DOI:10.3969/j.issn.1001 -4551.2017.03.018

基于 OPNET 的数字化变电站 DoS 攻击建模与仿真研究*

朱 玛[1],李 勇[1],章坚民[2*],侯连全[2],金乃正[1],陈 益[2]
(1.国网绍兴供电公司,浙江 绍兴 312000;2.杭州电子科技大学 自动化学院,浙江 杭州 310018)

摘要:针对智能变电站通信网络面临后果中最为严重的拒绝服务攻击(DoS)类型,首先对数字化变电站的周期性、随机性、突发性等不同特性的数据流进行了建模,随后给出了基于 SYN-flood 攻击原理的数字化变电站 DoS 攻击建模,并详细介绍了基于 OPNET 的仿真模块设计及实现方案;搭建了变电站星型网络站控层服务器遭受 SYN-flood 的攻击仿真场景,并针对变电站常见的 10BaseT、100BaseT 两种链路宽带场景进行了仿真。仿真结果展示了 DoS 攻击前后的站控层服务器主要性能特性以及后果,即导致服务器 CPU 持续处于高利用率状态;TCP 连接延时增加;链路吞吐量增加以消耗链路带宽等,从而揭示 DoS 攻击企图达到服务器无法响应正常的业务请求即拒绝服务的目的。

关键词:数字化变电站;通信信息网络;拒绝服务 DoS;攻击仿真;OPNET
中图分类号:TM63 **文献标志码**:A **文章编号**:1001 -4551(2017)03 -0304 -06

OPNET based modeling and simulation of DoS attack of digital substation

ZHU Ma[1], LI Yong[1], ZHANG Jian-min[2], HOU Lian-quan[2], JIN Nai-zheng[1], CHEN Yi[2]
(1. State Grid Shaoxing Electric Power Supply Company, Shaoxing 312000, China;
2. College of Automation, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: Aimming at the problem that DoS (Denial of Service) as the most serious cyber attack for digital substation, a modeling of data flow with different properties as periodic, random, sudden response was firstly introduced, followed by a simulation modeling of DoS attack based on the SYN-Flood principle; the module design and simulation implementation scheme based on OPNET platform was proposed in detail. The simulation scenario was selected as the star network where the control bay server was under the SYN_flood attack, and the case studies were made for wide-band of 10BaseT and 100BaseT data link. The simulation results gives the performances of the bay server before and after SYN_flood attack, and the attack consequences are long stay at a high CPU utilization, time delay increasing of TCP connection, and the increasing of link throughput to exhaust the link band, etc., in which the attempts of DoS are exposed to make the bay server disable to response the normal business request, i.e., to deny the service.

Key words: digital substation; communication and information network; denial of service (DoS); attack simulation; OPNET

0 引 言

智能变电站中引入开放的 IEC61850 通信协议使得设备间的信息交互更加紧密[1-2],信息传输量巨大。同时,智能变电站的安全运行更加依赖于现代信息技术,其信息安全也存在很大隐患[3-4]:①信息

收稿日期:2016 -09 -08
基金项目:国家自然科学基金资助项目(51677047);国网浙江省电力公司科技项目(ZBGW15-011-007-83)
作者简介:朱玛(1980 -),女,浙江绍兴人,硕士,高级工程师,主要从事继电保护管理运行方面的研究. E-mail:zhuma1201@sina.com
通信联系人:章坚民,男,教授. Email: zhangjmhzcn@hdu.edu.cn

采集环节的安全性。由于采集报文的实时性要求比较高,智能电子装置一般不会加入复杂的加密技术就把报文发出,一旦这些设备受到攻击,则攻击者可以向电网提供虚假信息,影响监控中心决策者做出错误的判断,从而造成巨大的电网事故。②信息传输环节的安全性。智能变电站采用高速、双向、实时、集成的以太网通信技术,从而保证了信息流高速传输到数据处理中心,但是这也为恶意攻击者提供了更多的入口,加大了信息流被截获、监听、篡改的风险。③智能控制的安全性。智能变电站智能控制系统通过收集到的各类信息流对智能变电站进行分析、诊断、和预测,并及时采取适当的措施对智能变电站运行状况进行调节,使之运行在安全、可靠和稳定的状态。然而网络间谍,变电站内部人员误操作,厂家维护人员的恶意违规操作都使得智能变电站的智能控制的安全性受到威胁。以上问题已经引起了人们广泛的研究。

