·安全技术· 文章编号:1000-3428(2017)07-0156-07 文献标志码:A 中图分类号:TP301.6

基于节点状态跳转统计分析的干扰攻击检测算法

胡 飞[1],范建华[2],魏祥麟[2],孙 钦[2]

(1. 解放军理工大学 通信工程学院,南京 210007; 2. 南京电讯技术研究所,南京 210007)

摘 要: 干扰攻击会导致节点状态跳转规律发生变化。为此,在节点状态跳转统计分析的基础上,提出一种改进的干扰检测算法。在学习阶段,通过学习无干扰和有干扰场景下的样本,获取节点各状态时间占比的干扰检测判决门限和干扰类型判决门限。在检测阶段,对节点的各状态时间占比与对应的判决门限进行比较,检测干扰攻击并判断其类型。采用加权检测置信度方法进一步提高检测正确率并降低误报率。在 NS3 上的仿真结果表明,该算法的误报率较低,能够准确检测到典型的按需和持续干扰攻击。

关键词: 无线自组织网络;干扰检测;状态时间占比;状态跳转;加权检测置信度

中文引用格式: 胡 飞,范建华,魏祥麟,等. 基于节点状态跳转统计分析的干扰攻击检测算法[J]. 计算机工程,2017,43(7):156-162.

英文引用格式: Hu Fei, Fan Jianhua, Wei Xianglin, et al. Jamming Attack Detection Algorithm Based on Statistical Analysis of Node State Transition[J]. Computer Engineering, 2017, 43(7): 156-162.

Jamming Attack Detection Algorithm Based on Statistical Analysis of Node State Transition

HU Fei[1], FAN Jianhua[2], WEI Xianglin[2], SUN Qin[2]

(1. College of Communication Engineering, PLA University of Science and Technology, Nanjing 210007, China;
2. Nanjing Telecommunication Technology Research Institute, Nanjing 210007, China)

【Abstract】 Jamming attacks may cause the change of node state transition rule. Based on the statistical analysis of node state transition, this paper puts forward an improved jamming detection method. At the learning phase, the jamming detection judgment thresholds and jamming type judgment thresholds of the proportion of node state time are extracted through learning from samples collected from jamming and jamming-free scenarios. At the detection phase, these corresponding decision thresholds are compared with the proportion of node state time to detect the jamming attacks and determine the jamming types. The method of weighted detection confidence is proposed to further improve the detection rate and reduce the false alarm rate. Simulation results on NS3 validate that the proposed algorithm can accurately detect the typical on-demand and continuous jamming attacks with low false alarm rate.

【Key words】 Ad hoc network; jamming detection; proportion of state time; state transition; weighted detection confidence

DOI: 10.3969/j.issn.1000-3428.2017.07.026

0 概述

无线自组织网络是由一组带有无线收发装置的节点组成的无线通信网络,它不依赖预设的基础设施就能实现灵活动态组网,具有临时、按需、自主等特性。当前,无线自组织网以其独有特性广泛应用在军事通信、应急通信、可穿戴设备、医疗监护、车载通信、农业生产等多个领域[1]。但无线媒介的开放性特点使得节点在通信过程中极易遭受蓄意干扰攻击。为了消除干扰攻击的影响,必须采取有效的抗干扰手段,而及时准确的干扰攻击检测则是采取抗干扰手段的必要前提。因此,干扰攻击检测是否及时准确对于维护网络性能至关重要。

干扰攻击检测是指利用观察或搜集到的节点级、链路级、网络级现象,通过数据处理及分析,采用对比报文投递率等方法,检测干扰攻击的存在以

基金项目: 国家自然科学基金"基于短距离无线通信的数据中心网络管控平面构建、调度及应用关键技术研究"(61402521);江苏省自然科学基金"面向多条无线网络的干扰部署、定位与识别关键技术研究"(20140068)。

作者简介: 胡 飞(1987—),男,硕士,主研方向为干扰攻击检测;范建华,研究员、博士;魏祥麟,工程师、博士;孙 钦,硕士。

收稿日期: 2016-12-01 **修回日期:** 2017-01-27 **E-mail:** hufei_njupt@163.com

及类型[2]。当前,从干扰攻击针对的目标、干扰攻击采取的干扰策略等角度[3],国内外研究者已经提出了多种干扰攻击检测方法,例如基于物理层信息的干扰攻击检测方法、基于链路层信息的干扰攻击检测方法、基于网络层信息的干扰攻击检测方法和基于多层信息的干扰攻击检测方法等。这些方法在设定环境中可以有效地检测出特定的干扰攻击模式。但是,现有干扰攻击检测方法普遍存在针对特定干扰模型或者依赖多个节点实施干扰攻击检测的问题。

