计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(12):41−50 [doi: 10.15888/j.cnki.csa.008832]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

面向 VNDN 的兴趣包洪泛攻击检测①

樊　娜, 李思瑞, 邹小敏, 高艺丰

(长安大学 信息工程学院, 西安 710064)
通信作者: 李思瑞, E-mail: 2020124137@chd.edu.cn

摘　要: 在车载命名数据网络 (VNDN) 中, 兴趣包洪泛攻击 (IFA) 通过发送大量恶意兴趣包占用甚至耗尽网络资源, 导致合法用户的请求无法被满足, 严重危害了车联网的运行安全. 针对上述问题, 本文提出了一种基于流量监测的 IFA 检测方法. 首先构建基于 RSU 的分布式网络流量监测层, 每个 RSU 监测其通讯范围内的网络流量, RSU 之间通信互联形成 RSU 网络流量监测层. 其次, 设定固定时间窗口, 对每个窗口内的网络流量通过信息熵、网络自相似性和奇异点 3 个维度进行分析. 其中, 为了利用信息熵反映兴趣包来源的分布, 在兴趣包中添加了新的字段. 最后, 综合上述 3 个指标, 判断兴趣包洪泛攻击的存在. 仿真实验结果表明, 本文提出的方法有效地提升了兴趣包洪泛攻击检测的准确率, 降低了误判率.

关键词: 车载命名数据网络; 兴趣包洪泛攻击; 小波分析; 自相似性; 信息熵; 信号处理; 网络安全

引用格式: 樊娜,李思瑞,邹小敏,高艺丰.面向 VNDN 的兴趣包洪泛攻击检测.计算机系统应用,2022,31(12):41–50. http://www.c-s-a.org.cn/1003-3254/8832.html

Interest Flooding Attack Detection for VNDN

FAN Na, LI Si-Rui, ZOU Xiao-Min, GAO Yi-Feng

(School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: In vehicular named data network (VNDN), interest flooding attack (IFA) occupies or even exhausts network resources by sending a large number of malicious interest packets, which results in the failure to meet the requests of legitimate users and seriously endangers the operation safety of Internet of Vehicles (IoV). To solve the problems, this study proposes an IFA detection method based on traffic monitoring. Firstly, a distributed network traffic monitoring layer based on RSU is constructed, where each RSU monitors the network traffic within its communication range, and the communication interconnection between RSUs forms the RSU network traffic monitoring layer. Secondly, a fixed time window is set, and the network traffic in each window is analyzed from three dimensions, i.e., information entropy, network self-similarity, and singularity. Additionally, a new field is added to the interest packet, and thus information entropy can be used to reflect the distribution of interest packet sources. Finally, the above three indicators are comprehensively employed to judge the existence of attack. The simulation results indicate that the proposed method effectively improves the accuracy of IFA detection and reduces the misjudgment rate.

Key words: vehicular named data network (VNDN); interest flooding attack (IFA); wavelet analysis; self-similarity; information entropy; signal processing; network security

近年来, 车联网作为智能交通的重要组成部分, 越来越受到工业界和学术界的关注. 车联网与道路安全、行车安全、驾驶员的生命安全息息相关, 因而车联网中信息的准确性是保障车联网安全运行的关键.

① 基金项目: 陕西省重点研发科技计划 (2022GY-039)
收稿时间: 2022-03-19; 修改时间: 2022-04-14; 采用时间: 2022-04-29; csa 在线出版时间: 2022-07-29

然而, 以 TCP/IP 为中心的传统网络架构在移动性、安全性和内容分发方面存在限制, 不能很好地适应车联网环境, 提升车联网系统的性能. 为了更好地适应车联网特性, 在车联网中引入了命名数据网络 (named data networking, NDN) 架构[1], 形成车载命名数据网络 (vehicular named data network, VNDN). 命名数据网络作为新一代网络架构, 是以内容为中心的网络.

VNDN 中有两个角色, 分别是消费者和生产者. 消费者通过发送兴趣包 (interest packet) 请求所需的数据, 生产者根据兴趣包返回相应的数据包 (data packet). VNDN 中每个节点维护 3 个数据结构, 分别是待处理兴趣表 (pending interest table, PIT)、 内容存储 (content store, CS) 和转发信息库 (forwarding information base, FIB). VNDN 中节点处理兴趣包和数据包的过程如图 1 所示[2].

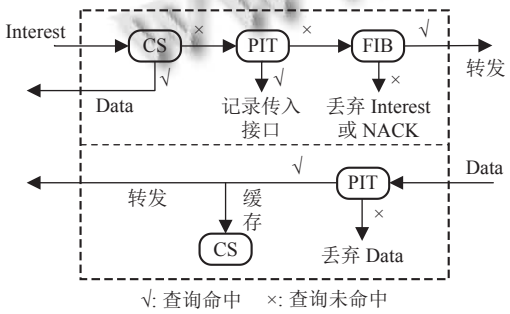


图 1 VNDN 转发机制

VNDN 中, 恶意节点通过发送大量不合法兴趣包发动兴趣包洪泛攻击 (interest flooding attack, IFA). 大量违法兴趣包所产生的大量 PIT 条目在过期或被满足之前都会存在于合法节点的 PIT 中, 从而占用或耗尽 PIT 资源, 导致合法的兴趣包无法得到满足, 进一步导致合法车辆无法获取相关信息, 降低整个网络的性能. VNDN 的正常运行, 与实时准确的信息获取密切相关, 因此 IFA 严重危害了 VNDN 的网络安全.

近年来, 关于命名数据网络中的兴趣包洪泛攻击已有大量研究, 很多学者提出了 IFA 检测方法. Abdullah 等[3] 提出一种基于流量优先级的 IFA 检测方案. 该方案通过邻居协作的方式, 计算传入兴趣包流的优先级, 判定恶意车辆节点传入的可疑流量. 然而, 该方法依赖于多个指标的计算. Sattar 等[4] 提出一种基于 PIT 的检测方案. 计算 PIT 中前缀对应的兴趣包数量, 并与网络中广播 1 s 发送的兴趣包数值相比较, 如果大于该数值则判定攻击发生. 然而, 该方案的判别标准较为单一. Benmoussa 等[5] 提出拥塞感知的 IFA 检测方案. 网络拥塞会导致路由器错误地认为合法用户是恶意用户. 该方案引入网络拥塞参数, 以避免由路由器行为引发的错误警报.

