



一种基于 BF-DT-CUSUM 算法的电网 工控系统 DDoS 攻击检测方法

费稼轩,张涛,马媛媛,周诚

(国网智能电网研究院,江苏 南京 210003)

摘 要:信息通信技术的高速发展使得国家电网已经迈进了智能化、信息化、自动化发展时代,然而同时智能电网中信息通信技术的广泛应用也为攻击者提供了更多的途径入侵和攻击电网工控系统。提出一种基于 BloomFilter 地址统计的动态阈值更新的改进型 CUSUM(BF-DT-CUSUM)DDoS(distributed denial of service)入侵攻击检测方法,针对电网工控系统存在的 DDoS 攻击采用基于 BloomFilter 正常流量统计的动态阈值技术,同时改进了传统的 EWMA 算法使其可用于计算识别 DDoS 攻击用阈值,并对 CUSUM(cumulative sum)算法作出一定变动,以此来更高效地检测电网工控系统 DDoS 攻击事件。仿真实验验证了该方法对电网工控系统中 DDoS 攻击具有较高的检测速度和精度,且系统开销小。

关键词:电网工控系统;攻击检测;DDoS;EWMA;CUSUM

中图分类号:TP311;TP39

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2015402

Efficient detection technology of DDoS attacks based on BF-DT-CUSUM algorithm in smart grid industrial control system

FEI Jiaxuan, ZHANG Tao, MA Yuanyuan, ZHOU Cheng

State Grid Smart Grid Research Institute, Nanjing 210003, China

Abstract: Rapid development of information and communication technology has led China National Grid Corp into the era of intelligent, informational and automated, simultaneously with wide application of information and communication technology in smart grid also providing more ways for attackers to invade and attack power system. A DDoS attacks detection method based on modified CUSUM with dynamic threshold was proposed according to BloomFilter address statistics in smart grid. The proposed method used dynamic threshold technology based on BloomFilter normal traffic statistics, and optimized traditional EWMA algorithm to identify threshold of DDoS attacks, finally modified CUSUM algorithm in order to efficiently detect DDoS attacks in smart grid. Simulation experiments demonstrate that proposed method has high detection speed and precision for DDoS attacks in smart grid, and the system overhead is small.

Key words: smart grid industrial control system, attack detection, DDoS, EWMA, CUSUM

收稿日期:2015-10-17; 修回日期:2015-12-09

基金项目: 国家电网公司 2015 年科技项目(电网智能化单元传输规约安全分析及增强技术研究)

Foundation Item: The 2015 Science and Technology Project of State Grid Corporation of China: Security Analysis and Enhance Technical Research of Power Grid's Intelligent Transmission Protocols

1 引言

智能电网^[1]通过采用双向流动的电力与通信网络,将传感、嵌入式处理、数字通信等信息网络技术应用到电力系统,支持电流和信息在网内所有用户和节点间双向流动,使得智能电网工控系统的各个部分连接在一起,并进行自动可靠的电力传输与控制,显著提升了电力系统的可观性、可控性、顽健性与自愈性^[2]。智能电网工控系统安全是智能电网建设中必须要解决的关键问题,目前电网安全主要在于电网基础设施安全和网络安全。网络安全是智能电网工控系统要解决的重中之重,由于网络的异构性、复杂性以及大规模化使得安全问题变得更加具有挑战性^[3,4]。先进基础设备,量测设备的引进可以使得电网更加稳定但同时也会引入更多的网络安全风险。

通信网络安全在智能电网工控系统建设中显得更加突出,在信息时代网络通信安全本来就非常严重,在信息通信网中存在的安全风险与隐私问题也同样存在于智能电网工控系统通信网络中。例如伊朗 Bushire(布什尔)核电站的控制系统曾在 2010 年 9 月遭到非法攻击者发起 Stuxnet(震网)蠕虫病毒攻击^[5],引发严重后果及不良影响,大大延迟了伊朗的核进程。这些安全威胁引发了人们对智能电网工控系统安全的恐慌和思考,如何检测各种针对智能电网工控系统的攻击行为,已经成为智能电网工控系统安全、稳定运行急需解决的问题^[6,7]。

