,稳定性可靠,传输延迟小(低于 1 s),能满足大部分报文传输的实时性要求。



PDSN:分组数据服务节点 SGSN:业务支持节点 PCU:分组控制单元
LNS:L2TP 网络服务器 GGSN:网关支持节点 BSC:基站控制器
AAA:鉴权、授权和计费 VLR:拜访位置寄存器 MSC:交换中心
HLR:归属位置寄存器

图 3 无线通信详细组网方式

Fig.3 Structure of wireless communication network

2.3 全方位安全防护设计

由于无线网络采用公共的电磁波作为载体,任何人都有条件窃听或干扰信息,因此在无线网络中,网络安全显得尤为重要。系统远动安全网关从网络

接入点、网络传输通道、传输数据加密认证 3 方面对无线通信层做了全方位的安全防护设计。

2.3.1　APN 专线接入

为了确保网络接入的安全性,采用了电信公司提供的访问点域名 APN(类似互联网的 DNS 域名)服务,该 APN 为电力公司专有 APN,对访问接入范围进行了严格的限制。通过将 APN 与终端静态 IP 地址绑定,使只有属于自己的特定终端 IP 地址才可访问自己的 APN。电力公司如果需要增加该 APN 的设备,必须由电力公司出具授权书,委派移动公司另行开卡接入,确保该 APN 的安全性。

2.3.2　基于 VPN 隧道技术的网络架构

虚拟专用网 VPN[13]依靠 Internet 服务提供商 ISP(Internet Service Provider)和其他网络服务提供商 NSP(Network Service Provider)在无线网络中建立专用的数据通信通道,通过私有的隧道技术在公共无线网络上仿真一条点到点的专有网络,它并不是真的专有网络,却能提供专有网络的功能。如图 4 所示的网络结构中,调度中心和变电站内部局域网都受到远动安全网关的保护。安全网关的出口 IP 地址设置为无线网络专网静态地址。通过这样的安全配置对接入访问的范围和资源进行限制,2 个子网之间传输的数据都是经过 2 个安全网关协商后处理过的加密和认证的数据。信息在网关之间的专有隧道上传输,保证了数据在公共网络上的传输安全,从而构成一个有安全保证的 VPN。即使外部用户非法获取这些数据也不会对源主机或网络造成巨大的威胁。

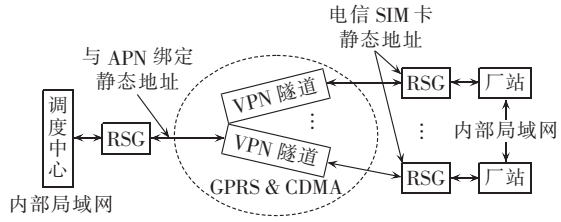


图 4　VPN 通信结构

Fig.4　Structure of VPN communication

2.3.3　传输数据的加解密技术

IPSec 安全认证技术[14]是在网络层上对数据包进行安全处理,从而提供数据源验证、无连接的数据完整性、数据机密性、抗重播和有限的业务流机密性等安全服务。IPSec 体系是一个开放性的标准框架,它包括 3 个主要的安全协议,即认证头协议 AH(Authentication Header)、封装安全有效载荷协议 ESP(Encapsulating Security Payload)和密钥交换协议 IKE(Internet Key Exchange)。

如图 4 中 VPN 两端连接的都是具有 IPSec 安全认证的远动安全网关,远动安全网关采用工业级服务器,通过 HTTPS 加密通信数据协议访问安全网关服务器,经过身份认证后,设置网关的安全策略。调度中心和厂站之间传输的网络数据都是经过远动安全网关协商后处理过的加密和认证的数据。每个远动安全网关都是一个网络聚合点,目的地是 VPN 的所有通信,都经过安全网关上的认证头协议 SA 来定义加密或认证的算法和密钥等参数,即从 VPN 的一个安全网关出来的数据包只要符合安全策略,就会用相应的 SA 来加密或认证(加上 AH 或 ESP 包头)。所有的加密和解密由两端的安全网关全权代理,其详细处理流程如图 5 所示。