Hou 等[6] 提出 TC 检测方案. 该方案将兴趣包进行分组, 利用组内和组间名称的分布来检测 IFA. 通过计算名称的熵值, 反映名称分布. 然而该方法无法应对复杂攻击. 侯睿等[7] 提出一种基于信息熵的兴趣包洪泛攻击检测方法 EIM. 该方法在考虑信息熵的基础上, 又引入了用户的信誉值, 以达到较低的误判率. Zhi 等[8] 提出一种基于熵-SVM 和 JS 散度的 IFA 抵抗机制. 通过基于 KKT 条件的增量学习, 该方法能够有效地检测和缓解 IFA. 邢光林等[9] 提出了一种基于包标记的攻击检测方法. 该方法在兴趣包中添加了路由器 ID 和接口号字段, 并利用累积熵和相对熵检测攻击. 利用兴趣包的路由器接口分布, 追溯攻击.

Mounika 等[10] 提出一种基于卡方检验和相似性检验的 IFA 检测技术. 利用卡方检验的易感性来区分兴趣包前缀的差异. Nguyen 等[11] 提出一种基于概率分布的方案. 通过扩展局部检测来解决数据包丢失率未知的情况. 为了提高检测精度, 还提出一种顺序检测方法. Xin 等[12] 提出一种基于小波分析的检测方法, 该方法面向共谋兴趣包洪泛攻击 (collusive interest flooding attacks, CIFA). 经小波变化后, CIFA 的能量谱密度主要集中在低频及其高次谐波上. 基于上述现象, 提取攻击子频带内的信号, 从而检测 CIFA. Shigeyasu 等[13] 提出一种新的 CIFA 检测方法. 该方法通过计算中继路由器上缓存引用的数目来检测攻击. 吴志军等[14] 提出一种基于关联规则算法和决策树算法的联合检测方案, 该方案提出新的判断指标“CS 异常偏离率”, 并且可以实现对 IFA 和 CIFA 的有效区分.

文献 [3–5] 提出的方法适用于 VNDN, 通过统计相关接口的传输速率或相关资源的利用率实现攻击检测, 依赖车辆节点自身的算力, 然而车辆节点的计算能力有限. 文献 [6–9] 均采用了熵值的计算, 然而由于车联网的动态性, 正常网络流量的熵值也存在波动, 容易造成误判. 文献 [10–14] 提出的方法仅适用于命名数据网络, 未考虑车辆节点的移动性, 因而在车联网环境中不能发挥最大性能.

针对上述方法的不足, 以及车联网高移动、高动

态拓扑的特点[15], 本文提出一种基于流量监测的 IFA 检测方案, 利用路侧基础设施 (road side unit, RSU) 作为流量监测节点, 结合信息熵与自相似性检测攻击, 使用小波分析定位攻击. 本方案适用于车联网场景, 能有效地检测出 IFA 攻击, 提升攻击检测准确率.

1 VNDN 攻击类型分析

VNDN 中的主要攻击类型是兴趣包洪泛攻击, 类似于传统网络中的分布式拒绝服务攻击 (distributed denial of service attack, DDoS). 恶意车辆通过发送恶意兴趣包至附近的合法车辆及 RSU[16], 占用网络资源, 导致合法请求无法得到满足.

针对兴趣包洪泛攻击, 本文考虑以下两种类型.

(1) 简单类型 IFA: 简单类型的兴趣包洪泛攻击是最常见的攻击类型[17], 恶意节点通过发送大量前缀无效的兴趣包以请求网络中不存在的数据. 大量无效的兴趣包在传播过程中, 占用传播链路上合法节点的 PIT 资源. 由于这些兴趣包无法被满足, 在过期被删除之前, 将会一直占用甚至耗尽合法节点的 PIT 资源, 从而影响整个网络的性能. 简单类型 IFA 的攻击示意图如图 2(a) 所示. 简单类型 IFA 在某一时刻发起, 恶意节点在时间 T 内以某一恒定速率发布无效兴趣包, 攻击流大小为 d. 简单兴趣包洪泛攻击持续的时间较长, 攻击频率呈不规则性.

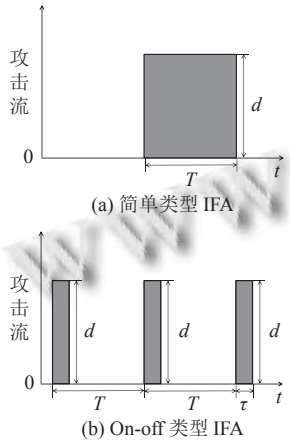


图 2 IFA 攻击形式示意图

(2) On-off 类型 IFA: On-off 类型的 IFA 也称为开关型的兴趣包洪泛攻击. 开关型攻击类似于分布式低速率拒绝服务攻击 (distributed low-rate denial of service attack, DLDoS), 隐匿性更强, 其网络流量具有一定特征[18]. On-off 类型 IFA 的攻击者具有两种状态, 即攻击状态和正常状态. 当恶意节点处于攻击状态时, 发起攻击, 其攻击方式与简单类型 IFA 相同; 当恶意节点处于正常状态时, 停止攻击. On-off 类型 IFA的攻击示意图如图 2(b) 所示. 开关型 IFA 攻击频率呈周期性. 恶意节点在周期 T 内, 以某一恒定速率发送无效兴趣包, 持续时间为 τ, 攻击流大小为 d. 开关型 IFA的平均攻击速率较低, 类似于分布式低速率拒绝服务攻击.

2 基于流量监测的 IFA 检测方法

车联网中车辆节点具有高速移动性, 如果依靠车辆节点监测网络流量, 则无法实时准确地反映网络流量状况. 因此, 本文提出基于 RSU 的分布式网络流量监测层. 由于 RSU 计算能力大于车载单元的计算能力, 并且 RSU 的通讯范围通常大于车辆的通讯范围, 所以将 RSU 作为监测节点, 每个 RSU 监测其通讯范围内的网络流量. RSU 之间构成静态网络拓扑, 实现网络流量的实时监测.