本文针对以上问题,提出基于节点状态跳转统计分析的干扰攻击检测算法。该算法分为学习阶段和检测阶段 2 个阶段。学习阶段通过学习多种场景下的样本确定干扰检测门限和干扰类型检测门限。检测阶段依据干扰检测门限完成干扰检测并判断干扰类型。

1　相关工作

干扰攻击是一种通过占用通信信道或者破坏通信协议等方式,使其不能进行正常数据传输或转发的拒绝服务攻击[4-6]。根据干扰攻击方式的不同,可以将干扰源分为 4 种[7]:1)持续干扰源,是指持续不断发射高功率的随机无意义比特信号的干扰源。该类干扰源信号产生过程中不遵守任何 MAC 协议;2)随机干扰源,是指干扰源在睡眠模式和干扰模式之间随机切换状态的干扰源。处于睡眠状态时,干扰源关闭射频模块。处于干扰模式时,发射合法报文破坏网络正常传输;3)按需干扰源,是指在网络中有数据传输时才发起干扰攻击的干扰源。如果信道处于空闲状态,干扰源保持静默并持续侦听信道。一旦侦听到有数据开始传输,就发射有意义的报文,使得网络中的数据在接收端无法通过校验;4)欺骗干扰源,是指持续发射合法报文的干扰源。由于持续发送报文,导致网络中的其他节点始终认为信道忙,推迟报文发送甚至丢弃报文。在这 4 种干扰攻击中,以持续干扰和按需干扰最具有代表性,文中主要针对这 2 类干扰进行检测和识别。

基于物理层信息的干扰检测主要利用搜集物理层上的相关测度检测干扰攻击。基于接收信号强度的干扰检测[8]通过比较接收信号强度来检测干扰攻击:1)通过平均信号强度或者信号总能量检测干扰。如果当前接收信号强度大于无干扰时的信号强度,表明存在干扰攻击。2)利用信号强度的频谱差分检测干扰。通过比较无干扰时的信号强度频谱与干扰导致的信号强度频谱异常检测干扰。该检测方法虽然能够检测出持续干扰,但无法检测出持续干扰。基于干扰信号脉冲时长的干扰攻击检测方法[9]对比信号强度异常时长与报文中每个符号传输时长实现干扰检测并判断相应干扰类型。持续干扰引起信号强度异常时长为整个检测时长,而按需干扰引起的信号强度异常时长与破坏报文中一个符号的最小时长相当,依据以上信息可以实现干扰类型的判断。但该方法缺点在于判断信号强度异常的门限难以确定,以及检测算法有效性缺乏实验验证。文献[10]根据干扰造成的比特错误时该比特信号强度要大于无干扰时的特点实现干扰检测。该方法的缺点在于搜集无干扰时的错误比特对应的信号强度需要节点之间实现有线连接,这在无线网络通信场景中难以实现。

基于链路层信息的干扰攻击检测方法主要依据链路层上相关测度检测干扰攻击。基于报文投递率的干扰检测[8]根据报文投递率的变化来检测干扰攻击。报文投递率是指接收报文数量与发送报文数量的比值。由于网络高度拥塞的场景下报文投递率依然能够达到 78% 以上,而干扰攻击会使得报文投递率锐减。因此,如果报文投递率与拥塞场景下的值相差较大,就可以判断干扰的存在。文献[8]根据干扰源持续占用信道会导致其他节点的载波侦听时间显著增加的特点,通过设定阈值可以区分出受干扰和正常通信,以此达到检测目的。但该方法只能检测出持续干扰而无法检测出按需干扰攻击。

基于网络层信息的干扰攻击检测方法主要利用网络层相关测度检测干扰攻击。基于低功率探测的干扰检测[11]通过广播低于正常功率值的探测报文检测空闲信道评估(Clear Channel Assessment, CCA)攻击。由于干扰源提高了自身 CCA 阈值来占用更多带宽,因此不会回复低于正常信号强度的报文。接入点通过向各个节点发送低于正常功率值的探测报文,如果存在没有回复报文的节点,就表明干扰攻击的存在。文献[12]依据干扰攻击导致节点无法回复报文的特点,通过向邻居节点发送探测报文并统计回复报文数量的方法实现干扰检测。

基于多层信息的干扰攻击检测方法依据多层搜集的测度检测干扰攻击,例如一致性干扰检测[8]。该检测方法在报文投递率测度的基础上,加入节点位置和接收信号强度 2 种测度进行干扰检测。在非干扰情况下,如果 PDR 值较低,对应的信号强度应该较低,或者节点间距离应该较远。因此,在依据报文投递率初步检测后,排除接收信号强度小和节点间距离较大的误判因素,可以进一步提高检测的准确性。文献[13]提出了利用机器学习的方法搜集多种测度在干扰和无干扰时的值,确定各测度的检测