SYN-Flood 是利用 TCP 协议漏洞展开的一种 DoS 攻击方式[5]。攻击者通过利用 TCP 使用 3 次握手机制对 TCP SYN 报文源地址不加验证的安全缺陷,在报文中加入虚假的不可达源地址,使得受害者服务器将不会收到最后的 ACK 包来完成 3 路握手。同时服务器因维护大量的半连接,消耗大量内存和网络资源以至于不能响应正常的用户请求,甚至引起服务器瘫痪。据调查,利用 TCP 展开的 DOS 攻击占所有 DOS 攻击的 90%[6]。由于智能变电站中大部分的报文是通过 TCP/IP 协议进行传输的,如果智能变电站受到 DOS 攻击,智能变电站网络中将存有大量的冗余数据[7],这将可能造成网络或监控系统瘫痪。同时,DOS 攻击者甚至仅仅假装数据交换就能使监控中心操作者做出错误的判断而隔离保护装置造成电力系统瘫痪[8]。

OPNET 是业界公认的通信网络、协议、设施的优秀建模与仿真工具[9],并已在变电站通信网络性能仿真上得到了一定的应用[10-12]。本研究尝试基于 OPNET,对于变电站通信网络信息安全进行仿真。

本研究首先对数字化变电站的周期性、随机性数据流、突发性数据流进行建模分析,给出数字化变电站 DoS 攻击的仿真建模,以及 OPNET 的模块设计并对此进行仿真;通过对仿真结果的分析,提出相应的 DoS 攻击监测,并部署相应的通信网络安全防范措施。

1　变电站通信与信息建模

1.1　变电站物理模型

本研究采用 T1-1 型变电站物理模型为研究目标。Tl-1 型变电站具有 1 条母线,1 条进线,2 条出线和一台变压器;不采取冗余继电保护,馈线保护一般直接跳闸,采用母线差动保护。因此,在组建变电站通信网络时可分为 3 个间隔,即变压器组成一个间隔命名为间隔 1,2 条出线各组成一个间隔命名为间隔 2 和间隔 3。其中,每个变压器间隔包括 1 个 MU IED,2 个断路器 IED 和 2 个保护控制 IED,每个出线间隔包括 1MU IED,1 个断路器,2 个保护 IED。各间隔内部 IED 设备通过交换机互联,各间隔交换机连接中央交换机,组成以太网与站控中心通信。Tl-1 型变电站网络结构如图 1 所示。

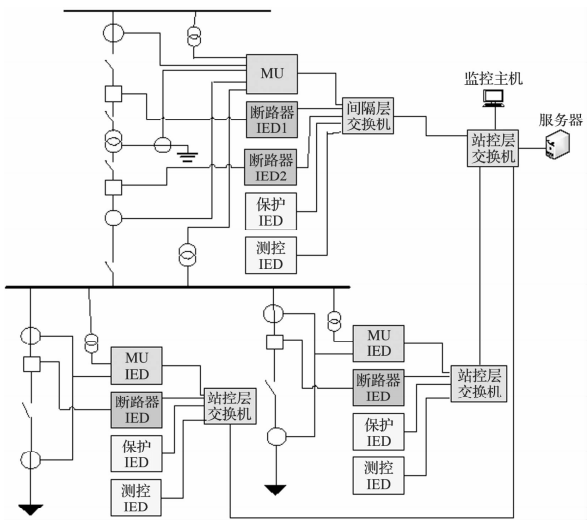


图 1　Tl-1 型变电站网络结构

1.2　数据流的建模

根据 IEC61850-5 标准,本研究在变电站中将所有的报文分为 7 类:快速报文,中速报文,低速报文,原始数据报文,文件传输,时间同步报文,访问控制命令报文。然而这样的分类显然太过冗余,比如过程层的合并单元的 SAV 报文既属于原始报文又属于快速报文。因此,从数据流的特性在时域中来分析,本研究把变电站数据流分为 3 类:周期性数据,随机性数据,突发性数据。对于本研究的 Tl—1 型变电站数据流如图 2 所示。