其次, 本文提出多指标联合判断 IFA 产生的方法 DSFA (detection scheme based on flow analysis). 首先, 提取每个时间窗口内的网络流量数据; 其次, 通过 3 个维度分析流量特征; 最后, 经过阈值比较, 判断攻击是否发生. 3 个判别条件分别是: 利用信息熵判断兴趣包来源的分布, 计算流量的 Hurst 指数判断自相似性是否异常, 利用离散小波变换技术进行奇异点检测.

2.1 RSU 网络流量监测层

本文设计了一个基于 RSU 的网络流量监测层, 将流量监测的任务从车辆节点转移至 RSU 节点, 解决了由车辆节点移动、车辆节点计算能力有限而引发的监测结果不准确的问题, 实现对 VNDN 中流量状况的实时监测. RSU 是静态分布的节点, 在 VNDN 中担任中间路由的角色. RSU 互联通信, 形成 RSU 网络流量监测层, 同时构成数据检索层. 该网络具有分层结构, 边缘节点设置为接入节点 (access point, AP), 直接与车辆节点进行交互, 同时与其他节点进行通信; 除边缘节点外的其他节点称为路由节点 (route, R), 不与车辆节点直接交互, 仅与路由节点进行通信. RSU 网络流量监测层的结构图如图 3 所示.

RSU 均匀分布在道路两侧, 分别担任接入节点和路由节点的角色. 在车联网场景中, 当车辆节点请求数据时, 首先需要接入 RSU 网络流量监测层, 即车辆节

点发送兴趣包至最近的 RSU. 该网络完成数据检索后, 返回相应的数据包至车辆节点. 该场景下, IFA 产生的大量无效兴趣包进入 RSU 网络, 占用或耗尽 PIT 资源, 降低合法节点的数据请求效率或致使合法请求无法得到满足. 利用上述特点, 将静态节点 RSU 作为车联网的流量监测节点, 每个 RSU 负责监测通讯范围内的流量状况. RSU 监测网络流量的场景图如图 4 所示. 图 4 展示了网络中存在攻击的场景, RSU 监测的网络流量是由合法流量和恶意流量构成的混合流量. 本文通过在混合流量中检测恶意流量的存在, 判断网络是否遭受 IFA 的攻击.

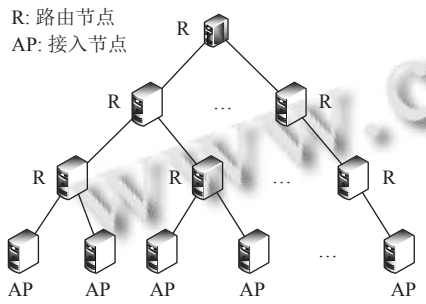


图 3 RSU 网络流量监测层的结构示意图

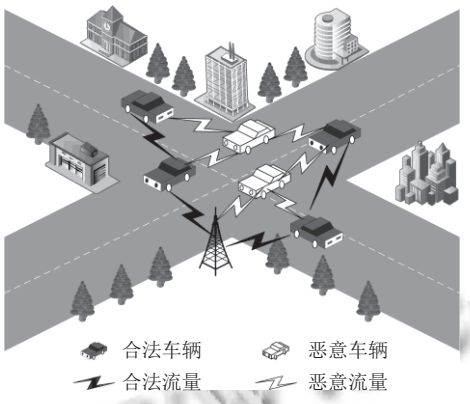


图 4 VNDN 攻击场景示意图

2.2 IFA 检测方案

以上述网络架构为基础, 本文提出一个基于流量分析的 IFA 检测方案 DSFA. 从 3 个维度对流量进行分析, 分别是熵、自相似性和奇异点. 首先, 通过在兴趣包中添加字段 Source ID, 计算熵值; 其次通过计算 Hurst 指数检测网络的自相似性; 然后综合考虑上述两个指标, 判断攻击的存在; 最后利用小波分析法对流量的奇异性进行检测, 确定网络流量中奇异点的位置, 定位攻击.

本方案设定固定的时间窗口[19], 依次判断每一个时间窗口内的流量是否异常. 具体检测流程如算法 1 所示. 其中, 步骤 3 中的 $Th1$ 与 $Th2$ 分别是熵值 E 和 Hurst 指数 H 值对应的阈值; $Th1$ 与 $Th2$ 是经多次实验得到的经验值.

算法 1. DSFA 工作流程

输入: 时间窗口 T_m 内的流量数据 $X(T_m)$
输出: 攻击警告 alarm, 攻击发生时刻 t_{attack}

1. 计算信息熵 E
2. 计算 Hurst 指数 H 值
3. **if** $E<Th1$ && $H>Th2$ **then**
4. 根据算法 3 检测奇异点的存在
5. **if** *exist* := true **then**
6. **return** alarm && t_{attack}
7. **end if**
8. **else**
9. 进入下一个时间窗口 T_{m+1}, 返回步骤 1
10. **end if**

2.2.1 信息熵计算

为了确定兴趣包来源节点的分布, 本文对兴趣包的结构进行修改, 添加 Source ID 字段. Source ID 指发送该兴趣包的消费者的 ID. 兴趣包的格式如图 5 所示.

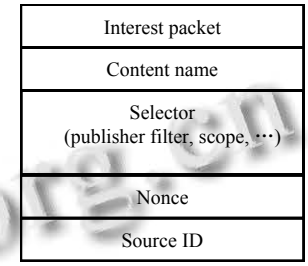


图 5 兴趣包格式

借助信息熵能反映出信息源分布随机性的特点, 本文利用信息熵对 VNDN 中的 interest 包来源分布情况进行实时检测, 熵值 E 的计算公式如式 (1):

$$E = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{1}$$

其中, p_i 是第 i 个兴趣包来源节点出现的频率. 当 n 为 1 时, E 取最小值 0. 当每个兴趣包来源节点出现的频率均为 $1/n$ 时, E 取最大值 $\log_2 n$. 熵值可以反映 RSU 监测节点所接收兴趣包的来源情况. E 越大, 说明 RSU 接收兴趣包的来源越随机; 反之, 说明兴趣包的来源越集中, 仅某些节点的出现频率较高, 即存在部分兴趣包均来源于某一节点的情况. 上述场景可能是网络中合

法节点的偶然情况, 也可能是网络中恶意节点的攻击行为. 车联网场景中, 由于车辆的移动性, 兴趣包的来源分布情况较为随机, 即便熵值存在波动, 也在一个有限的范围内. 因此, 只要选取合适的阈值, 就能利用熵值检测 IFA 的存在.