门限,从而利用干扰检测门限实现干扰检测。该方法的缺点在于算法复杂度较高,且搜集多种测度花费时间较长。

2 节点状态跳转检测

2.1 干扰攻击对节点状态跳转的影响

在采用 CSMA/CA 协议的网络中,节点状态跳转情况如图 1 所示。图中各状态说明如表 1 所示。

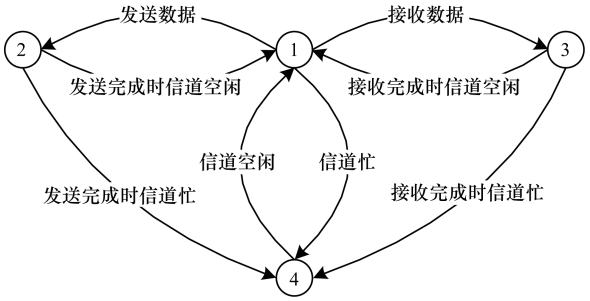

图 1 节点状态跳转

表 1 节点各状态说明

状态标号	状态名称	含义
1	IDLE	物理层处于空闲状态
2	TX	物理层在发送一个报文
3	RX	物理层在接收一个报文
4	CCA_BUSY	物理层接收到的信号功率大于 CCA 阈值

采用 802.11 协议标准时的节点状态跳转过程如下:假设节点起始状态是 IDLE,那么节点在需要发送报文时,需要跳转到状态 TX。按照协议描述,节点必须在成功竞争信道后才能发送报文,即节点在发送报文前必须侦听信道为空闲。因此,只能从状态 IDLE 跳转到状态 TX。同理,如果节点需要跳转到状态 RX 上接收报文,只能由状态 IDLE 跳转到状态 RX。而如果节点检测到信道忙,那么直接跳转到状态 CCA_BUSY。为了避免发生碰撞,在通信双方收发报文期间,通信范围内的其他节点在网络分配向量(Network Allocation Vector,NAV)时间内需要保持静默。由于 NAV 为发送节点预先估计的通信时间,与实际通信时间并不完全一致。因此,如果 NAV 大于实际通信时长,那么通信双方节点在传输完成后侦听信道为空闲,由 TX 或者 RX 跳转至 IDLE。否则,侦听信道繁忙,由 TX 或者 RX 跳转至 CCA_BUSY。在受到持续干扰攻击时,节点始终检测信道为忙,将持续处于CCA_BUSY 状态。在受到按需干扰攻击时,节点正常进行信道侦听,但发送或者接收报文时,按需干扰源会发起干扰攻击,使得通信双方在传输完成时始终侦听信道为忙,节点始终由 TX 或者 RX 跳转到 CCA_BUSY。

2.2 检测算法设计

依据干扰攻击对节点状态跳转造成的影响,提出基于节点状态跳转统计分析的干扰攻击检测算法。算法分为学习和检测 2 个阶段。

2.2.1 学习阶段

该阶段通过学习节点状态跳转样本得到干扰判决门限和干扰类型判决门限。每个样本中包含无干扰和有干扰 2 种情况。在检测时间为 T 时,样本中的数据表示为(n_k,t_k),$1\leqslant k\leqslant K$。其中,n_k表示记录的第 k 个记录数据中的节点状态;t_k表示该状态持续时间;K 表示时间 T 内搜集到的数据个数。如果节点存在 N 个状态$(s_1,s_i,\cdots,s_N)$,那么节点状态的时间占比分布表示为 $R(T,N)=(r(s_1),r(s_2),\cdots,r(s_N))$。其中,$r(s_i)$表示节点处于状态 s_i的时间检测时间 T 的百分比。状态时间占比的计算公式如下:

$$r(s_i)=\frac{\sum_{k=1}^{K}t_k\times P_k}{T},1\leqslant i\leqslant N$$

其中,$P_k=\begin{cases}1,n_k=s_i\\0,n_k\neq s_i\end{cases}$。

学习样本中包含无干扰场景和有干扰场景的节点状态跳转数据。以节点状态 s_i为例,在学习 m 组无干扰场景下的样本后,s_i在无干扰场景下的时间占比集合表示为 $\varphi_n(s_i,m)=\{r_n^1(s_i),r_n^2(s_i),\cdots,r_n^m(s_i)\}$。其中,$r_n^j(s_i)$,$1\leqslant j\leqslant m$ 表示第 j 组无干扰学习样本对应的 s_i的时间占比 $r(s_i)$。同样,得到 s_i在持续干扰场景下的时间占比集合 $\varphi_c(s_i,m)=\{r_c^1(s_i),r_c^2(s_i),\cdots,r_c^m(s_i)\}$以及按需干扰场景下的时间占比集合 $\varphi_r(s_i,m)=\{r_r^1(s_i),r_r^2(s_i),\cdots,r_r^m(s_i)\}$。根据 3 类集合的位置关系选取干扰检测判决门限和干扰类型判决门限。考虑到 $\varphi_c(s_i,m)$和 $\varphi_r(s_i,m)$可能处在 $\varphi_n(s_i,m)$的同侧或者两侧,这里以 $\varphi_c(s_i,m)$和 $\varphi_r(s_i,m)$在 $\varphi_n(s_i,m)$右侧的情形举例说明:

1)$\varphi_c(s_i,m)$,$\varphi_r(s_i,m)$和 $\varphi_n(s_i,m)$均不重叠。如图 2 所示,可以在 $\varphi_n(s_i,m)$和其相邻 $\varphi_r(s_i,m)$之间选取 s_i的干扰判决门限 α_i。若 $\varphi_n(s_i,m)$和其相邻 $\varphi_r(s_i,m)$的距离为 b,α_i 与 $\varphi_n(s_i,m)$的距离为 a,那么将$\frac{a}{b}$记为干扰判决门限偏移量 λ。此时选取的干扰判决门限可以检测出持续干扰和按需干扰。同样,可以在 $\varphi_c(s_i,m)$和 $\varphi_r(s_i,m)$之间 s_i的干扰判决门限干扰类型判决门限 β_i。将$\frac{c}{d}$记为干扰类型判决门限偏移量 ε。

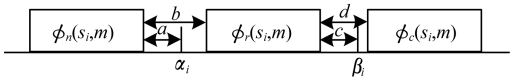

图 2　$\varphi_c(s_i,m)$,$\varphi_r(s_i,m)$和 $\varphi_n(s_i,m)$三者均不重叠的情形

2)$\varphi_c(s_i,m)$,$\varphi_r(s_i,m)$两者不重叠但其中有一个与 $\varphi_n(s_i,m)$重叠。如图 3 所示,$\varphi_r(s_i,m)$与 $\varphi_n(s_i,m)$发生重叠,可以在 $\varphi_n(s_i,m)$和 $\varphi_c(s_i,m)$之间选取 s_i的干扰判决门限 α_i。此时选取的干扰检测判决门限只能检测出持续干扰。

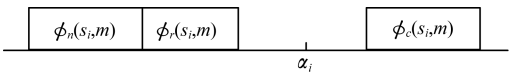

图 3　$\varphi_r(s_i,m)$与 $\varphi_n(s_i,m)$重叠的情形

3)$\varphi_c(s_i,m)$,$\varphi_r(s_i,m)$两者重叠但不与 $\varphi_n(s_i,m)$重叠。如图 4 所示,可以在 $\varphi_n(s_i,m)$和 $\varphi_r(s_i,m)$之间选取 s_i的干扰检测判决门限。此时选取的干扰检测判决门限可以检测出持续干扰和按需干扰,但由于 $\varphi_r(s_i,m)$和 $\varphi_c(s_i,m)$重叠,因此无法选取干扰类型判决门限。

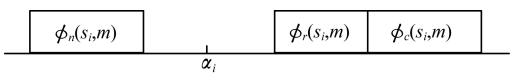

图 4　$\varphi_c(s_i,m)$,$\varphi_r(s_i,m)$重叠但不与 $\varphi_n(s_i,m)$重叠的情形

4)$\varphi_c(s_i,m)$与 $\varphi_r(s_i,m)$重叠且均与 $\varphi_n(s_i,m)$重叠,如图 5 所示。那么无法选取干扰判决门限,此时不存在干扰判决门限和干扰类型判决门限。

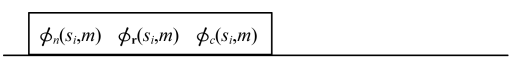

图 5　$\varphi_c(s_i,m)$,$\varphi_r(s_i,m)$和 $\varphi_n(s_i,m)$三者重叠的情形

这样,就得到了节点 N 个状态的干扰检测门限 $\zeta(T,N)=(\alpha_1,\alpha_2,\cdots,\alpha_N)$以及干扰类型检测门限 $\sigma(T,N)=(\beta_1,\beta_2,\cdots,\beta_N)$。