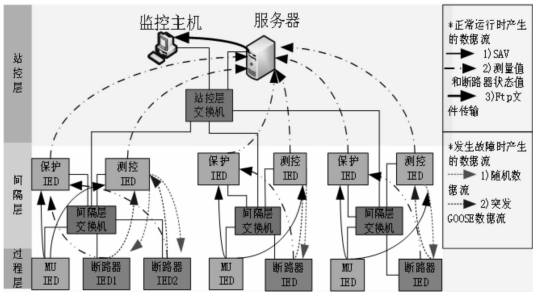


图 2 Tl—1 型变电站数据流

1.3 周期性数据流的建模

周期性报文主要来自两类周期数据,一类是过程层 PT、CT 传感器合并单元(MU)采集的 SAV 报文,然后发送到间隔层的保护 IED 和控制 IED。根据 IEC61850-5 规定,SAV 报文的传输时间必须在 Ds = 4 ms以内。否则系统的性能就会受到影响,造成灾难性的后果。例如,在变电站出现短路错误,而保护 IED 因 SAV 报文不能及时传输而不能立即动作,这将可能造成电气设备过期的服务和电力负荷的损耗。因此 SAV 报文端到端的延时应该满足一下定义:

$$D_C \leqslant D_S \tag{1}$$

式中:D_C—报文端到端的延时。

而另一类周期性报文是上传到服务器的间隔层测量值和断路器的状态值。这类报文属于周期性的 GOOSE 报文,这类数据周期性比较稳定,属于一种中速报文。其端到端的网络延时被规定在 100 ms 以内,对应上式的 $D_S = 100$ ms。

1.4 随机数据流的建模

随机数据流属于典型的事件驱动数据,主要包括:开关操作命令、保护功能闭锁、时间同步、变压器分接头调整、电容器投切等。随机性数据是由变电站事件触发的报文。数据接收有如下特征:在任何一个时间段内,数据的出现是随机的,假设报文分组出现的概率为 P,其与时间没有任何关系,且前后报文的到达情况也不相关;假设报文的平均到达率为 λ,则在时间 t 的间隔里,有 k 个报文到达的概率服从参数为 λ 的泊松 Poisson 分布[13],即对任意的 $s,t \geqslant 0$ 有:

$$p\{N(T+S) - N(S) = K\} = \frac{(\lambda t)^k e^{-\lambda t}}{k!} \tag{2}$$

1.5 突发性数据流的建模

突发性数据流主要包括间隔层上传的保护控制信息和断路器的状态改变信息,而断路器的状态信息也属于 GOOSE 报文。当故障发生时,保护控制装置动作,然后 GOOSE 报文由周期传输模式转为突发模式,从而引发突发性数据报文。这类数据报文要求传输的时间集中,具有突发性特点,可以最简单的 ON/OFF 模型模拟:当数据以一定的速率产生时,处于 ON 状态;没有任何数据产生时,处于 OFF 状态;数据 ON 期间服从的分布函数与 OFF 期间的分布函数可以相同,也可以不同,且两部分叠加之后的数据相关性由分布函数决定。

单个数据源 ON 状态的持续时间设为 $\tau(i)$,服从重尾分布函数:

$$p(\tau > t): t^{-\alpha} t \to \infty, 1 < \alpha < 2 \tag{3}$$

而 OFF 状态服从的分布函数是持续时间为 $\theta(i)$ 采用传统泊松过程当中的负指数分布:

$$p(\tau > t): e^{-\lambda t}, t \to \infty \tag{4}$$

只要 ON 或 OFF 期间的时间长度所服从的分布函数当中之一为重尾分布,那么将这种类型的无数多个 ON/OFF 数据进行相加,就会形成具有自相似这种特性的突发性数据流,且满足下式:

$$\begin{cases} \beta = \alpha - 1 \\ H = 1 - \dfrac{\beta}{2} = \dfrac{3-\alpha}{2} \end{cases} \tag{5}$$

