软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(5):1207−1221 [doi: 10.3724/SP.J.1001.2012.04059]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

无线网络中的干扰攻击*

孙言强+, 王晓东, 周兴铭

(国防科学技术大学 并行与分布处理国防科技重点实验室,湖南 长沙 410073)

Jamming Attacks in Wireless Network

SUN Yan-Qiang+, WANG Xiao-Dong, ZHOU Xing-Ming

(National Key Laboratory for Parallel and Distributed Processing, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: E-mail: yq_sun@nudt.edu.cn, http://www.nudt.edu.cn

Sun YQ, Wang XD, Zhou XM. Jamming attacks in wireless network. *Journal of Software*, 2012,23(5): 1207−1221. http://www.jos.org.cn/1000-9825/4059.htm

Abstract: The broadcast nature of wireless network with sharing medium makes it particularly vulnerable to the jamming style of the denial of service attack, which is a great threat to network performance and security. In this paper, the state-of-the-art jamming metrics and jamming models are first analyzed, and the recent literatures on jamming attack are surveyed in detail in terms of jamming detection, defense and jammer localization. Finally, the possible future trends and key points about this issue are solved.

Key words: wireless network; jamming attack; metric; model; detection; defense; localization

摘 要: 在无线网络中,媒介的广播、共享特性使其易于受到干扰性质的拒绝服务攻击,严重影响着网络的性能和安全.分析了当前存在的干扰攻击测度标准和攻击模型;从干扰攻击的检测、防御以及干扰源定位 3 个方面对当前具有代表性的研究工作进行了详细的分析和总结.最后给出未来可能的研究方向和研究重点.

关键词: 无线网络;干扰攻击;度量;模型;检测;防御;定位

中图法分类号: TP393 **文献标识码**: A

在无线网络中,媒介信道的开放广播特性使得节点间的数据转发容易受到噪音或者干扰的影响[1].特别地,有意地进行干扰被称为干扰攻击(jamming attack 或者 interference attack),攻击节点被称为 Jammer[2].这种攻击只需通过被动侦听以获取当前网络节点的通信频段,就可以迅速地发动攻击,简单、有效.为了应对这种类型的拒绝服务攻击,各种技术和策略相继出现.传统的方法是使用复杂的物理层技术,如在军事领域中采用的直接序列扩频(direct sequence spread spectrum,简称 DSSS)[3]和跳频序列扩频(frequency hopping spread spectrum,简称 FHSS)[4].但在实际应用中,考虑到基于 802.11 的无线局域网,自组织网络以及基于 802.15.4 的无线分布式传感器网络在频宽、能耗以及计算能力方面的受限性[5−7],设计复杂的物理层技术对于这种类型的网络并不适合.针对此现状,各种基于链路层以及链路层以上的的干扰攻击检测、防御、定位以及攻防博弈策略被陆续提出来.干扰攻击问题的严重性和重要性,引起了学术界的广泛重视.当前,在无线网络干扰攻击方面比较有影响力的研究小组有:在 ETH 由 Capkun 教授负责的系统安全小组[8]、在美国史蒂文森学院由 Chen 教授负责的数据分析

* 基金项目: 国家自然科学基金(61070203); 国家重点基础研究发展计划(973)(2006CB303000)
收稿时间: 2011-01-16; 修改时间: 2011-04-02; 定稿时间: 2011-05-25

与信息安全小组[9]以及南卡罗琳娜州大学的 Xu 教授负责的 ARENA 小组[10]等.

本文详细分析了当前无线网络中干扰攻击的研究现状,从干扰攻击的度量标准、干扰模型、检测机制、防御策略、定位算法等几个方面分别进行了总结和归纳,并结合我们自己的研究工作,展望未来值得研究的主要方向.

1 干扰攻击研究概述

干扰攻击是一种通过占用网络节点通信信道,使其不能进行正常数据转发的拒绝服务攻击[2],攻击的发起者称之为干扰源(jammer).图 1 展示了无线自组织网络或传感器网络中典型的干扰攻击场景,干扰攻击将网络分为干扰区域(jammed region)和非干扰区域,干扰区域内的节点(jammed node)由于受干扰影响,无法与外部节点通信,从而使得该区域形成通信“空洞”,对网络的转发、路由等性能以及安全都可以造成严重影响.