2.2.2 Hurst 指数

传统网络中的正常网络流量存在自相似性, 在 VNDN 中, 亦是如此. 针对 DDOS 攻击, 采用基于流量自相似性的检测方案, 被验证是可行的[20]. 利用自相似性, 可以实现正常网络流量与被攻击网络流量的区分, 能有效地完成攻击检测. 本文针对的 IFA 类似于 DDOS 攻击, 因此引入自相似性作为判别 IFA 的标准之一.

Hurst 指数是唯一一个描述自相似性的参数, 它反映网络流量的自相似程度. 通过计算 H 值, 可以判断网络流量的状况. 当 $0<H<0.5$ 时, 网络流量不具有自相似性; 当 $H=0.5$ 时, 网络流量不表现出自相似性; 当 $0.5<H<1$ 时, 网络流量具有一定的自相似性, 即在长时间尺度上, 网络流量具有相关性. 正常网络流量的 H 值范围在 (0.5, 1) 区间. 当网络中发生 IFA 攻击时, H 值会下降. 根据上述特征, 本文通过 R/S 方法计算 H 值[21], 检测 IFA 的发生. R/S 方法的计算流程如算法 2 所示.

算法 2. R/S 算法

输入: 时间窗口 T_m 内的流量数据 $X(T_m)=\{X_i, 1\leqslant i\leqslant L\}$
输出: H 值

1. 将 $X(T_m)$ 划分成 L/n 个长度为 n 的子序列
2. 根据式 (2) 求子序列的和
3. 根据式 (3) 求样本方差
4. 根据式 (4) 求极差
5. 对式 (5) 两边取对数, 得到式 (6)
6. 画出所有的 ($\log n$, $\log E(R/S)$) 点
7. 拟合直线
8. 求斜率即为 H

子序列求和公式:

$$Y(n)=\sum_{i=1}^{n}X_i \tag{2}$$

样本方差计算公式:

$$s^2(n)=\frac{1}{n}\sum_{i=1}^{n}X_i^2-\left(\frac{1}{n}Y(n)\right)^2 \tag{3}$$

极差计算公式:

$$R(n)=\max_{0\leqslant t\leqslant n}\left[Y(t)-\frac{t}{n}Y(\mathrm{n})\right]-\min_{0\leqslant t\leqslant n}\left[Y(t)-\frac{t}{n}Y(n)\right] \tag{4}$$

自相似过程满足关系:

$$E\left(\frac{R(n)}{S(n)}\right)\sim \alpha n^H,\ n\to\infty \tag{5}$$

关系式:

$$\log E\left(\frac{R(n)}{S(n)}\right)=H\log n+c,\ n\to\infty \tag{6}$$

其中, α、c 均为常数.

2.2.3 奇异性检测

简单类型 IFA 和 on-off 类型 IFA 都类似于分布式拒绝服务攻击 DDOS. 传统网络中, 面向 DDOS 检测的网络流量分析方法主要分为 3 个方面: 网络流量分析方法, 异常网络流量检测方法, 网络流量的自相似性. 其中, 基于小波技术的异常网络流量检测方法是一种常见的技术手段. 小波变换类似加窗傅里叶变换, 但在研究信号奇异性方面, 前者优于后者. 两者的差异体现在, 傅里叶变换只能从整体性质来反映函数的奇异性, 无法敏感地检测出信号突变; 小波变换具有在时间域对信号进行局部化分析的能力, 刻画信号的细节特征. 因此, 利用小波变换可确定信号奇异点的分布情况. 小波分解信号的基本流程如图 6 所示.

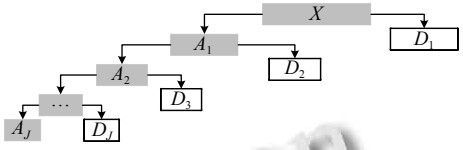


图 6 J 级小波分解示意图

图 6 展示了 J 级小波分解的过程, 其中 J 表示分解的最大层数, X 表示原信号. 经过 1 级小波分解, 原信号被分为低频分量 A_1 和高频分量 D_1. 然后再对低频分量 A_1 进行 2 级小波分解, 得到低频分量 A_2 和高频分量 D_2. 以此类推, 完成 J 级分解后, 得到低频系数 A_J 和一组高频系数 $D_1, D_2, \cdots, D_J$. 低频系数也称近似系数 (approximation coefficients), 反应信号的轮廓信息; 高频系数也称细节系数 (detail coefficients), 反应信号的细节信息. 给定一个小波基函数 $\psi(t)$, 其经过平移和缩放得到函数 $\psi_{j,k}(t)$:

$$\psi_{j,k}(t)=2^{j/2}\psi\left(2^j t-k\right) \tag{7}$$

设原始信号为 $x(t)$, 其 J 级小波级数展开如式 (8) 所示:

$$x(t)=\sum_k a_x(J,k)\,\Phi_{J,k}(t)+\sum_{j=1}^{J}\sum_k d_x(j,k)\,\psi_{j,k}(t) \tag{8}$$

其中, $\Phi_{J,k}(t)$ 是小波尺度函数, $\psi_{j,k}(t)$ 是小波母函数, $a_x(J,k)$ 是小波尺度系数, $d_x(j,k)$ 是小波系数. 小波系数的定义为:

$$d_x(j,k) = < x, \psi_{j,k}(t) > \tag{9}$$

第 j 层小波系数重构信号的公式如下:

$$x_j(t) = \sum_k d_x(j,k)\psi_{j,k}(t) \tag{10}$$

本文利用小波变换检测奇异点的具体步骤如算法 3 所示.