式中:H— 自相似程度参数 Hurst;β— 自相关函数的系数 $\beta = \dfrac{r(k) = E[(x_i - u)(x_t + k - u)]}{\sigma^2} \sim k^{-\beta}$,并且 β 的约束条件是 $0 < \beta < 1$。

2 基于 OPNET 变电站通信网络 DoS 攻击建模

2.1 IP-ENCAP 进程模型

本研究利用 OPNET 仿真软件对 SYN-flood 攻击进程建模;为达到攻击的效果,需要建立合适的 IP_ENCAP 进程模型。本节将对 IP_ENCAP 进程的建模进行详细的介绍,IP-ENCAP 进程模型如图 3 所示。

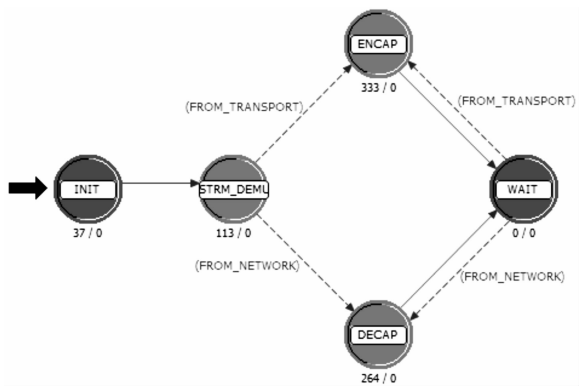


图 3 IP-ENCAP 进程模型

IP_ENCAP 进程模型主要完成两项功能:一是将传输层发来的报文进行封装,在包头加入源地址和目的地址后发送到网络层。二是解封装来自网络层的数据包,根据数据包中的上层协议类型,将其转发到上层的传输层。

IP_ENCAP 进程共有 5 个有限状态机,具体描述如下:

(1)INIT 状态。init 为绿色强制状态,完成初始化功能;

(2)STRM_DEMUX 状态。初始化操作完成后,立即跳入 STRM_DEMUX 状态,等待触发条件而跳转到不同的状态;

(3)DECAP 状态。负责接收来自网络层的数据包,解析数据包的源 IP 地址和目的 IP 地址,然后根据不同的传输层协议将数据包通过相应的数据流发送;

(4)ENCAP 状态。负责接收来自传输层的数据把文,在报文的头部加入本机 IP 和要发送的目的 IP,创建格式为 ip_dgram_v4 的数据包,完成封装后转发到网络层;

(5)WAIT 状态。当触发条件为"收到传输层发来的数据包"(FROM—TRANSPORT)时,进程转入"ENCAP"状态,当满足触发条件"收到网络层发来的数据包"(FROM_NETWORIO 时,进程转入"DECAP"状态。

2.2　SYN-Flood 攻击模块的设计

根据 SYN-Flood 攻击的原理,在设计攻击模块时,只需在 IP_ENAP 模块中完成对源 IP 地址的伪装,将源地址设置为不可达的 IP 地址即可。具体实现就是修改 ENCAP 状态机中封装的配置文件。双击图 3 中 ENCAP 模块,进入进程域代码,重新配置源地址 IP。因此只需在如下代码:

ip_dgram_fd_ptr - > src_addr = inet_address_copy (org_addr)之上添加一行代码,代码如下:

org_addr. address. ipv4 _addr = prg _ip _address _string_to_value("a. b. c. d")。

ENCAP 状态机入口代码如图 4 高亮部分所示。

```
if (-i != vrf_index)
    op_pk_fd_set_int32 (ip_pkptr, IPC_DGRAM_FD_INDEX_VRF_INDEX, vrf_index, 0 /* pseudo */);

/*  Create fields data structure that contains orig_len,    */
/*  ident, frag_len, ttl, src_addr, dest_addr, frag,        */
/*  connection class, src and dest internal addresses.      */
ip_dgram_fd_ptr = ip_dgram_fdstruct_create ();

/*  Assign values to members of the field structure.    */
org_addr.address.ipv4_addr=prg_ip_address_string_to_value("a.b.c.d");
ip_dgram_fd_ptr->src_addr           = inet_address_copy (org_addr);
ip_dgram_fd_ptr->dest_addr          = inet_address_copy (dest_addr);
ip_dgram_fd_ptr->connection_class   = conn_class;
ip_dgram_fd_ptr->orig_len           = data_len;
ip_dgram_fd_ptr->frag_len           = data_len;
ip_dgram_fd_ptr->ttl                = ttl;
ip_dgram_fd_ptr->protocol           = protocol_type;
ip_dgram_fd_ptr->tos                = type_of_service;
ip_dgram_fd_ptr->compression_method = IpC_No_Compression;
```