信息网络中的各种漏洞和脆弱性使得攻击者可以有更多的途径入侵电力网络系统,如拒绝服务攻击、数据窃听、信息泄露、非法注入控制命令等,给攻击者提供了渗透电力信息网络甚至危害物理系统的更多途径和可能。分布式拒绝服务(distributed denial of service, DDoS)攻击^[8]是一种基于拒绝服务(denial of service, DoS)的特殊式拒绝服务攻击,是一种分布、协作的大规模攻击方式。DoS 攻击只要一台计算机就能实现,而 DDoS 攻击是利用一批受控制的计算机发起攻击。DDoS 攻击的攻击者不需要直接对目标进行攻击,只需要控制大量的僵尸主机,就可以很容易地从不同站点并发地发起攻击,攻击来势迅猛,令人难以防备,因此,DDoS 攻击对于智能电网工控系统具有很大的破坏性。

本文希望通过研究智能电网工控系统安全体系结构,分析信息网络中的各种漏洞和脆弱性引发的侵入攻击,着重针对存在于智能电网工控系统中的 DDoS 攻击,提出一种智能电网工控系统中的 DDoS 侵入攻击检测方法,提高

对侵入攻击的检测准确性和精度。

2 相关工作

针对智能电网工控系统面临的安全威胁,许多研究者和机构提出不同的网络安全方法来进行安全监测与监控。入侵检测系统(intrusion detection system, IDS)和流量分析技术^[9]是目前应用最广泛的信息网络攻击检测方法之一,通过监视和分析网络流量以检测出带有异常行为的数据分组和用户。Cisco 公司在《智能电网安全白皮书》^[10]中提出了通过对智能电网中网络流量和设备状态进行实时监测和融合分析,保证数据传输和处理、设备调度和控制、业务运行的安全性。Liang 等人^[11]提出了电力二次系统安全防护的 DDoS 攻击原理及防御技术,结合 DDoS 攻击的特点,分析了安全防护系统中可能受到 DDoS 攻击的风险,最后对电力二次系统安全防护体系中的 DDoS 攻击防御技术进行了探讨,但该方法在遭受入侵攻击过程中,不能实时过滤攻击流量。

为了检测威胁数据入侵, Sun 等人^[12]提出将信息网络的报警事件和电力系统的错误数据关联,以检测入侵和攻击行为, Huang 等人^[12]提出了一种基于 CUSUM(cumulative sum)的最小检测时延的防御方法, Liu 和 Wang 等人^[13,14]将分布式状态估计应用到了威胁数据检测方面以提高检测精度并降低计算量。然而,攻击者可以利用系统对误差的容错裕量,设计特殊的攻击从而逃避系统的检测。Liu 和 Kosut 等人^[15,16]通过分析电力系统的状态估计,发现如果按照一定策略同时修改多个节点的数据,可以使得电网 SCADA(supervisory control and data acquisition)系统的状态估计结果保持平衡,躲避故障检测。然而随着攻击手段的不断增多,电网攻击可能产生的影响也越来越大,这些安全方法难以对威胁的严重性进行准确估计,并且由于缺少对控制命令物理意义的理解,无法检测格式正确但数据被篡改的通信。此外,高误报率也是部分信息安全检测技术的一个大问题,这也导致很难确定和定位攻击事件。

根据上面的分析,本文提出了一种基于 BloomFilter 地址统计的动态阈值更新的改进型 CUSUM(BF-DT-CUSUM) DDoS 异常流量识别算法,以检测智能电网工控系统的入侵攻击事件。在数据采集阶段中,利用基于 BloomFilter 的路由转发地址映射统计方案收集电网流量数据和更新存储的历史数据,在数据聚集判定阶段,利用改进 EWMA(exponent weighted moving average)动态阈值更新算法计算阈值并判定目标地址是否遭到攻击,利用改进型