算法 3. 奇异点检测算法

输入: 时间窗口 T_m 内的流量数据 $X(T_m)$, 小波基函数, 小波分解最大层数 J
输出: 奇异点的位置

1. 根据式 (8) 对 $X(T_m)$ 进行 J 级小波分解
2. **for** $j \leftarrow J/2, J$ **do**
3. 根据式 (9) 提取每一层的细节系数 $d_x(j,k)$
4. 根据式 (10) 在 j 层重构信号, 得到 $x_j(t)$
5. 对 $x_j(t)$ 取模, 得到$|x_j(t)|$
6. **end for**
7. **for** $j \leftarrow J/2, J-1$ **do**
8. $temp = |x_j(t)| \times |x_{j+1}(t)|$
9. $sum = sum + temp$
10. **end for**
11. 阈值处理 sum
12. 提取极大值位置, 即奇异点的位置
13. 返回奇异点的位置

算法 3 中步骤 8 和步骤 9 是为了增强模极大值, 使其更加显著. 步骤 11 阈值处理是指设定一个阈值, 低于该值的点被设置为 0, 而高于或等于该值的点保留原值. 上述两个步骤都是为了更快速地搜索极大值的位置. 步骤 13 可能返回多个位置, 其中包含由正常网络波动产生的干扰点.

3 实验分析

3.1 实验环境设置

为了验证本文提出的攻击检测方案 DSFA, 使用 ndnSIM 仿真平台模拟命名数据网络, 同时在该平台上搭建车联网环境. ndnSIM 是一种基于 ns3 的 NDN 网络模拟器[22]. 实验设置 85 个 RSU 节点, 构成 RSU 静态拓扑网络. 该网络中, 每个节点都只有一个父节点; 除叶子节点外, 每个节点均有 4 个子节点. 该网络中 16 个接入节点被设置为生产者, 其他节点设置为路由节点; 所有车辆节点设置为消费者. 本实验使用的操作系统为 Ubuntu 16.04 LTS, 车辆间通讯使用的协议为 IEEE 802.11p. 本文选择基于小波分析的检测方法[12]、基于自相似性的检测方法[21] 和基于信息熵的检测方法[7] 作为对比方案, 选择检测率、误判率和准确率作为对比指标. 其他实验参数如表 1 所示.

表 1 实验参数

参数	值
实验环境范围 (m×m)	1000×1000
车辆节点数量 (个)	100
恶意节点占比 (%)	20, 30
合法节点发包速率 (packets/s)	10
恶意节点发包速率 (packets/s)	50
RSU数量 (个)	85
RSU通讯半径 (m)	110
实验时间 (s)	100
On-off攻击周期 (T, τ) (s)	(20, 10)

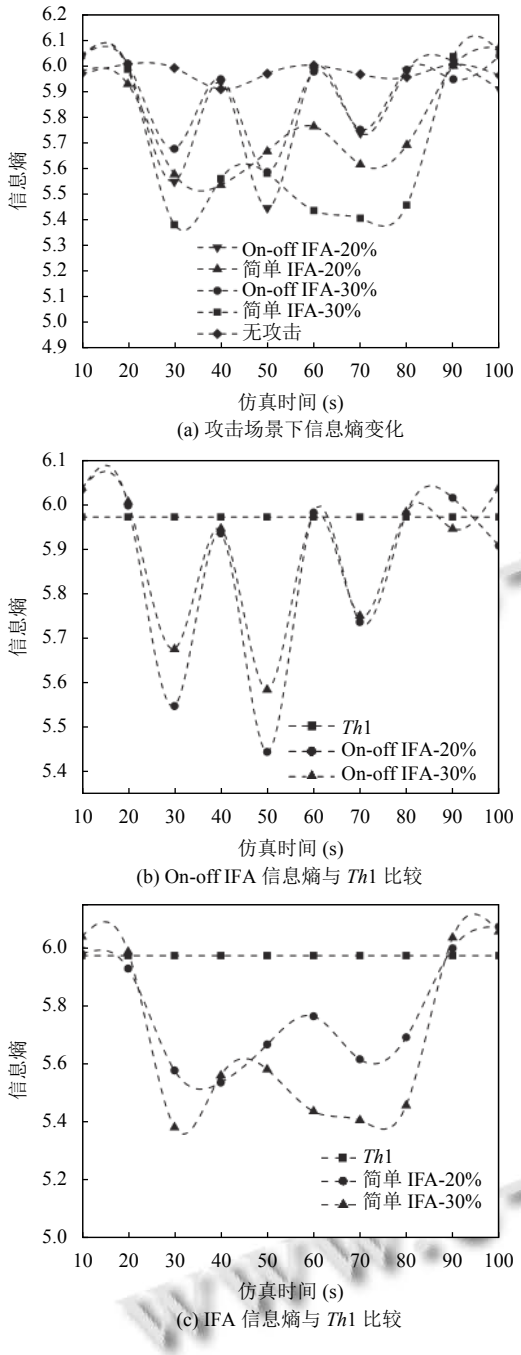
3.2 实验结果及分析

实验设置 4 组对比, 实验时间均为 100 s, 分别是: (1) on-off IFA, 恶意节点占比 20%, 攻击者的发包速率设置为 50 packets/s, 是合法节点的 5 倍, 攻击周期设置为 20 s, 攻击时间为 10 s; (2) on-off IFA, 恶意节点占比 30%, 其余设置与 (1) 相同; (3) 简单类型 IFA, 恶意节点占比 20%, 攻击者发包速率设置为 50 packets/s, 攻击时间从 20 s 开始, 80 s 结束, 持续时间为 60 s; (4) 简单类型 IFA, 恶意节点占比 30%, 其余设置与 (3) 相同.

3.2.1 信息熵评估

实验设置时间窗口大小为 10 s, 计算每个窗口内的信息熵, 实验结果如图 7 所示. $Th1$ 是经多次实验得到的经验值. 无攻击情况下, 信息熵在有限的范围内波动, 因此采用多次实验结果的均值作为阈值 $Th1$. 由于车辆节点的移动性, VNDN 中的数据来源分布具有随机性, 因此无攻击情况下的信息熵较高. 从图 6 可以看出, 4 组攻击场景下的信息熵虽然存在较大波动, 但信息熵都低于 $Th1$; 然而, 单纯依靠信息熵进行 IFA 检测是不准确的.