图 4　ENCAP 状态机入口代码

其中,"a. b. c. d" 是一个不可到达的 IP 地址。保存修改关闭 ENCAP 程序窗口。至此攻击模块已设计完成。

2.3　通信网络攻击模型的建模

本研究对站控层服务器进行攻击场景,通信网络模型如图 5 所示。

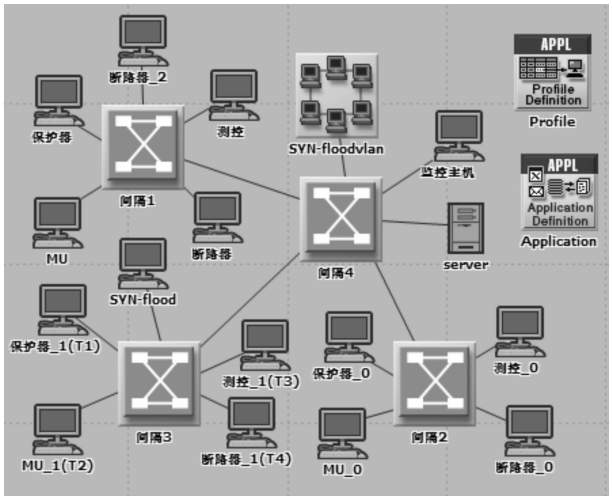


图 5　通信网络模型

场景分成 3 个子网,各个子网的设备通过各自的间隔交换机相连,然后通过核心交换机与站控层服务器及监控主机通信。在对服务器攻击的场景中,在核心交换机上加入局域网攻击节点 sysfloodvlan。

OPNET 用应用配置器设定应用的具体动作行为,用业务配置器描述用户所涉及的应用类别及应用的使用方式。本研究通过配置不同的 Video Conferencing 应用来模拟各个 IED 收发数据的行为,通过配置 ftp 应用来模拟间隔层上传到站控层的突发性数据。通过配置 http,email 应用模拟攻击节点的行为。仿真模型中的每一类应用都对应一类不同的数据类型。

主要配置参数为:

(1)周期性数据

Incoming Stream Interarrival Time (seconds): constant (0.025);

Outgoing Stream Interarrival Time (seconds): constant (0.025);

Incoming Stream Frame Size (bytes):constant (200);

Outgoing Stream Frame Size (bytes):constant (200);

Type of Service: Interactive Voice (6)

(2)随机性数据

Incoming Stream Interarrival Time (seconds): Poisson (0.02);

Outgoing Stream Interarrival Time (seconds): Poisson(0.02);

Incoming Stream Frame Size (bytes): constant (64);

Outgoing Stream Frame Size (bytes): constant (64);

Type of Service: Interactive Voice (6).

(3)突发性 FTP 文件传输数据

CommandMix(Get/Total):50%

Inter-request Time(seconds):Pareto(0.000512,1.1)

File Size(bytes):constant(1024)

Type of Sevice:Reserved(7)

(4)http 报文

Page Interarrival Time(seconds) :exponential (300)

Type of Service:Standard(2)

(5)email 报文

Send Group Size :constant(300)

Receive Interarrival Time(seconds):constant (300)

E-Mail Size(bytes) :constant(1000)

Type of Service:Standard(2)