2.2.2　检测阶段

计算待检测数据时间 T 内的节点状态时间占比记为 $R'(T,N)=(r'(s_1),r'(s_2),\cdots,r'(s_N))$。以图 6所示的判决门限为例,每个状态依据所对应的判决门限 α_i 和 β_i 所划分出的区域判断干扰是否存在并识别干扰类型。接下来,统计各状态的判决结果,计算干扰置信度。以检测干扰是否存在为例,具体说明置信度的计算方法。如果某个状态的判决结果为存在干扰,那么干扰检测置信度就加 1。否则,干扰置信度不变。而如果不存在干扰检测判决门限,那么干扰检测置信度同样保持不变。统计完所有状态干扰检测判决结果后,依据干扰检测置信度是否超过置信度门限 η,判断是否存在干扰。假设节点有3 个状态 s_1,s_2,s_3,其中 s_1,s_2对应的干扰判决门限 α_1,α_2 存在,而 s_3的干扰判决门限 α_3 不存在。状态 s_1 判决结果为存在干扰,状态 s_2判决结果为不存在干扰,状态 s_3不存在干扰判决门限,因此,得到的干扰检测置信度为 1。干扰类型检测同样依此方法进行。

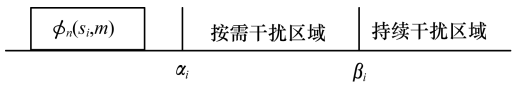

图 6　干扰检测区域划分

2.3　检测算法描述

基于节点状态跳转的干扰攻击检测算法的伪代码如下。

算法　基于节点状态跳转的干扰攻击检测算法

输入　学习样本,待检测的状态跳转数据,检测时间 T

输出　*Jamming_Type*(−1 表示不存在干扰,0 表示存在干扰但无法判断类型,1 表示持续干扰,2 表示按需干扰)

1. 根据学习样本,得到节点 N 个状态的 $\varphi_n(s_i,m)$,$\varphi_c(s_i,m)$和 $\varphi_r(s_i,m)$($1\leqslant i\leqslant N, i\in\mathbb{N}$)
2. for　i = 1:N (N 为节点状态的数量)
3. 　　if　$\varphi_n(s_i,m)\cap\varphi_c(s_i,m)=\varnothing$
4. 　　持续干扰判决门限 α_c^i = 距离 $\varphi_n(s_i,m)$偏移量为 λ 处的值
5. 　　else
6. 　　α_c^i 不存在
7. 　　end if
8. 　　if　$\varphi_n(s_i,m)\cap\varphi_r(s_i,m)=\varnothing$
9. 　　按需干扰判决门限 α_r^i = 距离 $\varphi_n(s_i,m)$偏移量为 λ 处的值
10. 　　else
11. 　　α_r^i 不存在
12. 　　end if
13. 　　if　α_c^i 和 α_r^i 都存在
14. 　　if α_c^i 和 α_r^i 在 $\varphi_n(s_i,m)$的同一侧
15. $\alpha_i=\alpha_c^i$ 和 α_r^i 中靠近 $\varphi_n(s_i,m)$的值
16. 　　if　$\varphi_c(s_i,m)\cap\varphi_r(s_i,m)=\varnothing$
17. 　干扰类型判决门限 β_i = 距离 $\varphi_r(s_i,m)$偏移量为 ε 处的值
18. else
19. 　β_i 不存在
20. end if
21. 　　else
22. $\alpha_i=(\alpha_c^i,\alpha_r^i)$,$\beta_i=(\alpha_c^i,\alpha_r^i)$
23. 　　end if
24. 　　else if　α_c^i 和 α_r^i 有一个不存在
25. 　　$\alpha_i=\alpha_c^i$ 和 α_r^i 中存在的值
26. 　　β_i 不存在
27. 　　else
28. 　　α_i 不存在
29. 　　β_i 不存在
30. 　　end if
31. 　end for

```
32.  for  k = 1:⌊待检测样本总时长/T?
33.       计算 R′(T,N) = (r′(s_1),r′(s_2),…,r′(s_N))
34.       vote = 0
35.     for  i = 1 :N
36.           if r′(s_i)与 φ_n(s_i,m)位于 α_i 的两侧
37. vote + +
38.       end for
39.       if  vote > η
40.           for  i = 1 :N
41.  if β_i 存在
42.     if r′(s_i)与 φ_c(s_i,m)在 β_i 的同一侧
43.        Jamming_Type(k) = 1
44.     else
45.        Jamming_Type(k) = 2
46.     end if
47.  else
48.     Jamming_Type(k) = 0
49.  end if
50.           end for
51.       else
52.           Jamming_Type(k) = -1
53.       end if
54.  end for
55.  return Jamming_Type
```

步骤 2 根据学习样本得到各状态在 3 类时间占比的集合,选取每个状态的干扰检测判决门限和干扰类型判决门限;步骤 3 ~ 步骤 7 判断持续干扰和无干扰时间占比集合之间的干扰检测门限;步骤 8 ~ 步骤12 判断按需干扰和无干扰时间占比集合之间的干扰检测门限;步骤 13 ~ 步骤 30 判断是否存在干扰类型门限;步骤 32 表示每隔时间 T 执行一次干扰检测;步骤 33 计算第 k 次干扰检测时的状态时间占比;步骤 34 ~ 步骤 38 计算干扰检测置信度,步骤 39 ~ 步骤 53 给出第 k 次检测结果;步骤 55 输出检测结果。