简单 IFA 和 on-off IFA 在攻击发生的时间窗口内, 信息熵均下降; 在攻击结束后, 信息熵均上升. 这两种攻击发生时, 网络中充斥着大量无效兴趣包, 并且均来源于攻击者, 因此信息熵下降; 攻击结束后, 网络又恢复到正常状态, 信息熵回升. 简单 IFA 在攻击期间的信息熵存在较小波动; on-off IFA 在攻击期间的信息熵存在较大波动, 这是由于攻击者具有两种攻击形态, 而形态的切换导致信息熵产生较大波动.



(a) 攻击场景下信息熵变化

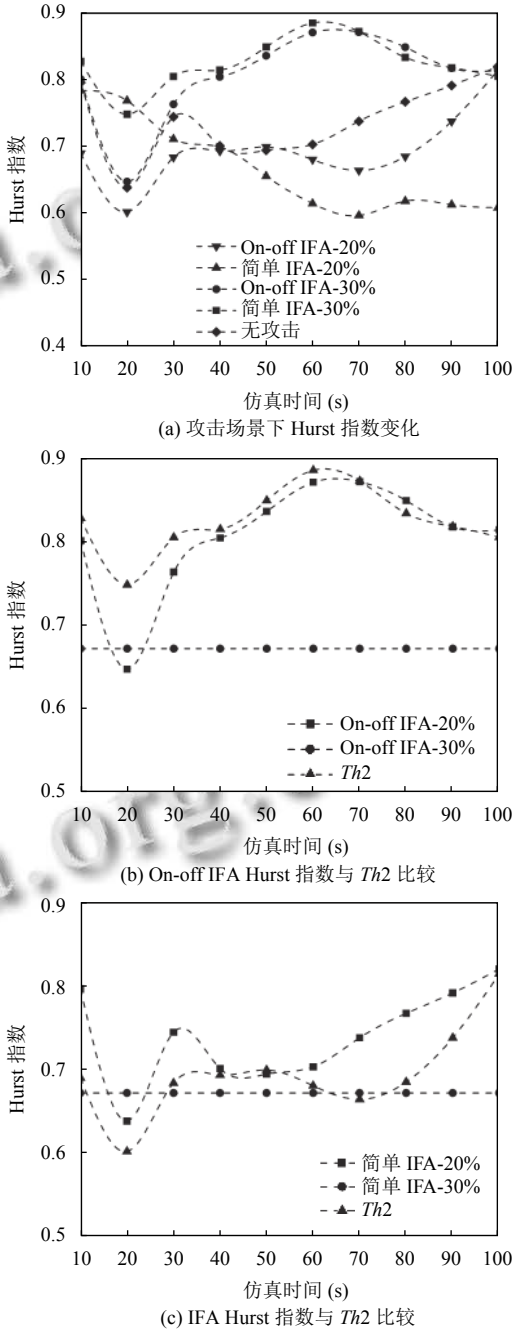
(b) On-off IFA 信息熵与 $Th1$ 比较

(c) IFA 信息熵与 $Th1$ 比较

图 7 信息熵对比图

3.2.2 Hurst 评估

实验设置时间窗口大小为 10 s, 获取时间窗口内的时间序列<t_i , $packets_i$>, 计算 Hurst 指数. 其中, t_i 指第 i 个时间子序列, $packets_i$ 指该时段内到达兴趣包的数量. 4 组实验的结果如图 8 所示, $Th2$ 是经多次实验得到的经验值. 无攻击情况下, 随着时间增长, Hurst 指数趋于稳定, 最终在某个数值附近微小波动. 将多次实验稳定值的平均值作为阈值 $Th2$. 攻击发生时, 攻击者短时间内以恒定频率发送大量兴趣包, 每个子序列内到达的兴趣包数量相似; 而无攻击场景, 每个子序列内到达的兴趣包数量具有随机性. 因此, 攻击场景下的 Hurst 指数较无攻击场景下的高. 如图 8 所示, 尽管 4 组实验的 Hurst 指数存在波动, 但绝大部分 Hurst 指数大于 $Th2$. 综上, 单独依赖 Hurst 指数判断攻击是不可靠的.



