文章编号:1001 - 893X(2010)05 - 0094 - 05

现代数字通信网有效攻击技术*

王红军

(解放军电子工程学院,合肥 230037)

摘 要:根据现代数字通信网的特点,针对无中心节点分布式网络,依据可利用的截获信息提出了基于网络层、链路层、物理层和内核、伪网、伪帧等有效攻击技术。此外,结合可能无细微先验知识的限制,提出了有限盲攻击技术。其中部分攻击技术已成功应用,试验结果表明所提出的有效攻击技术具有较高的攻击效能,其应用前景广阔。

关键词:数字通信网;链路层攻击;物理层攻击;内核攻击;伪网攻击;伪帧攻击

中图分类号:TN92 **文献标识码**:A doi:10.3969/j.issn.1001 - 893x.2010.05.021

Effective Interference Technology for Modern Communication Networks

WANG Hong-jun

(PLA Electronic Engineering Institute, Hefei 230037, China)

Abstract: According to the characteristic of modern communication networks, the effective interference technology based on network layer, link layer, physical layer, inner core, pseudo network and pseudo frame, is put forward on the basis of reconnaissance information to networks without the key nodes. The limited blind interference technology is presented in terms of no subtle priori knowledge. Parts of the effective interference technology have been applied in project. The experiment result shows the interference technology has more effective interference performance, and more extensive application prospect.

Key words: digital communication network; link layer interference; physical layer interference; inner core interference; pseudo network interference; pseudo frame interference

1 引 言

现代数字通信网综合了核心网络、无线接入单元和移动终端等设备,为便于后续阐述通信网的有效攻击技术,在此将核心网络和无线接入单元统称为网络侧,而移动终端则称为终端侧。需要说明的是,现代数字通信网中内部实体之间所有相关协议均采用了 SS7 类接口协议,其中最为重要的就是 MAP 协议,而与其它子网或网络之间的通信则基本采用了 IPv6 类协议。

常规的干扰或者对抗技术基本从信号层入手[1-2],包括目前常提到的灵巧式干扰技术,都没有尽可能地利用信息层信息,理论、仿真和试验表明:对这类无中心节点的通信网络仅采用阻塞式、转发式或扫频式依靠功率压制来进行干扰几乎没有效果。本文依据射频技术和信号处理技术的发展,以及截获手段的多样化,结合现代数字通信网的特点和越来越有可能获取的信息,提出了灵巧式攻击的

* **收稿日期**:2009 - 12 - 14;**修回日期**:2010 - 03 - 19
基金项目:"十一五"国防预研项目(41101040604)
Foundation Item: The National Defense Advanced Research Project in The 11th Five-year Plan(No.41101040604)

定义并对有效技术进行了详细阐述,认为相对灵巧式干扰而言,灵巧式攻击更具理论价值和实际意义,干扰从概念上和实际应用上只是解决了物理层的问题,而攻击则涉及到系统的各个层面。

2　网络侧的有效攻击技术

网络层解决的是网络与网络之间,即网际通信问题。相对于无线数字通信系统而言,网络层协议通常指的是通信系统间和系统内部实体之间的接口协议,较为重要的协议包括 MAP 协议和 A 接口协议,其中 MAP 协议采用交换协议数据和会话的方式实现各实体之间的通信,而 A 接口协议则负责完成移动和无线资源等管理。为了满足用户对数据速率的要求,IP 技术在该领域也得到越来越广泛的应用,使得恶意代码和恶意病毒的攻击成为可能。网络侧的有效攻击技术主要包括以下 4 个方面。

2.1　基于网络层的灵巧式攻击技术

针对核心网络的攻击,生成的攻击信号必须符合该通信网的协议,数据流能够通过无线接入单元透传到网络内部。

2.1.1　“合法”网络攻击法

攻击平台借助网络认可的设备,通过合法的通信过程发起对网络的攻击,如在移动通信系统中,可借助合法的终端、合法身份卡和控制台构成攻击设备。首先攻击设备需要对体系结构进行探测,即利用具有已知响应类型的数据库的自动工具,通过实时的回环数据链路对来自目标系统的和对坏数据包传送所做出的响应进行检查。由于每种操作系统都有其独特的响应方法,通过将此独特的响应与数据库中的已知响应进行对比,能够确定出目标主机所运行的操作系统。根据截获结果则可采用如下技术继续攻击:

(1)信息炸弹技术:在 A 接口协议的业务控制和无线资源管理、MAP 接口协议的业务处理、客户管理、操作和维护协议上借助终端指令集大量地发送短信、图像、电子邮件或 IP 包,耗尽网络的带宽,导致有效申请率降低,使系统容量下降;

(2)畸形消息攻击技术:各类操作系统上的许多服务都存在此类问题,由于这些服务在处理信息之前没有进行适当正确的错误校验,在收到畸形的信息时可能会崩溃。主要在 A 接口协议的指配、资源指示、切换、初始消息、排队指示、数据链路控制和移动管理上,以及 MAP 交换协议的呼叫建立期间客户参数的检索和切换上实现该功能;

(3)夹心毒面包技术:发送符合系统标准的携带病毒的短信、图像或 IP 数据流,借助终端指令集利用网络所采用的操作系统的漏洞,通过 MAP 协议和 A 接口协议对系统和各类数据库(如位置归属寄存器等)进行攻击,瘫痪其系统。

2.1.2　“非法”网络攻击法

在无法获得合法身份时,则可以通过非法途径进行攻击,首先是完成空闲时隙或者空闲码道的截获,即利用认知无线电技术,探测出系统空闲的时频信息,在系统不加以处理和识别的时隙或码道上上传信息进行攻击,具体技术包括:

(1)死亡之拼攻击技术:借助终端指令集产生畸形的超出数据帧尺寸的 IP 包,导致系统处理内存分配错误,致使系统崩溃;

(2)病毒流水线技术:网络对于空闲的时隙或码道,一般不进行数据处理,因此攻击设备可在所有探测出的空闲时隙或码道上,连续发送各种病毒程序,在网络没有察觉的情况下,借助该通道完成对系统的病毒注入。通过该手段可以进行病毒潜伏,伺机对系统和数据库进行攻击。

2.2　基于链路层的有效攻击技术

链路层的功能是建立、维持和释放网络实体之间的数据链路,对数据进行编码和编帧。数据链路层把流量控制和差错控制结合在一起进行。针对网络侧链路层的有效攻击技术主要为伪终端技术,即依据攻击对象发送符合其标准协议的复帧结构,对核心网络和重要无线接入单元进行攻击。

(1)伪复帧攻击技术

严格按照所针对的网络,利用有效的训练序列或者扰码,结合随机无效数据,根据信道估计和时延估计的结果,在对应信道上发送,使得网络在有效的训练序列或者扰码情况下,正常用户信息受到攻击而无法解析。

(2)病毒复帧攻击技术

严格按照所针对的网络,利用有效的训练序列或者扰码,结合病毒数据,根据信道估计和时延估计的结果,在对应信道上发送,一方面对落到该时隙或码道上的用户进行攻击,另一方面一旦网络进行数据处理,则引爆及时性病毒,使得网络最终瘫痪。

2.3　基于物理层的有效攻击技术

物理层作为系统和通信介质的接口,用来实现

数据链路实体间透明的比特流传输。攻击技术主要体现在无线接口上,对于网络侧而言,即依据攻击对象发送符合其标准协议的单帧结构进行攻击。

(1)伪接入攻击技术

利用截获到的网络接入信道或者接入码道,借助终端指令集以单帧形式连续发送接入申请,使得采用 ALOHA 碰撞避免体制的系统无法处理正常申请,导致系统接入信道或者接入码道崩溃。