CUSUM 算法检测 DDoS 攻击入侵。该方法能够提高攻击检测的准确性及在线检测速度,降低运算开销。

3 基于 BloomFilter 地址统计的动态阈值更新的改进型 CUSUM(BF-DT-CUSUM)DDoS 入侵攻击检测算法

3.1 CUSUM 算法描述

CUSUM 算法在异常监控领域得到广泛的使用,其作用是检测一个统计过程均值的变化,主要基于随机序列的概率分布会伴随变化发生这一统计学事实。该算法的核心数学形式化描述如下:

令 $x_1, x_2, \dots, x_t$ 为独立的 $N(0,1)$ 分布, $x_{t+1}, x_{t+2}, \dots$ 为独立的 $N(\delta,1)$ 分布,其中 t 为未知变点,对于给定的 $x_1, x_2, \dots, x_n$, 设 $t=v(v < n)$ 对于原假设 $t=\infty$ 的似然比统计量为:

$$L_{n,v} = \frac{\prod_{i=1}^v \Phi(x_i) \prod_{i=v+1}^n \Phi(x_i - \delta)}{\prod_{i=1}^n \Phi(x_i)} = \frac{\prod_{i=v+1}^n \Phi(x_i - \delta)}{\prod_{i=v+1}^n \Phi(x_i)} = \exp \left\{ \delta \sum_{i=v+1}^n \left(x_i - \frac{\delta}{2} \right) \right\} \quad (1)$$

其中, Φ 代表标准正态分布的分布密度函数。

考虑到 $\prod_{i=n+1}^n \Phi(x_i) = 1$ 及 $\sum_{i=n+1}^n x_i = 0$, 设其对数化为

$$A_{n,v} = \ln L_{n,v} = \delta \sum_{i=v+1}^n \left(x_i - \frac{\delta}{2} \right)$$

假设变量 $x_1, x_2, \dots, x_t$ 与 $x_{t+1}, x_{t+2}, \dots$ 有偏移,那么其对数似然统计量满足:

$$A_n = \max_{1 \leq v < n} A_{n,v} = \max \left\{ \delta \sum_{i=v+1}^n \left(x_i - \frac{\delta}{2} \right) \right\} \quad (2)$$

假设检测时发生向上偏移 ($\delta > 0$), 则 A_n 等价于:

$$Z_n = \max_{1 \leq v < n} \left\{ \sum_{i=v+1}^n \left(x_i - \frac{\delta}{2} \right) \right\} \quad (3)$$

定义 1 设 $n-1$ 个观测值未发生均值偏移并给定门限阈值 h (即 $Z_i \leq h, i=1, 2, \dots, n-1$), 如果在时段 n 满足 $x_n - \frac{\delta}{2} > h$, 或 $x_n + x_{n-1} - \delta > h$, 或 $x_n + x_{n-1} + x_{n-2} - \frac{3\delta}{2} > h, \dots$ 或 $x_n + x_{n-1} + \dots + x_1 - \frac{n\delta}{2} > h$ 这共计 n 种情况的任意一种, 则认定这个过

程发生了均值偏移。

记 $\tilde{x}_i = x_i - \frac{\delta}{2}$, 且 $\tilde{x}_0 = 0, \tilde{S}_0 = 0, \tilde{S}_k = \sum_{i=0}^k \tilde{x}_i$, 可知:

$$\begin{aligned} Z_n - Z_{n-1} &= \tilde{x}_n - \min \{0, \tilde{S}_n - \min_{0 \leq v \leq n-1} \tilde{S}_v\} \\ &= \max \{\tilde{x}_n, \tilde{x}_n - \tilde{S}_n + \min_{0 \leq v \leq n-1} \tilde{S}_v\} \\ &= \max \{\tilde{x}_n, \min_{0 \leq v \leq n-1} \tilde{S}_v - \tilde{S}_{n-1}\} \\ &= \max \{\tilde{x}_n, -Z_{n-1}\} \end{aligned} \quad (4)$$