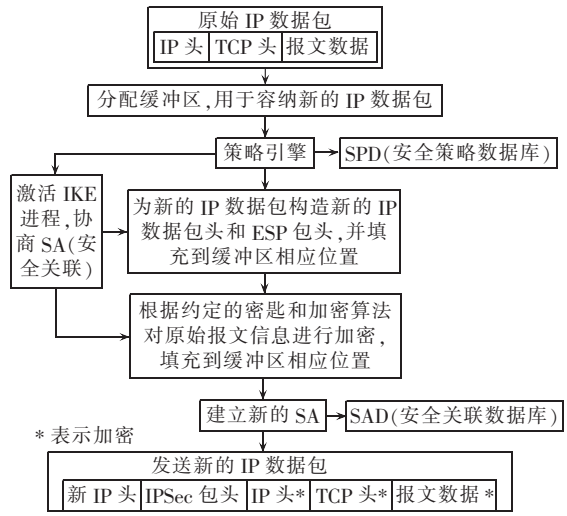


图 5　安全网关加密流程

Fig.5　Security gateway encryption process

2.4　双网热备与规约校验

鉴于无线信号的不稳定性,变电站侧采用双网热备技术提高通信网络的可靠性。双网热备技术即 GPRS 和 CDMA 互为热备用,考虑到 CDMA 网络在传输速率方面的优势,优先连接 CDMA 网络。

图 6 显示了双网热备机制的工作流程,当 CDMA 网络发生故障连接中断时,系统自动切换到 GPRS 网络,同时利用断点续传功能在传输网络切换后,保持数据传输的连续性,以防止无线网络的不稳定性导致数据丢失和误码。网络连接中断的 CDMA 网络通过自动重连功能,自动拨号尝试接入 CDMA 网络,一旦再次连接成功,即进入热备状态。如在 5 min 内仍不能接入网络,及时给出报警,提醒相关人员注意。由于处于热备状态的网络没有报文数据的传输,因此采用心跳功能(即当长时间没有数据通信时,在

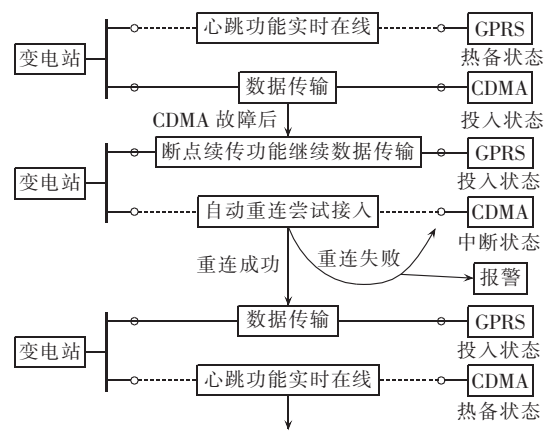


图 6　双网热备机制

Fig.6　Hot-standby mechanism of dual-network

连接被断开之前发送一个小数据包,以保持连接不被断开)保证其实时在线。

此外,利用基于TCP/IP协议的远动通信规约的数据校验和重传功能,进一步保证远动数据的完整性和正确性。以IEC60870-5-104规约[15]抗报文丢失和报文重复传送机制为例,在创建一个TCP连接后,将发送序列号N(S)和接收序列号N(R)设置为0。2个序列号在每个应用规范数据单元APDU和每个方向上都应按顺序加一。发送方增加发送序列号而接收方增加接收序列号。当接收站按连续正确收到的APDU的数字返回接收序列号时,表示接收站认可这个APDU或者多个APDU,发送站把一个或几个APDU保存到一个缓冲区里直到它将自己的发送序列号作为一个接收序列号收回,而这个接收序列号是对所有数字小于或等于该号的APDU的有效确认,这样就可以删除缓冲区里已正确传送过的APDU。

2.5 智能分包数据传输模式

变电站通信网络和系统国际标准[16]定义了7种类型的报文,即:快速报文、中速报文、低速报文、原始数据报文、文件传输报文、时间同步报文和具有访问控制的命令报文。本文采用的智能分包数据传输模式(见图7)对上述7种类型的报文再次进行了分类,主要分为3种类型进行通信:模拟量通信、状态量通信和控制量通信。

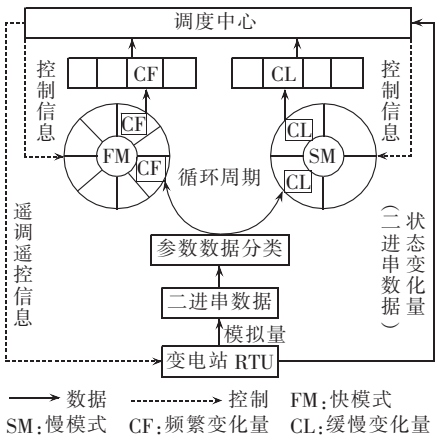


图7 智能分包数据传送模式

Fig.7 Smart sub-packet data communication mode

智能分包数据传送模式主要包括以下4点。

a. 实现所有模拟信号到数字信号的转变,并将每个RTU大约32位数字输入映射进一串二进位信息中,从而有助于通过单一数据包即可报告所有信息,也有助于将多重变化量纳入单一数据包。