3 算法评估

3.1 场景设定

本文采用 NS3 仿真软件[14]搭建了典型无线自组织网络环境。网络部署在 400 m × 400 m 的区域内,25 个节点均匀分布在 100 m × 100 m 的网络栅格中,干扰源的坐标为(90,90)。通信节点和干扰源的位置分布如图 7 所示,仿真设置的主要参数如表 2 所示。实验中节点采用固定位置模型(节点位置固定),路由协议分为优化链路状态路由协议(Optimized Link State Routing,OLSR)[15]、无线自组网按需距离向量路由协议(Ad hoc On-demand Distance Vector routing,AODV)[16]和目的节点序列距离矢量协议(Destination-Sequenced Distance-Vector routing,DSDV)[17]3 种典型路由。

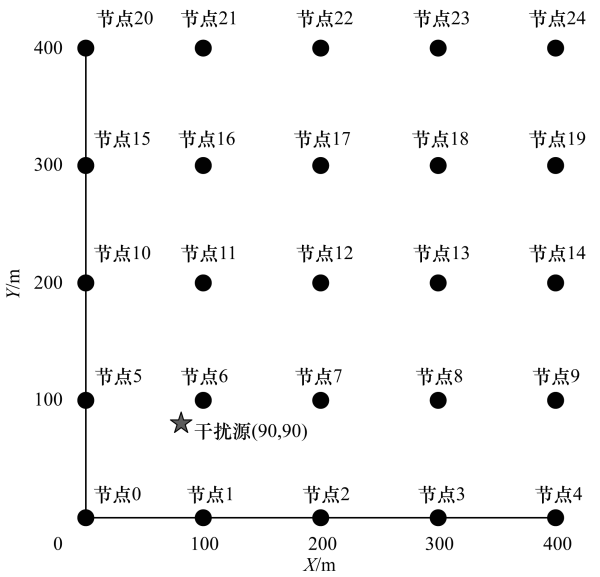

图 7 节点位置分布

表 2 仿真实验参数

参数	默认值	参数	默认值
节点数量	25	干扰源数量	1
节点发射功率/dBm	16	干扰源功率/dBm	32
节点发射增益/dB	1	干扰源发射增益/dB	1
相邻节点间距离/m	100	时隙大小/s	0.05
报文大小/Byte	1 000	仿真时隙数量	2 000

假设进行 w 次检测,其中干扰真实存在的次数 q 次,而正确检测存在干扰的次数为 p 次。误报存在干扰的次数为 e 次。那么检测正确率(True Positive Rate,TPR)表示正确检测干扰的次数与干扰存在次数的比值 p/q。误报率(False Positive Rate,FPR)表示误报干扰存在的次数 e 与干扰不存在的次数($w-q$)的比值 $e/(w-q)$。

3.2 实验结果分析

为验证干扰检测算法的有效性,在 OLSR 路由协议场景下,检测时间设置为 10 s,分别选取干扰区域内节点(节点 6)和干扰区域外节点(节点 18)运行干扰检测算法,得到的干扰检测结果分别如图 8、图 9所示。虚线表示节点受到干扰的真实情况,在 65 s ~ 165 s 期间发起持续干扰,265 s ~ 365 s 期间发起持续干扰,其余时间不存在干扰。实线中的星号表示每次得到的检测结果。节点 6 和节点 18 从 15 s 开始每隔 10 s 进行一次干扰检测,检测结果用星号表示。检测类型 1 ~ 检测类型 4 分别表示无干扰、存在干扰、持续干扰和按需干扰。由图 8 可知,干扰区域内节点能够在干扰发起时间段内准确检测干扰,并且准确识别干扰类型。由图 9 可知,干扰区域外