利用参数 k 代替 $\frac{\delta}{2}$, 就可以将 Z_n 的递推式表示为:

$$Z_n = \max \{0, \tilde{x}_n + Z_{n-1} - k\}, n=1, 2, \dots \quad (5)$$

此为 CUSUM 算法的主要数学表述,在实际检测中设定报警门限阈值 h , 在第 n 个观察点发现首次出现 $Z_n \geq h$, 则认为在过程 n 以前的统计量发生了均值偏移并进行报警。

3.2 基于 BloomFilter 的路由转发地址映射统计方案

在 IPv4 地址体系中,IP 地址被分为 4 段,每段的值可取十进制的 1 到 255。依照 BloomFilter 算法设置一个由 4 个独立散列函数组成的 4×256 表结构来跟踪时间段 t 内通过路由器到达不同目的地址的 IP 包数。当一个 IP 包进入路由器后,其目的地址被 4 个独立的散列函数(针对 IP 地址的 4 段分别映射)分别映射到各自不同的 256 个域中的某一个(对每一段的值进行映射),此时保存在被映射域(共 4 个,每个散列函数对应一个)中的变量 $a_{i,j} (1 \leq i \leq 256, 1 \leq j \leq 4)$ 加 1。其映射方法如图 1 所示。

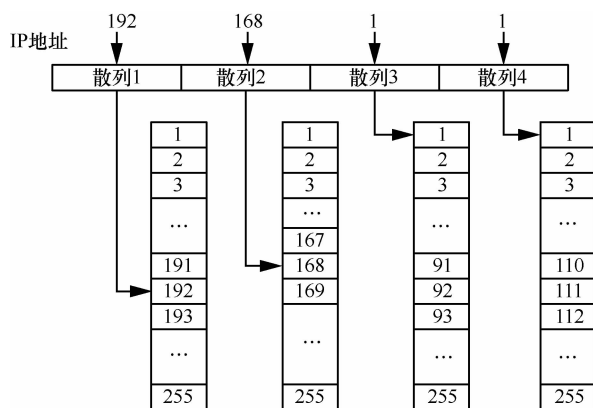


图 1 基于 BloomFilter 的地址映射统计示意

3.3 改进型 EWMA 动态阈值更新算法

传统 EWMA (exponentially weighted moving average, 指数加权移动平均) 算法是常用统计阈值生成方法之一,该算法从全期平均和移动平均方法发展而来,其特点在于对先前得到的流量值赋予不同的权值,依照权值对新的阈值加以计算,在 n 时段结束后,其基本阈值计算式如下:

$$h_n = \beta h_{n-1} + (1 - \beta)x_n \quad (6)$$

其中, h_n 表示第 $n+1$ 时段检测时所使用的预测阈值, x_n 表示 n 时段收集到的对象值, β 为数据更新系数 (一般取值 0.01~0.03), 随着 n 的增大, 先前的 x 对 h 的影响会逐步减小。该方案在统计对象长时间处于较低数值状态下所计算的阈值较小, 突发性的网络特点导致某个统计值的突发性变大会导致由于低阈值而产生误报。

本文设计的方案在传统 EWMA 算法上新增可以选择一个自然数 m , 记录预测阈值之前的 m 次实际数据采集值, 求出其标准差作为新阈值的调整项, 最终该标准项取值的正负取决于如下思路: 假设数据变化存在惯性, 即当计算第 n 次阈值时, 会检测第 $n-1$ 次和第 $n-2$ 次收集到的实际数据值, 若第 $n-1$ 次的流量大于第 $n-2$ 次的流量则调整项取正, 反之取负。

$$h_n = \beta h_{n-1} + (1 - \beta)x_n \pm \sqrt{\sum_{i=n-m+1}^{n-1} (x_i - x_{i-1})^2} \quad (7)$$