b. 无控制作用的模拟量和模拟变化量采用周期应答方式,不同类型的实时数据设置不同的循环周期,如电流、有功功率等频繁变化的实时数据设置较短的循环周期,其他实时数据设置较长循环周期。

c. 将相同循环周期的数据放入同一数据组传输,采用快慢2种循环扫描模式,由调度中心控制模式的切换。

d. 利用IP报文头中的服务类型TOS(Type Of Service)对状态量和控制量通信设置高的通信优先级,满足其较高的时限要求。

通过采用智能分包数据传输模式,减少了无线网络的数据传输量,改善了实时数据的更新时间,使得移动应急远动系统的实时性要求得到满足。

3 应用实例

利用河南某新建大型电厂远动调试的机会,在保证电网安全的前提下,将移动应急远动通信系统应用于电厂基建调试并对系统进行了全面的测试。

测试系统在现场共运行了23天,其中GPRS网络共断线2次,CDMA网络共断线4次,当其中一个网络断开连接后,另外一个网络能顺利切换进入运行状态。系统运行在GPRS网络状态时,传输报文的准确性、数据延时比在CDMA网络状态时要略低,其原因主要是CDMA网络比GPRS拥有更高的带宽和更快的传输速率。系统测试结果如表1所示。

表1 系统测试结果(23天)

Tab.1 Results of system test(23 days)

网络	断线次数	误码率	平均速率	时延
GPRS	2	10^{-4}数量级	>78 Kbit/s	<1 s
CDMA	4	10^{-5}数量级	>110 Kbit/s	<0.8 s

通过测试证明,若在电厂至省调的自动化通道不具备的情况下,利用无线信道协助电厂将RTU数据通过远动规约完整并正确地上送到了省调,实现了模拟主站提前与RTU对接,以协助RTU厂家进行数据点和报文的校对和测试,为通信通道具备时顺利并快速将数据上送到省调提供了保证。

4 结语

本文提出的移动应急远动通信系统方案,解决了远动系统无线通信模式中最主要的可靠性、安全性和实时性问题,但限于无线通信技术在通信带宽、通信速率、系统稳定性等方面固有缺陷的影响,其应用范围还仅限于电网基建调试、故障应急通信和偏远变电站通信,不足以取代有线通信在电力系统远动通信中的位置。但随着3G通信技术的推广,无线通信模式在电力系统远动通信中的应用范围将更为广阔,在其基础上开发手持移动终端访问SCADA系统,也将是下一步研究的重点。

参考文献:

[1] 卢强. 数字电力系统[J]. 电力系统自动化,2000,24(9):1-4.
LU Qiang. Digital power systems[J]. Automation of Electric Power Systems,2000,24(9):1-4.

[2] 李向荣,郝悍勇,樊涛,等. 构筑数字化电网建设信息化企业[J]. 电力系统自动化,2007,31(17):1-5.
LI Xiangrong,HAO Hanyong,FAN Tao,et al. Constructing digital grid and informatized enterprise[J]. Automation of Electric Power Systems,2007,31(17):1-5.