(2)伪应答攻击技术

根据针对的网络和其应答的帧结构和帧要求,借助终端指令集在合适的时隙和码道上发送应答信息,使得网络产生误判决发出错误指令导致网络工作紊乱。

(3)伪匹配攻击技术

利用截获的同步训练序列或者扰码信息组合成符合协议的帧,再结合随机攻击数据,借助终端指令集在同步基础上与特定用户的帧信号同步达到网络,使得网络无法解析信息。

该技术和后续的盲灵巧式攻击技术可以根据需求在不同的时隙、频隙或码道上采用分时攻击方法,使得攻击设备能够有效攻击多个目标。

2.4 盲灵巧式攻击技术

对于未知系统且难以解析协议层或者信令层协议,则可以通过信号截获手段获取频点、带宽和调制样式等信息,然后根据实际情况对无线接入单元进行攻击。主要采用随机攻击技术,即根据截获的带宽和调制样式信息,在相应频率上以随机数据进行调制,以连续或者时分发送的方式对网络进行攻击。

3 终端侧的有效攻击技术

终端侧的有效攻击技术主要包括以下 4 个方面。

3.1 基于内核的灵巧式攻击技术

对终端侧内核攻击只能利用具有合法身份的攻击设备来进行,因为每个终端不仅只对应其唯一的时隙和码道,而且种类较多,一般拥有多种操作系统,如 Symbian OS、Palm OS、Microsoft Smartphone OS 和 Linux OS,并且具有 GUI、办公套件和手写识别功能,装载和运行各种各样的程序软件。终端内核通常均具备微处理器、基本库和功能库、通信体系结构、应用程序、引擎和协议等特性。针对终端内核的特点可以通过如下方式对终端进行攻击:

(1)隐形信息攻击技术:利用选择性群发措施,在其它终端没有察觉被动接收的情况下,通过传输系统约定的信息传播特洛伊木马和恶意代码,感染宿主并自动进行复制,根据实际情况瘫痪终端的通信,或者随时开启与关闭终端,窃取终端自身相关信息或者监听该终端周围接收灵敏度范围内的语音类信息。所谓隐形即是采用一定的技术措施使得对方在没有任何察觉的情况下终端被激活且被传输了一定的信息;

(2)恶意扫描攻击技术:可根据号码段对用户进行扫描传播 Mabir.A 类手机病毒,使得被扫描终端成为“肉鸡”,实现用户级和内核级 RootKit,替换或修改终端使用的可执行程序,用来隐藏和创建后门,使得终端为我所控;

(3)自动蓝牙攻击技术:对于具备无线蓝牙功能的终端,在没有用户干预的情况下启动终端自动从远端系统下载的病毒、恶意移动代码和后门软件,越过一般的保密控制为攻击者提供通道,并通过网络自动复制传播。

在完成对终端的控制后,可以通过触发等方式使得终端无法通信或者为我定时提供相关有用信息。

3.2 基于伪网的灵巧式攻击技术

基于伪网的灵巧式攻击可通过对终端采用伪装网络,根据网络的一系列信令特点,发出改变终端正常状态的且终端能够接收的合法指令,来诱惑和控制终端的方式来进行。

(1)伪基站攻击技术

又称为伪接入单元攻击技术、伪 RAU 攻击技术,根据所针对的网络体制和标准,由攻击设备发送包含连续的含导频(或 FCCH)、同步等符合协议的复帧同步信息,并分发接入信道或者接入码道信息,使得终端将攻击设备视为其合法可用的网络,将之作为其当前网络。在其发起通信请求时,攻击设备也发出相应的应答信息,使得终端始终处于无法摆脱又无法通信的状态,此时对帧结构要求严格,必须为符合标准的复帧数据格式。