如果 $n < m$, 则式 (7) 中参数不足, 改写为:

$$h_n = \beta h_{n-1} + (1 - \beta)x_n \pm \sqrt{\sum_{i=0}^n (x_i - x_{i-1})^2}, h_0 = 0 \quad (8)$$

为了保存计算出的阈值, 需要一个与收集流量数据形式相同的 4×256 表结构用于存储。每次计算出新的阈值后, 新的数据将覆盖先前保存的阈值信息。

考虑到 CUSUM 算法的检测步骤需求, 发现均值偏移时, 该 x_{n+1} 作为非法数值, 将不参与后续阈值更新。

3.4 基于改进型 CUSUM 的 DDoS 攻击识别算法

通常情况下 CUSUM 算法采用随机序列生成偏移识别所需要的参数, 但网络环境具有自身的特点, 其参数构造会影响 CUSUM 算法的初始参数, 本文根据常规网络应用和 DDoS 攻击的特点, 设计适用于 DDoS 攻击识别 CUSUM 算法参数, 假设在时间段 n , 某个转发端口采集到的数据流量为 x_n , 定义如下参数:

$$\delta_n = \alpha \delta_{n-1} + (1 - \alpha)x_n \quad (9)$$

$$Z_n = \begin{cases} x_n - \delta_n, & x_n > \delta_n \\ 0, & x_n \leq \delta_n \end{cases} \quad (10)$$

$$S_n = \sum_{i=1}^n Z_i, S_0 = 0 \quad (11)$$

$$Y_n = S_n - \min_{0 \leq k \leq n-1} S_k \quad (12)$$

此时 δ_n 表示某个 IP 地址转发数据量均值, α 取值范围是 0.01~0.03, 用于调整不同网络环境下的识别参数。为了完成攻击识别, 给出如下定义。

定义 2 在本文设计的 DDoS 攻击识别模型中, 在检测时段 $t-1$, 如果满足:

$$Y_{t-1} < \frac{h_{t-2}}{\lambda} \quad (13)$$

而在检测时段 t , 发生:

$$Y_t \geq \frac{h_{t-1}}{\lambda} \quad (14)$$

则认为时间段 t 中发生 DDoS 异常攻击, 其中 h_{t-2} 、 h_{t-1} 为利用第 2.3 节中给出的方法计算的流量阈值, λ 为门限调整倍数, 其取值范围为 $10 \leq \lambda \leq 20$ 。

4 系统实现与系统测试

4.1 系统实现环境与步骤

本系统部署于路由器, 系统主要分为 2 个模块, 其一为数据采集模块, 主要利用 BloomFilter 算法收集流量数据和更新存储的历史数据; 另一个模块为数据聚集判定模块, 利用改进 EWMA 算法计算阈值并利用改进 CUSUM 算法判定目标地址是否遭到攻击。

其关键步骤包括:

步骤 1 分配存储历史数据 x 的 m 个 BloomFilter 散列表;

步骤 2 分配存储上一次报警阈值 h_{n-1} 的 BloomFilter 散列表;

步骤 3 分配存储当前报警阈值 h_n 的 BloomFilter 散列表;

步骤 4 分配记录当前时段检测流量的 BloomFilter 散列表。

每当检测时段结束, 攻击检测的关键步骤包括:

步骤 1 利用式 (9)~式 (12) 计算识别参数 δ_n, Z_n, S_n, Y_n ;

步骤 2 比较 Y_n 及 $\frac{h_{t-1}}{\lambda}$, 如果满足式 (14) 则认为发生

DDoS 攻击, 并跳过步骤 3、步骤 4;

步骤 3 利用当前数据 x_n 替代历史数据散列表最旧的数据 x_{n-m+1} , 如果 $n < m$ 则直接更新 x_n 至历史数据散列表;