3 变电站通信网络攻击仿真方案

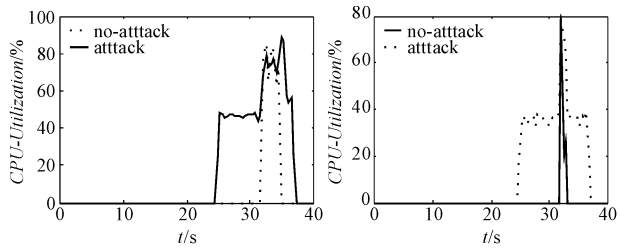
3.1 仿真场景和指标的选取

设置仿真模型链路宽带分别为 10BaseT、100BaseT 两种场景。为了便于观察仿真结果,本研究对于不同业务设置不同的起始时间:周期性报文从仿真 0 s 开始加载,直到仿真结束;随机性数据从 20 s 开始加载,持续10 s;突发性报文从 16 s 到 16.1 s 随机开始,持续 10 s;FTP 文件传输业务 32 s 开始加载持续 1 s;攻击节点 25 s 开始发动攻击,持续 12 s,仿真总时间设置 40 s。

SYN-flood 攻击的对象主要是网络中服务器。攻击使服务器的各项性能下降以至于不能提供优质的服务。在仿真当中选取 CPU 占用率、链路负载、TCP 连接时延作为评估 SYN-flood 攻击效果的指标。其中 CPU 占用率越大,链路负载越大,TCP 延时越长就可认为对服务器的攻击效果越好。

3.2 仿真结果及分析

站控层服务器遭受 SYN-flood 攻击时,服务器 CPU 占用率的影响如图 6 所示。

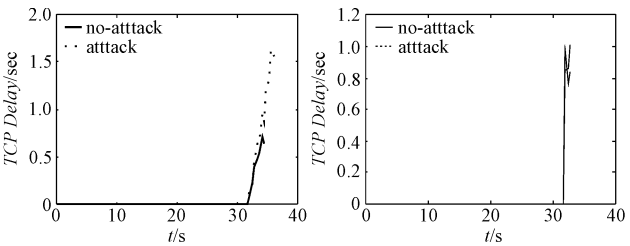


(a) 带宽10 BaseT (b) 带宽100 BaseT

图 6 站控服务器 CPU 占用率

从图中可以看到,在 25 s 时遭到攻击节点的攻击,随之服务器 CPU 占用率开始增加,最大利用率在 32 s,此时站控层服务器向站控层主机进行大文件传输,在带宽 10BaseT 时,CPU 最大利用率 88%;带宽 100BaseT 时,CPU 最大利用率为 80%。虽然无攻击状态下,在 32 s 时服务器 CPU 也突然增加,但是持续 1 s 后会迅速回落,而处于攻击状态的服务器就会持续处于高利用率状态,并且占用大量的半连接时间,内存资源不断消耗。

站控层服务器受到攻击时,与网络中没有受到攻击节点时相比,在 32 s 时监控主机开始与服务器建立 TCP 连接,然后进行大文件传输,由于在仿真开始 25 s 时,服务器受到 SYN-flood 攻击,造成 TCP 连接延时增加;带宽 10BaseT 时监控主机最大延时为 1.62 s,而没有受到攻击时最大延时为 0.71 s;带宽 100BaseT 的监控主机最大延时 0.001 s;而没有受到攻击时最大延时为 0.000 97 s。显然带宽越大延时越小,但是随着攻击的不断进行,突发性 FTP 报文的传输逐渐将受到很大的影响。监控主机 Ftp 业务的 TCP 连接延时变化如图 7 所示。



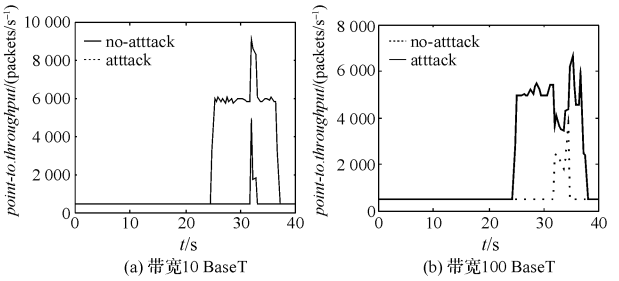
(a) 带宽10BaseT (b) 带宽100 BaseT

图 7 监控主机 TCP 连接延时

站控层服务器受到攻击时,对站控层交换机与服务器之间的链路宽带的影响。从 0 s 开始,间隔层各 IED 状态报文通过站控层交换机与服务器之间的链路到达站控层服务器,25 s 时,站控层服务器遭受 SYN-flood 攻击,此时,不管带宽 10BaseT 链路,还是 100BaseT 链路,都能明显观察出链路吞吐量瞬间增