(a) 攻击场景下 Hurst 指数变化

(b) On-off IFA Hurst 指数与 $Th2$ 比较

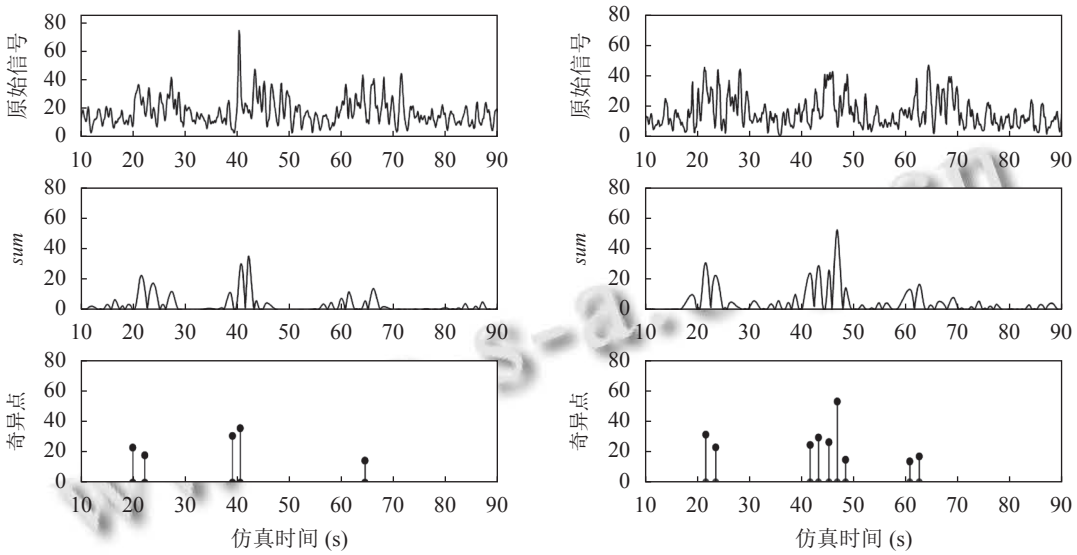
(c) IFA Hurst 指数与 $Th2$ 比较

图 8 Hurst 对比图

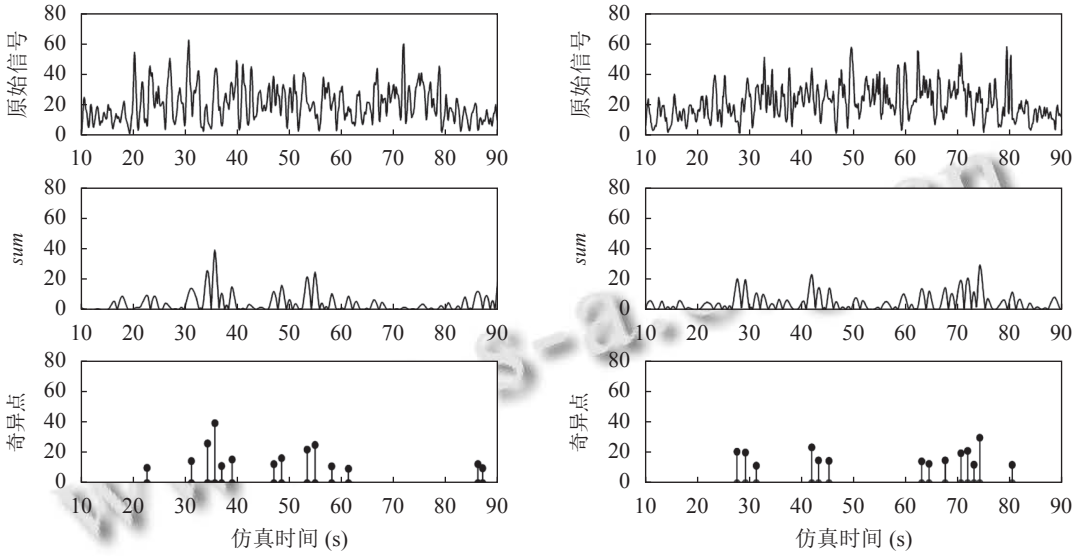
3.2.3 奇异点评估

实验通过检测奇异点的位置确定攻击发生的时

刻, 实验结果如图 9 所示. 当 IFA 发生时, 网络中的流量会产生突变, 而该突变点被称为奇异点. 图 9(a) 和图 9(b) 分别展示了恶意节点占比 20% 与 30% 时 on-off 型 IFA 的实验结果. 两组实验均设置在 20–30 s、40–50 s、60–70 s 发动攻击. 由图 9(a) 和图 9(b) 可以看出, 在上述 3 个区间内均存在奇异点. 由于网络波动, 每个区间内存在多个奇异点, 但仍可以大致判断攻击发起的时刻.



(a) On-off IFA 攻击占比 20%　　(b) On-off IFA 攻击占比 30%



(c) IFA 攻击占比 20%　　(d) IFA 攻击占比 30%

图 9　奇异点检测对比图 (纵坐标表示兴趣包数量)

图 9(c) 和图 9(d) 分别展示了恶意节点占比 20% 与 30% 时简单型 IFA 的实验结果. 两组实验设置在 20–80 s 发动攻击. 由图 9(c) 可以看出, 在 20–70 s 区间内存在多个奇异点, 而 70–80 s 区间内不存在奇异点. 由图 9(d) 可以看出, 在 20–50 s 区间及 60–80 s 区间内存在多个奇异点, 而 50–60 s 区间内不存在奇异点. 这是由于简单 IFA 在持续一段时间后, 网络达到了一个相对稳定的阶段, 因此存在检测不到流量突变的情况. 而在攻击结束后, 网络恢复正常时, 即 80–90 s 区间, 由于网络流量下降产生突变点, 这成为攻击判断的干扰项. 因此, 基于小波分析的方法存在较高的误判率.

3.2.4 检测结果评估

本文选择基于信息熵分析法、基于相似性分析法及基于小波分析法作为对比方法, 分别比较检测率、误判率和准确率. 对比实验结果如表 2 所示. 其中检测率、误判率、准确率的计算方式分别如式 (11)–式 (13) 所示:

$$检测率=\frac{检测出的攻击次数}{总攻击次数}\times 100\% \tag{11}$$

$$误判率=\frac{误判次数}{检测出的总次数}\times 100\% \tag{12}$$

$$准确率=\left(1-误判率\right)\times 100\% \tag{13}$$

表 2 实验结果 (%)

方法	攻击类型	检测率		误判率		准确率	
		20%	30%	20%	30%	20%	30%
基于信息熵分析法	On-off IFA	94.0	94.8	13.0	12.7	87.0	87.3
	简单型IFA	60.3	60.7	10.8	10.4	89.2	89.6
基于相似性分析法	On-off IFA	93.7	92.8	12.2	13.2	87.8	86.8
	简单型IFA	78.6	77.9	11.4	12.1	88.6	87.9
基于小波分析法	On-off IFA	79.3	83.5	11.7	12.4	88.3	87.6
	简单型IFA	90.4	90.2	14.2	13.8	85.8	86.2
本文方法DSFA	On-off IFA	92.1	92.4	9.7	9.3	90.3	90.7
	简单型IFA	91.8	91.5	8.9	8.6	91.1	91.4

注: 表头中的20%与30%分别表示恶意节点占比20%和恶意节点占比30%

由表 2 可以看出, 在恶意节点占比为 20% 与 30% 情况下, 检测 on-off IFA 时, 除基于小波分析法外, 基于信息熵分析法、基于相似性分析法和本文提出的 DSFA 均有较高的检测率. 在保持较高检测率的情况下, 恶意节点占比 20% 时, DSFA 的误判率只有 9.7%, 准确率达到 90.3%; 恶意节点占比 30% 时, DSFA 的误判率只有 9.3%, 准确率达到 90.7%; 均优于其他 3 种方法. 在恶意节点占比为 20% 与 30% 情况下, 检测简单 IFA 时, 基于信息熵分析法和基于相似性分析法的检测率都有所降低, 而基于小波分析法的检测率有所提升. DSFA 的检测率没有较大波动, 仍维持在 91.8% 与 91.5% 的较高水平, 同时误判率 8.9%、8.6% 和准确率 91.1%、91.4% 均优于其他 3 种方法. DSFA 面向两种类型 IFA 不同攻击占比情况均有较高的检测率, 并降低误判率, 提升攻击判断的准确性.