节点在整个检测阶段都没有检测到干扰。

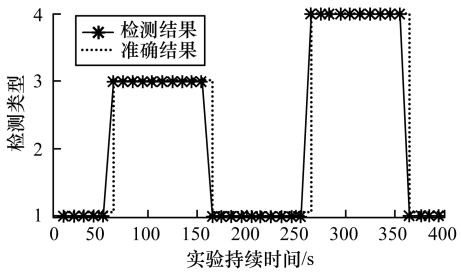

图 8　节点 6 干扰检测结果

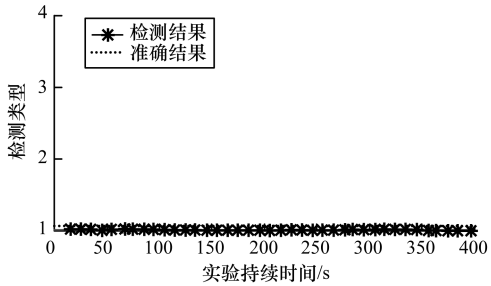

图 9　节点 18 干扰检测结果

判决门限偏移量决定干扰判决门限偏向无干扰区域还是受干扰区域,进而影响到每个状态干扰判决的结果。如图 10 所示,在保持 TPR 为 1 的情况下,随着判决门限偏移量的增加 FPR 逐渐降低。由于增加判决门限偏移量,使得干扰判决门限距离无干扰区域的距离增加,这样增加了无干扰的状态时间占比落在无干扰区域的概率,使得误报率有所降低。

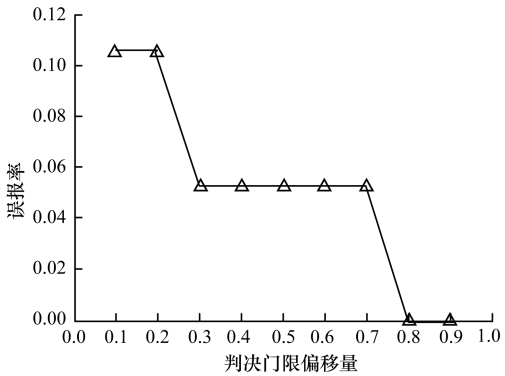

图 10　判决门限偏移量对检测准确性的影响

同样,增加检测置信度门限使得判断存在干扰的条件更加严格。以干扰判决门限为 0.5 为例,提高检测置信度门限对 TPR 和 FPR 的影响如图 11 所示。在检测置信度门限增加到 2 时,能够在 TPR 不变的同时降低 FPR,但继续增加检测置信度门限会导致 TPR 急剧下降。

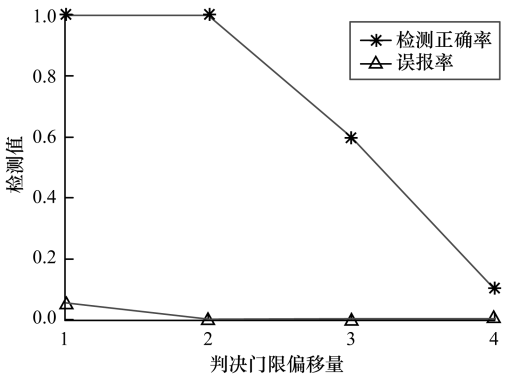

图 11　检测置信度门限对检测效果的影响

由图 11 看出,通过增加检测置信度门限可以在一定程度上降低 FPR,但是在降低 FPR 的同时无法获取满意的 TPR。为此,考察了干扰攻击对具体各状态时间占比的影响,并依据影响程度设定各状态的权值,提高检测置信度的可靠性。根据干扰攻击造成 TX 状态的时间占比明显变化,增加计算检测置信度时 TX 的权值,得到如图 12 所示的检测结果,在增加检测置信度门限时,降低 FPR 的同时依然保持较高的 TPR。例如,在检测存在干扰的样本时,为了提高检测正确率而将检测置信度门限设为 3。即使将偏移量设为最大值,节点的 4 种状态 CCA_BUSY,IDLE,TX 和 RX 中只有 CCA_BUSY 和 TX 判决存在干扰。如果各状态的检测置信度权值均为 1,那么检测置信度为 2,小于门限 3,判断为不存在干扰,导致漏报情况发生。而如果提高 TX 的检测置信度权值为 3,那么计算检测置信度为 4,判断存在干扰。这样,实现了降低误报率的同时提高检测正确率的目的。

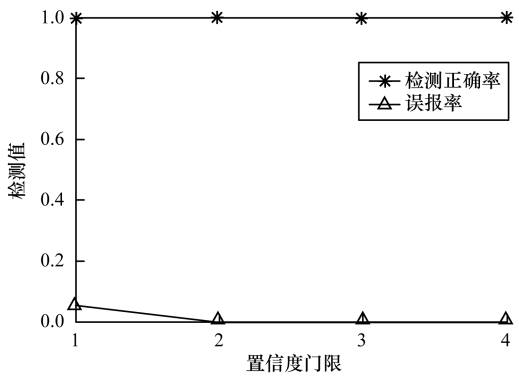

图 12　加权检测置信度门限对检测效果的影响

此外,还验证了该算法在 AODV 和 DSDV 两种场景下的检测效果。检测结果如表 3 所示,检测正确率都为 1,采用加权检测置信度的方法可以获取较低的误报率。

表 3 干扰判决门限偏移量为 0.5 时的误报率

检测置信度门限	AODV 场景	DSDV 场景
1	0.736 8	0.157 9
2	0.631 6	0.157 9
3	0.421 1	0.157 9
4	0.052 6	0.157 9