(2)伪鉴权攻击技术

利用网络具备的合法性检查的“特权”,对终端发送鉴权指令,截取终端的身份号码,使得终端用户的身份参数为我所控。

(3)伪加密攻击技术

在伪鉴权过程中,攻击设备可根据实际情况发出不同于当前网络所用的加密要求,使得网络和对方终端无法解析其信息而导致其无法进行有效通信。

(4)伪切换攻击技术

根据截获的终端切换请求信息,发出切换指令,将终端引导到另一个终端所在的时隙或者码道上,使之发生信息碰撞,中断双方的有效通信,并且可有效降低网络的容量。

此外,还可以实施“伪测量”等指令,使得终端做出网络难以“理解”的行为,影响网络和终端的正常工作。

3.3　基于伪帧的灵巧式攻击技术

基于伪帧的攻击即是对网络的导频或者 FCCH、同步等信息进行攻击,该类攻击技术需要截获到网络的导频头或者帧同步头,并进行信道和时延估计。需要强调的是,此时的帧结构符合复帧的要求,但只发送部分帧数据进行攻击,其它帧没有严格要求。具体可采用如下方式展开:

(1)导频(或 FCCH)攻击技术:搜索导频(或 FCCH)是所有终端进行同步的前提条件,破坏或者恶化该信息可起到关键性作用,因此攻击设备可根据截获到的同步信息在截获到的频点上,根据所攻击的网络发送符合攻击对象协议的伪导频(或伪 FCCH)信息,使得终端散失频率纠正与搜索能力,无法实现载波同步,使得难以进一步解析同步信息而导致其瘫痪;

(2)同步攻击技术:在完成载波同步后,终端需要连续对同步信息进行解调和解码,针对该特点,攻击设备可在截获到的时隙或者码道,以相应的训练序列或者扰码,结合随机数据在比特同步的基础上进行攻击,使得终端难以解析同步信息而失去与系统通信能力;

(3)信息帧攻击技术:通过截获到的用户数据的帧同步头,通过时延估计,在完全时隙或码道匹配的情况下,采用连续或者时分方式发送攻击数据,数据包含训练序列或者扰码加成帧随机数据,使得特定或非特定终端无法进行通信。

上述技术也可组合使用,如采用“导频 + 同步”攻击技术。该技术和后续的盲灵巧式攻击技术可以根据需求在不同的时隙、频隙或者码道上采用分时攻击方法,使得攻击设备能够有效攻击多个目标。

3.4　盲灵巧式攻击技术

同样,在对于未知系统且难以解析协议层或者信令层协议,则可以通过信号截获手段获取频点、带宽和调制样式等信息,采用比特攻击技术,在相应频率上以随机数据进行调制,并结合采样解调后的同步比特信息,以连续或者时分发送的方式对网络发给终端的信息进行比特对齐式的攻击,最大限度地扰乱其接收特性,使其难以有效解码。

4　有效攻击技术性能分析

对于网络侧,经过理论推导和计算机仿真,基于网络层的现代通信网灵巧式攻击技术与计算机网络攻击技术具有相当的效果[3-4];基于链路层和物理层的灵巧式攻击技术相比其它干扰手段,可以大大降低攻击设备的所需功率。灵巧式攻击试验结果如表 1 所示。

表 1　网络侧攻击试验结果

Table 1 The test result of interference to network

系统体制	信号功率/dBm	干扰方式	攻击样式	所需功率/dBm	备注
时分/频分	-80	非灵巧式干扰	噪声 FM	-70	
			单音	-71	
		灵巧式干扰	基于链路层	-78	
			基于物理层	-79	
			盲灵巧式	-74	
码分体制	-80	非灵巧式干扰	噪声 FM	-60	扩频增益为 20 dB
			单音	-59	
		灵巧式干扰	基于链路层	-78	
			基于物理层	-77	
			盲灵巧式	-64	

表中的信号功率为典型移动终端到达无线接入单元处的信号强度。所谓非灵巧式干扰,即噪声调频与单音干扰。由表 1 可见,采用灵巧式攻击技术明显可以降低攻击设备所需功率,时分/频分体制节省功率为 7 ~ 8 dB,码分体制则节省功率幅度为 17 ~ 20 dB(与扩频增益有关)。即使是近盲的攻击方式,与非灵巧式干扰相比可节约 3 ~ 4 dB。