4 结论与展望

本文提出一种基于流量监测的 IFA 检测方法. 该方法面向两种 IFA, 分别为开关型 IFA 和简单型 IFA. 该方法首先利用 RSU 组建 RSU 网络流量监测层, 实时监测网络流量. 然后设定固定的时间窗口, 分析每个窗口内流量数据的信息熵、Hurst 指数及奇异点, 由此判断该窗口内是否存在攻击. 同时, 通过奇异点的位置, 可以推断攻击发启的时刻. 通过仿真实验, 验证了该方法在具有较高检测率时, 降低了误判率, 提升了准确率. 在未来的工作中, 将研究如何缓解攻击所带来的影响, 进一步降低攻击对网络的危害.

参考文献

1 马红桥, 杨文忠, 康鹏, 等. 命名数据网络研究综述. 计算机应用, 2022: 1–14. [doi: 10.11772/j.issn.1001-9081.2021091576]

2 Yu LJ, Ai HL, Choi DO. Countermeasures of interest flooding attack in named data networking: A survey. The International Journal of Electrical Engineering & Education, 2021. [doi: 10.1177/0020720920983518]

3 Abdullah M, Raza I, Zia T, *et al*. Interest flooding attack mitigation in a vehicular named data network. IET Intelligent Transport Systems, 2021, 15(4): 525–537. [doi: 10.1049/itr2.12042]

4 Sattar MU, Rehman RA. Interest flooding attack mitigation in named data networking based VANETs. 2019 International Conference on Frontiers of Information Technology (FIT). Islamabad: IEEE, 2019. 245–2454.

5 Benmoussa A, El Karim Tahari A, Lagaa N, *et al*. A novel congestion-aware interest flooding attacks detection mechanism in named data networking. 2019 28th International Conference on Computer Communication and Networks. Valencia: IEEE, 2019. 1–6.

6 Hou R, Han M, Chen J, *et al*. Theil-based countermeasure against interest flooding attacks for named data networks.

IEEE Network, 2019, 33(3): 116–121. [doi: 10.1109/MNET.2019.1800350]

7 侯睿, 韩敏, 陈璟, 等. 命名数据网络中基于信息熵的 Interest 洪泛攻击检测与防御. 中南民族大学学报 (自然科学版), 2019, 38(2): 273–277. [doi: 10.12130/znmdzk.20190222]

8 Zhi T, Liu Y, Wang JS, *et al*. Resist interest flooding attacks via entropy-SVM and Jensen-Shannon divergence in information-centric networking. IEEE Systems Journal, 2020, 14(2): 1776–1787. [doi: 10.1109/JSYST.2019.2939371]

9 邢光林, 陈璟, 余俊乐, 等. 命名数据网络中基于包标记的 Interest 泛洪攻击缓解研究. 中南民族大学学报 (自然科学版), 2021, 40(2): 204–209.

10 Mounika V, Sai NR, Bhavani V, *et al*. Interest flooding attack detection method in NDN networks. Proceedings of the 2nd International Conference on Smart Electronics and Communication (ICOSEC). Trichy: IEEE, 2021. 298–307.

11 Nguyen T, Mai HL, Cogranne R, *et al*. Reliable detection of interest flooding attack in real deployment of named data networking. IEEE Transactions on Information Forensics and Security, 2019, 14(9): 2470–2485. [doi: 10.1109/TIFS.2019.2899247]

12 Xin YH, Li Y, Wang W, *et al*. Detection of collusive interest flooding attacks in named data networking using wavelet analysis. 2017 IEEE Military Communications Conference (MILCOM). Baltimore: IEEE, 2017. 557–562. [doi: 10.1109/MILCOM.2017.8170763]

13 Shigeyasu T, Sonoda A. Detection and mitigation of collusive interest flooding attack on content centric networking. International Journal of Grid and Utility Computing, 2020, 11(1): 21–29. [doi: 10.1504/IJGUC.2020.103966]

14 吴志军, 张入丹, 岳猛. 一种联合检测命名数据网络中攻击的方法. 计算机研究与发展, 2021, 58(3): 569–582. [doi: 10.7544/issn1000-1239.2021.20200448]

15 张瑶. 车联网环境下基于机会网络的可信路由模型. 计算机系统应用, 2021, 30(3): 214–220. [doi: 10.15888/j.cnki.csa.007851]

16 惠飞, 唐书宇, 邢美华, 等. 基于 LTE-V 车辆密集场景的车联网资源分配算法. 计算机系统应用, 2021, 30(2): 132–139. [doi: 10.15888/j.cnki.csa.007821]

17 Lee RT, Leau YB, Park YJ, *et al*. A survey of interest flooding attack in named-data networking: Taxonomy, performance and future research challenges. IETE Technical Review, 2021: 1–19. [doi: 10.1080/02564602.2021.1957029]

18 Wang XC, Yang QW, Xie ZC, *et al*. Low-rate DoS attack detection based on WPD-EE algorithm. 2020 IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking. Exeter: IEEE, 2020. 384–391.

19 Liu L, Feng WZ, Wu ZJ, *et al*. LDDoS attack detection method based on wavelet decomposition and sliding windows. The Journal of China Universities of Posts and Telecommunications, 2020, 27(1): 51–61. [doi: 10.19682/j.cnki.1005-8885.2020.0009]

20 荣红佳, 盛虎, 闫秋婷. 基于改进 R/S 估计算法的网络流量长相关性分析. 大连交通大学学报, 2021, 42(2): 114–119. [doi: 10.13291/j.cnki.djdxac.2021.02.022]

21 李源, 谢一臻, 王永建, 等. 面向车联网泛洪攻击的流量异常检测方法. 南京理工大学学报, 2020, 44(4): 454–461. [doi: 10.14177/j.cnki.32-1397n.2020.44.04.010]

22 Ananthakrishnan S, Tahiliani MP, Tandur D, *et al*. Group based publisher-subscriber communication primitives for ndnSIM. 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). New Delhi: IEEE, 2020. 1–6.

(校对责编: 牛欣悦)