加,特别 32 s 时,服务器向站控层主机发送 FTP 业务,链路吞吐量达到峰值。从攻击者的目标角度来看,就是消耗链路带宽,阻塞间隔层上传的数据流请求,增加站控层监控主机 FTP 请求在链路中的排队时间,直到服务器无法响应正常的业务请求,从而达到拒绝服务的目的。

站控层交换机到服务器链路吞吐量如图 8 所示。



(a) 带宽10 BaseT　　(b) 带宽100 BaseT

图 8　站控层交换机到服务器链路吞吐量(bits/sec)

4　结束语

本研究在 OPNET 平台下对站控层服务器进行攻击模型建模和仿真,并对攻击结果进行了分析,得到了预期的仿真结果。由于目前网络攻击行为仿真还处于初期阶段,仍有许多问题尚待解决。如:缺乏丰富的攻击仿真模型库,不能对节点中操作系统和应用程序的精确建模,没有通用的指标来衡量攻击效果等。因此对数字化变电站的网络安全而言,仍需要投入大量的研究力量,不断提升仿真水平,才能掌握各类攻击特性以及防护技术采取后的特性,提高防范技术的适应能力并减少其对变电站实时性能的影响。

参考文献(References):

[1] WANG W, LU Z. Cyber security in the Smart Grid: Survey and challenges[J]. **Computer Networks**, 2013, 57(5): 1344-1371.

[2] YOO H, SHON T. Challenges and research directions for heterogeneous cyber-physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture[J]. **Future Generation Computer Systems**, 2016(61): 128-136.

[3] 汤　奕,陈　倩,李梦雅,等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化,2016,40(17):59-69.

[4] 侯连全,章坚民,金乃正,等. 变电站过程层与 SMV 安全传输的网络攻击检测与取证设计[J]. 电力系统自动化,2016,40(17):87-92.

[5] NISSANKE N SUN J. A model for analysis of SYN flood DoS attacks[C]. 13th International Telecommunications Network Strategy and Planning Symposium, New York: IEEE, 2008.

[6] MOORE, D. VOELKER, G. SAVAGE. S. Inferring internet denial of service activity[J]. **Acm Transactions on Compater Systems**, 2006, 24(2): 115-139.

[7] 杨　漾,黄小庆,曹一家,等. 变电站通信报文安全认证及其实时性仿真[J]. 电力系统自动化,2011,35(13):77-82.

[8] KOUTSANDRIA G, MUTHUKUMAR V, PARVANIA M, et al. A hybrid network IDS for protective digital relays in the power transmission grid[C]. 2014 IEEE International Conference on Smart Grid Communications, New York: IEEE, 2014.

[9] 龙　华. OPNETModeler 与计算机网络仿真[M]. 西安:西安电子科技大学出版社,2006.

[10] 董　楠,朱　林,段献忠. 基于 OPNET 的变电站过程层网络的仿真研究[J]. 继电器,2006,34(21):40-45

[11] 谢　栋,李　勇,章坚民,等. 基于 OPNET 的数字化变电站通信网络仿真建模及应用[J]. 机电工程,2016,33(3):313-318.

[12] 方晓洁,季夏轶,卢志刚. 基于 OPNET 的数字化变电站继电保护通信网络仿真研究[J]. 电力系统保护与控制,2010(23):137-140.

[13] ZHANG Z, HUANG X, KEUNE B, et al. Modeling and simulation of data flow for VLAN-based communication in substations[J]. **IEEE Systems Journal**, 2015(99): 1-12.

[**编辑**:周昱晨]

本文引用格式:

朱　玛,李　勇,章坚民,等. 基于 OPNET 的数字化变电站 DoS 攻击建模与仿真研究[J]. 机电工程,2017,34(3):304 - 309.

ZHU Ma, LI Yong, ZHANG Jian-min, et al. OPNET based modeling and simulation of DoS attack of digital substation[J]. Journal of Mechanical & Electrical Engineering, 2017,34(3):304 - 309.

《机电工程》杂志:http://www.meem.com.cn