4 结束语

本文提出了基于节点状态跳转统计分析的干扰攻击检测方法。该方法根据干扰攻击造成节点状态跳转规律发生变化的观察结论,依据无干扰和有干扰环境下节点状态时间占比不一致的原则,从有干扰和无干扰场景下的样本中获取各状态的干扰检测判决门限和干扰类型判决门限,并通过设置干扰置信度的方式检测干扰是否存在。在此基础上,根据干扰对节点状态影响程度大小设定不同的干扰置信度权值,提高了干扰检测正确率。在仿真实验中对检测算法的有效性进行了论证,并讨论了干扰判决门限偏移量和干扰置信度门限对检测结果的影响。实验结果显示,通过增加干扰判决门限偏移量和干扰置信度门限可以降低误报率,但会导致检测正确率的下降。在增加与干扰攻击关联紧密的状态干扰置信度权值后,检测正确率得到了显著提升。下一步工作将就如何选取更具代表性的学习样本对学习算法进行优化。

参考文献

[1] 孙言强,王晓东,周兴铭. 无线网络中的干扰攻击[J]. 软件学报,2012,34(5):1207-1221.

[2] 王棋萍,魏祥麟,范建华,等. 基于接收干扰信号强度估计的干扰源定位算法[J]. 军事通信技术,2016(2):28-32.

[3] 赵 泽,尚鹏飞,陈海明,等. 无线传感器网络干扰分类识别机制的研究[J]. 通信学报,2013,34(10):28-36.

[4] 向亦宏,朱燕民. 无线传感器网络中高效建立干扰模型的研究[J]. 计算机工程,2014,40(8):1-5.

[5] Pelechrinis K, Iliofotou M, Krisshnamurthy S V. Denial of Service Attacks in Wireless Networks: The Case of Jammer [J]. IEEE Communications Surveys and Tutorials,2011,13(2):245-257.

[6] Wei Xianglin, Wang Qiping, Wang Tongxiang, et al. Jammer Localization in Multi-hop Wireless Network: A Comprehensive Survey [J]. IEEE Communications Surveys & Tutorials,2016,99:1-37.

[7] Vadlamani S, Eksioglu B, Medal H, et al. Jamming Attacks on Wireless Networks: A Taxonomic Survey[J]. International Journal of Production Economics,2016,172:76-94.

[8] Xu Wenyuan, Ma Ke, Trappe W, et al. Jamming Sensor Networks: Attack and Defense Strategies [J]. IEEE Network,2006,20(3):41-47.

[9] Sufyan N, Saqib N A. Detection of Jamming Attacks in 802.11b Wireless Networks[J]. EURASIP Journal on Wireless Communications and Networking, 2013, 208:1-18.

[10] Strasser M, Danev B, Čapkun S. Detection of Reactive Jamming in Sensor Networks[J]. ACM Transactions on Sensor Networks,2010,7(2):1-29.

[11] Pelechrinis K, Yan Guanhua, Eidenbenz S, et al. Detecting Selfish Exploitation of Carrier Sensing in 802.11 Networks[C]//Proceedings of INFOCOM'09. Washington D.C., USA: IEEE Press,2009:657-665.

[12] Liu Donggang, Raymer J, Fox A. Efficient and Timely Jamming Detection in Wireless Sensor Networks[C]// Proceedings of the 9th International Conference on Mobile Ad Hoc and Sensor Systems. Washington D.C., USA: IEEE Press,2012:335-343.

[13] Puñal O, Akta I, Schnelke C J, et al. Machine Learning-based Jamming Detection for IEEE 802.11: Design and Experimental Evaluation[C]//Proceedings of the 15th International Symposium on World of Wireless, Mobile and Multimedia Network. Washington D.C., USA: IEEE Press,2014:1-10.

[14] 马春光,姚建盛. NS-3 网络模拟器基础与应用[M]. 北京:人民邮电出版社,2014.

[15] Clausen T, Jacquet P. Optimized Link State Routing Protocol (OLSR) [J]. Manet Working Group, 2003, 527(2):1-4.

[16] Ad M, Perkins C E, Das S R. Ad hoc On-demand Distance Vector(AODV) Routing[EB/OL]. (2000-06-18). https://tools.ietf.org/pdf/rfc3561.pdf.

[17] Perkins C E. Highly Dynamic Destination-sequenced Distance-Vector Routing(DSDV) for Mobile Computers[J]. ACM SIGCOMM Computer Communication Review, 1994, 24(4):234-244.

编辑 顾逸斐