步骤 4 基于 n 和 m 的大小关系利用式 (7) 或式 (8) 计算新的报警阈值并更新上一次报警阈值散列表和当前报警阈值散列表;

步骤 5 进入下一个检测周期。

攻击检测的主要流程如图 2 所示。

4.2 系统测试

本文设定的系统在电力系统内部仿真环境进行了仿

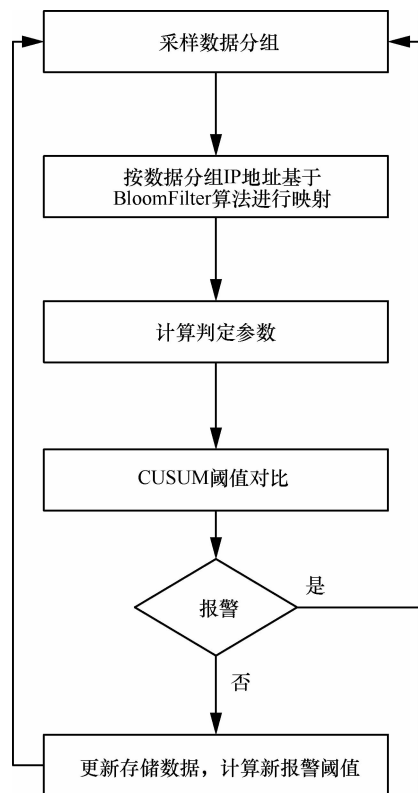


图2 基于 BF-DT-CUSUM 算法的 DDoS 攻击检测示意

真, 这里采用多台傀儡机实现大规模 TFN-DDoS 攻击, 并在路由端记录每一分钟内转发的数据分组数量(每秒完成一次检测周期), 其结果如图 3、图 4 所示。

低强度 DDoS 攻击(如图 3(a)所示)中, 平均总数据分组在 700 左右, 预设攻击数据分组为 660 个, 每次约有 650 个数据分组被拦截, 而发生大规模 DDoS 攻击(如图 3(b)所示)时, 每秒有 1 万个攻击的数据分组被接收(另有 4 000 个正常数据分组), 这些数据分组全部被丢弃。

图 4 给出了在图 3(b)条件下的开始 DDoS 攻击 1 min 内总的接收/发送数据分组示意(攻击于第 25 s 开始), 可见在起始攻击阶段, 识别算法未发现存在攻击, 总接收数据分组数量与转发数量一致, 而到约 28 s 识别算法发现存在 DDoS 攻击, 并在 30 s 开始拦截数据分组, 从而导致 DDoS 攻击被有效防御。

5 结束语

针对智能电网工控系统中的入侵攻击检测问题, 本文提出了一种基于 BloomFilter 地址统计的动态阈值更新的改进型 CUSUM(BF-DT-CUSUM)DDoS 异常流量识别算法。通过分析智能电网工控系统安全体系结构, 结合电网流量特性与 DDoS 攻击特征, 提出了一种基于 BloomFilter 算法和 CUSUM 算法的动态阈值 DDos 被攻击地址检测模型, 和一种存在上限并包含调整项和缓冲流量项的改进型 EWMA 动态阈值生成算法, 该方法中调整区间长度因子大小可变, 该调整项正负性由流量变化惯性决定。

Log File Details:

total_num=5197	drop_num=5120	t
total_num=5848	drop_num=5760	t
total_num=6499	drop_num=6400	t
total_num=7144	drop_num=7040	t
total_num=7769	drop_num=7660	t
total_num=8426	drop_num=8300	t
total_num=9077	drop_num=8940	t
total_num=9728	drop_num=9580	t
total_num=10376	drop_num=10220	t
total_num=11027	drop_num=10860	t
total_num=11678	drop_num=11500	t
total_num=12329	drop_num=12140	t
total_num=12980	drop_num=12780	t
total_num=13631	drop_num=13420	t
total_num=14282	drop_num=14060	t
total_num=14933	drop_num=14700	t
total_num=15584	drop_num=15340	t
total_num=16235	drop_num=15980	t
total_num=16886	drop_num=16620	t
total_num=17537	drop_num=17260	t
total_num=18188	drop_num=17900	t
total_num=18839	drop_num=18540	t