对于终端侧,基于内核的现代通信网灵巧式攻击技术与计算机网络攻击技术同样具有相当的效果[5];基于伪网和伪帧的灵巧式攻击技术相比其它干扰手段,同样能够有效降低攻击设备的所需功率。同样以典型的移动通信系统为例,给出灵巧式攻击试验结果,如表 2 所示。表 2 中的信号功率为网络覆盖可供移动终端进行通信的典型的信号强度。由表 2 可见,采用灵巧式攻击技术明显可以降低攻击设备所需功率,时分/频分体制节省功率为 7 ~ 9 dB,码分体制则节省功率 19 ~ 20 dB(与扩频增益

有关)。即使是近盲的攻击方式,与非灵巧式干扰相比,时分/频分体制节省功率为 3 ~ 4 dB,码分体制则节省功率为 4 ~ 5 dB。

表 2 终端侧攻击试验结果

Table 2 The test result of interference to terminals

系统体制	信号功率/dBm	干扰方式	攻击样式	所需功率/dBm	备注
时分/频分	-65	非灵巧式干扰	噪声 FM	-56	
			单音	-55	
		灵巧式干扰	基于伪网	-63	
			基于伪帧	-64	
			盲灵巧式	-59	
码分体制	-65	非灵巧式干扰	噪声 FM	-43	扩频增益为 20 dB
			单音	-42	
		灵巧式干扰	基于伪网	-63	
			基于伪帧	-62	
			盲灵巧式	-47	

5 结束语

现代分布式无中心节点数字通信网将在未来军用和民用通信领域占据越来越重要的位置,展开对该类网络有效对抗技术的研究具有前瞻性意义。有效攻击技术可借助截获的信息依托从通信网的核心网络(CN)、无线接入单元(RAU)和移动终端(MS)等各个层面展开,可根据实际需求点面结合,综合各种措施和手段以达到最佳攻击效果。本文所提的攻击技术经过大量的研究和实验,针对数字通信网的对抗具有普遍有效性,在区域电磁屏蔽领域具有广阔的应用前景。

参考文献:

[1] 王铭三,钟子发, 杨俊安. 通信对抗原理[M]. 北京:解放军出版社,1999.
WANG Ming-san, ZHONG Zi-fa, YANG Jun-an. Communication Countermeasures Principles[M]. Beijing: PLA Press, 1999.(in Chinese)

[2] 邵国培. 电子对抗作战效能分析[M].北京:解放军出版社,1998.
SHAO Guo-pei. Efficiency Analysis of Electronic Warfare Countermeasures[M]. Beijing: PLA Press, 1998.(in Chinese)

[3] Richard A Poisel. 现代通信干扰原理与技术[M].北京:电子工业出版社,2005.
Richard A Poisel. Modern Communications Jamming Principles and Techniques [M]. Beijing: Publishing House of Electronic Industry, 2005.(in Chinese)

[4] 兰俊杰,景勍,高云波,等.通信干扰技术及其发展趋势[J].舰船电子对抗,2007,1(2):50 - 53.
LAN Jun-Jie, JING Jie, GAO Yun-bo, et al. Communication Jamming Technologies and Their Development Trend[J]. Shipboard Electronic Countermeasure, 2007, 1(2): 50 - 53.(in Chinese)

[5] 宋石磊,于振海,赵国庆.直扩通信干扰技术分析与比较[J]. 中国电子科学研究院学报,2006,1(5):415 - 417.
SONG Shi-lei, YU Zhen-hai, ZHAO Guo-qing. The analysis and comparison of interference methods of direct sequence spread spectrum system[J]. Journal of China Academy of Electronic and Information Technology, 2006, 1(5): 415 - 417.(in Chinese)

作者简介:

王红军(1968 -),男,江苏镇江人,副教授,主要研究方向为通信对抗、认知无线电、移动通信。

WANG Hong-jun (male) was born in Zhenjiang, Jiangsu Province, in 1968. He is now an associate professor. His research interests include communication countermeasure, cognitive radio and mobile communication.

Email: hongjun-wang@163.com