[3] CHOI T I,LEE K Y,LEE D R,et al. Communication system for

distribution automation using CDMA[J]. IEEE Trans on Power Delivery,2008,23(2):650-656.
[4] 唐海军. 基于 GPRS 的配电网馈线自动化模式探讨 [J]. 电力系统自动化,2006,30(7):104-107.
TANG Haijun. The investigation about distribution feeder automation mode based GPRS[J]. Automation of Electric Power Systems,2006,30(7):104-107.
[5] 李惠宇,罗小莉,于盛林. 一种基于 GPRS 的配电自动化系统方案[J]. 电力系统自动化,2003,27(24):63-65.
LI Huiyu,LUO Xiaoli,YU Shenglin. A GPRS based distribution automation system[J]. Automation of Electric Power Systems,2003,27(24):63-65.
[6] 苗世洪,谌小莉,刘沛,等. 基于无线传感器网络的配电线路故障定位方案[J]. 电力系统自动化,2008,32(20):61-66,82.
MIAO Shihong,CHEN Xiaoli,LIU Pei,et al. A distribution lines fault location schema based on wireless sensor network[J]. Automation of Electric Power Systems,2008,32(20):61-66,82.
[7] CLLEVELLAND F. Use of wireless data communications in power system operations[C]//2006 PES Power Systems Conference and Exposition. Chongqing,China:IEEE,2006:631-640.
[8] 所旭,张萍. 无线通信技术应用于变电站自动化的探讨[J]. 电力系统自动化,2004,28(17):88-91.
SUO Xu,ZHANG Ping. A discussion on wireless communication and its application in the substation automation system[J]. Automation of Electric Power Systems,2004,28(17):88-91.
[9] 黄新波,刘家兵,王向利,等. 基于 GPRS 网络的输电线路绝缘子污秽在线遥测系统[J]. 电力系统自动化,2004,28(21):92-96.
HUANG Xinbo,LIU Jiabing,WANG Xiangli,et al. On line remote monitoring system for transmission line insulator contamination based on the GPRS net[J]. Automation of Electric Power Systems,2004,28(21):92-96.
[10] GUI Xun,YAO Lan,LIU Zhigang,et al. General power transmission line on-line monitoring software system based on wireless public network[C]//Proceedings of the 7th World Congress on Intelligent Control Automation. Chongqing,China:IEEE,2008:2777-2782.
[11] 黄敏,李达,朱婷. 基于 CDMA1X 网络的架空输电线路无线视频监控系统[J]. 电力系统自动化,2007,31(5):101-107.
HUANG Min,LI Da,ZHU Ting. A wireless video surveillance system about overhead transmission lines based on GPRS[J]. Automation of Electric Power Systems,2007,31(5):101-107.
[12] CHEUNG R W L,FUNG Y F. Wireless access to SCADA system[C]//Proceedings of the 5th International Conference on Advances in Power System Control,Operation and Management. Hong Kong,China:IEEE,2000:553-556.
[13] BROWN S. 构建虚拟专用网[M]. 董晓宇,魏鸿,马洁,等,译. 北京:人民邮电出版社,2000.
[14] 唐佳佳,周晓东,陆建德. IPsec VPN 安全网关的认证优化设计与实现[J]. 计算机应用与软件,2008,25(5):59-61.
TANG Jiajia,ZHOU Xiaodong,LU Jiande. Optimized authentication design and implementation of IPSec VPN security gateway[J]. Computer Applications and Software,2008,25(5):59-61.
[15] 国家经济贸易委员会. DL/T 634.5104-2002,IEC60870-5-104-2000.远动设备及系统,第 5-104 部分:传输规约采用标准传输协议子集的 IEC60870-5-101 网络访问[S]. 北京:[出版者不详],2002.
[16] IEC. Communication networks and systems in substations[S]. Geneva,Switzerland:IEC,2001.

(**责任编辑**:康鲁豫)

作者简介:

周恒俊(1984-),男,江苏镇江人,博士研究生,研究方向为智能信息处理技术在电力系统中的应用、分布式电源并网技术(**E-mail**:zhj221@zju.edu.cn);

郭创新(1969-),男,湖北黄岗人,教授,博士研究生导师,研究方向为智能电网和分布式能源并网、智能信息处理技术及其在电力系统中的应用;

范　斗(1969-),男,河南郑州人,高级工程师,硕士,研究方向为电力调度自动化;

陈　济(1985-),男,浙江温州人,硕士研究生,研究方向为智能信息处理技术在电力系统中的应用。

Mobile emergency tele-control system based on GPRS & CDMA

ZHOU Hengjun[1],GUO Chuangxin[1],FAN Dou[2],CHEN Ji[1]
(1. Zhejiang University,Hangzhou 310027,China;
2. Henan Electric Power Company,Zhengzhou 450052,China)

Abstract: The operating features of wire and wireless communication modes used in tele-control system are analyzed and the mobile emergency tele-control system based on GPRS & CDMA is studied,which integrates the technologies of Access Point Name service,Virtual Private Network and IPSec security authentication to protect the system security in all aspects,applies the technologies of dual-network and protocol checksum retransfer to ensure the reliability of network data communication,and adopts the smart sub-packet transfer mode to improve the real-time performance of system. The site test shows its extremely low error rate and communication lag,satisfying the requirements of tele-control communication,and validates the feasibility of wireless communication mode in tele-control system.

This work is supported by the National Natural Science Foundation of China(50677062),the New Century Excellent Talents in University(NCET-07-0745),the Natural Science Foundation of Zhejiang Province(R107062),and the National 863 Plans(2008AA05Z210).

Key words: GPRS & CDMA; dual-network; APN; IPSec protocol; VPN; smart sub-packet