(a) 低强度DDoS攻击

Log File Details:

total_num=150588	drop_num=65600	t
total_num=164659	drop_num=75740	t
total_num=178829	drop_num=85100	t
total_num=192923	drop_num=94300	t
total_num=207145	drop_num=104300	t
total_num=221041	drop_num=114100	t
total_num=235098	drop_num=122780	t
total_num=249188	drop_num=132500	t
total_num=263433	drop_num=142640	t
total_num=277272	drop_num=151678	t
total_num=291377	drop_num=161718	t
total_num=305671	drop_num=171978	t
total_num=319788	drop_num=181018	t
total_num=333842	drop_num=190438	t
total_num=347918	drop_num=200338	t
total_num=361873	drop_num=210118	t
total_num=375938	drop_num=218918	t
total_num=390170	drop_num=228858	t
total_num=404390	drop_num=238218	t
total_num=418376	drop_num=247958	t
total_num=432518	drop_num=257978	t
total_num=446667	drop_num=267998	t

(b) 高强度DDoS攻击

图3 日志记录转发数据分组与拦截情况示意

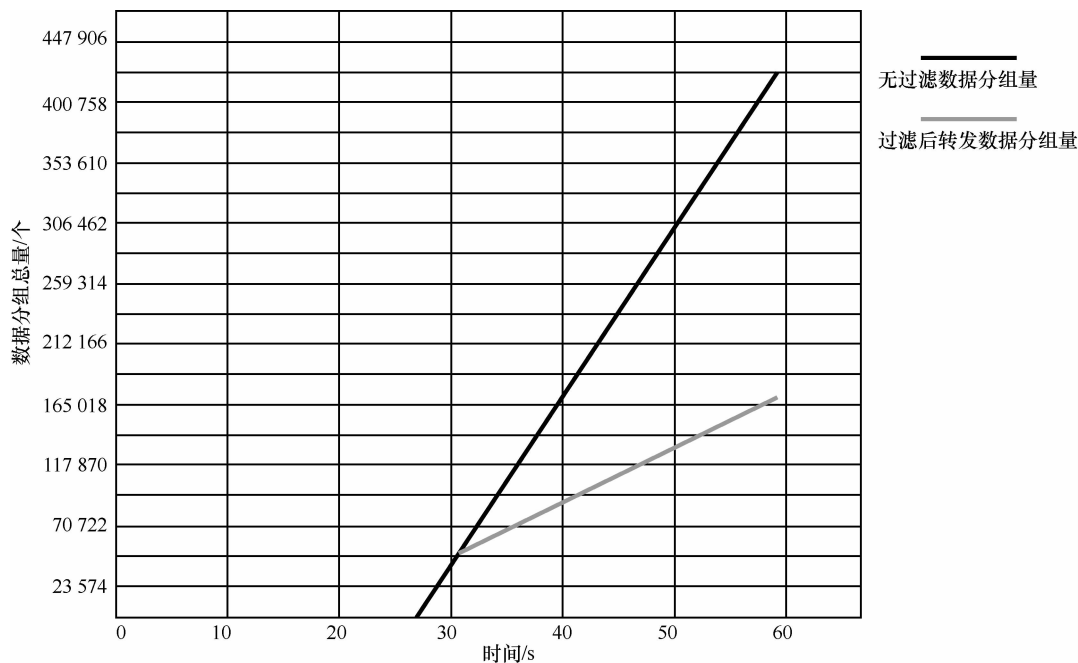


图4 高强度 DDoS 攻击起始 1 min 内数据分组转发情况示意

仿真实验表明该算法能够提高入侵攻击检测的准确性以及在线检测速度,并降低运算开销,该算法可以作为嵌入式模块,安装在核心路由器中,提高电力网络的总体性能。

参考文献:

- [1] FANG X, MISRA S, XUE G L, et al. Smart grid-the new and improved power grid: a survey [J]. IEEE Communications Surveys & Tutorials, 2012, 14(4): 944-980.
- [2] WANG W Y, LU Z. Cyber security in the smart grid: survey and challenges [J]. Computer Networks, 2013, 57 (5): 1344-1371.
- [3] METKE A R, EKL R L. Security technology for smart grid networks [J]. IEEE Transactions on Smart Grid, 2010, V1(1): 99-107.
- [4] LINE M B, TONDEL I A, JAATUN M G. Cyber security challenges in smart grids [C]// The 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe), December 5-7, 2011, Manchester, United Kingdom. New Jersey: IEEE Press, 2011: 1-8.
- [5] FALLIERE N, MURCHU L O, CHIEN E. W32stuxnet dossier [R]. 2011.
- [6] CHEN T M. Stuxnet, the real start of cyber warfare? [J]. IEEE Network, 2010, 24(6): 2-3.
- [7] LU Z, LU X, WANG W, et al. Review and evaluation of security threats on the communication networks in the smart grid [C] // The 2010 Military Communications Conference (MILCOM 2010), October 31-November 3, 2010, San Jose, USA. [S.l.: s.n.], 2010: 1830-1835.
- [8] DOULIGERIS C, MITROKOSTA A. DDoS attacks and defense mechanisms: classification and state-of-the-art [J]. Computer Networks, 2004, (44): 643-666.
- [9] VALDES A, CHEUNG S. Intrusion monitoring in process control systems [C] // The 42nd Hawaii International Conference on System Sciences(HICSS'09), January 5-8, 2009, Hawaii, USA. Washington: IEEE Computer Society, 2009: 1-7.
- [10] Systems C. Security for the smart grid [R]. San Jose: Cisco, 2009.
- [11] LIANG Z Q, FAN Y. Principles and defense techniques of DDoS attacks in electricity auxiliary system security protection [J]. Computer Security, 2010(9): 70-72.
- [12] SUN Y A, GUAN X H, LIU T, et al. A cyber-physical monitoring system for attack detection in smart grid [C] // IEEE INFOCOM 2013, April 26-May 1, 2013, Hong Kong, China. Washington: IEEE Computer Society, 2013.
- [13] YI H, EEMALIFALAK M, NGUYEN H, et al. Bad data injection in smart grid: attack and defense mechanisms [J]. IEEE Communications Magazine, 2013, 51(1): 27-33.
- [14] LIU T, YUN G, DAI W, et al. A novel method to detect bad data injection attack in smart grid [C] // The 2013 IEEE Conference on Computer Communications Workshops



(INFOCOM WKSHPS), April 14-19, 2013, Turin, Italy. Washington: IEEE Computer Society, 2013: 49-54.

[15] WANG D, GUAN X H, LIU T, et al. Extended distributed state estimation: a detection method against tolerable false data injection attacks in smart grids [J]. Energies, 2014, 7(3): 1517-1538.

[16] KOSUT O, JIA L Y, THOMAS R J, et al. Malicious data attacks on the smart grid [J]. IEEE Transactions on Smart Grid, 2011, 2(4): 645-658.

[17] LIU Y, NINE P, REITER M K. False data injection attacks against state estimation in electric power grids [J]. ACM Transactions on Information and System Security, 2011, 14(1): 1301-1333.

[作者简介]



费稼轩(1984-),男,国网智能电网研究院工程师,主要研究方向为电网工控安全。



张涛(1976-),男,国网智能电网研究院高级工程师,主要研究方向为电网信息安全。



马媛媛(1978-),女,国网智能电网研究院高级工程师,主要研究方向为电网信息安全。



周诚(1981-),男,国网智能电网研究院工程师,主要研究方向为电网信息安全。