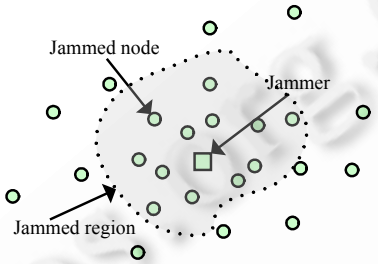


Fig.1 A scenario of jamming attack

图 1 干扰攻击实例

当前,干扰攻击的研究主要集中在 4 个方面,即干扰攻击模型、攻击检测、攻击防御和干扰源定位.图 2 给出了干扰攻击的主要研究内容框架.本文遵循该框架,从 4 个方面详细地介绍了当前干扰攻击的主要进展,并对主要内容进行了分析和归纳.

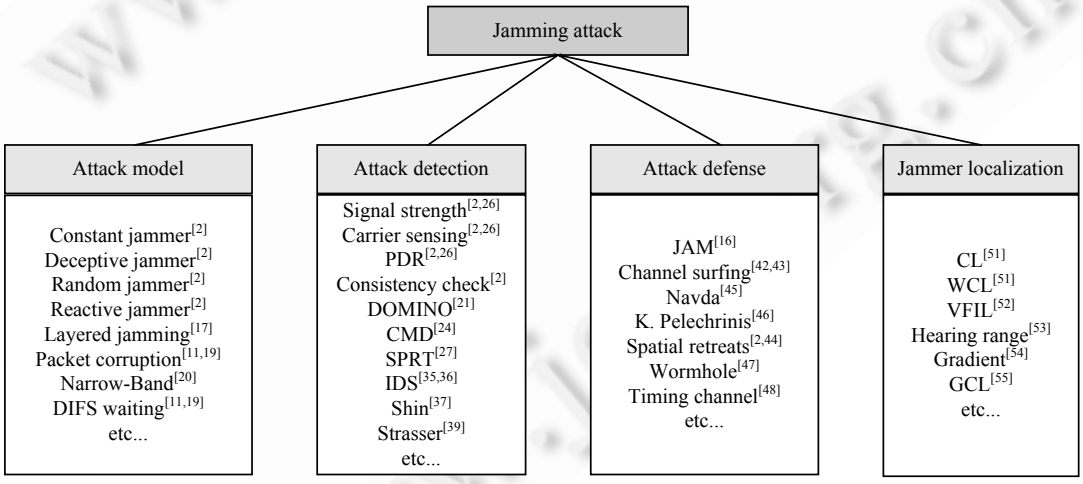


Fig.2 Framework for studying jamming attack

图 2 干扰攻击研究内容框架

从上述研究内容框架可以看出,当前,针对干扰攻击的研究主要分为两个方面,即“攻”和“防”.“攻”主要体现为各种攻击策略和攻击模型的提出;而“防”则分为不同的层次,包括了干扰攻击的检测、防御以及干扰源的定位等.另一方面,“攻”和“防”的研究思路又存在一定的依存关系,即,针对不同的攻击手段和策略,提出不同的防御

机制和方法;而“防”的巩固性又进一步增强了攻击者改进攻击手段或攻击模型的动机.因此,干扰攻击的研究在“攻”和“防”的不断博弈中前行.因此,本文从“攻”和“防”两个方面阐述当前的最新研究现状,分析当前研究已有的研究成果和仍存在的问题,为今后的研究提供一定的借鉴作用.

2 测度标准及干扰模型

2.1 测度标准

测度标准主要指干扰攻击的有效性度量方法,典型的测度标准包括能量有效性、检测成功率、DoS(denial of service)以及针对物理层技术(FHSS,DSSS 及 CDMA 等)的对抗能力[11].从攻击者的角度考虑,一次理想的干扰攻击过程应当具备较低的能耗、较低的被检测成功率、较强的 DoS 攻击性以及抗物理层防御技术等.根据恶意节点或者攻击者的目标不同,选择不同的有效性标准是至关重要的.如在传感器网络中,攻击者可能为一般的传感节点,能量受到限制,则在发起干扰攻击时就需要将能耗放在重要的位置加以考虑.

为了在不同程度上满足以上提到的干扰攻击的有效性标准,需要对干扰攻击的度量属性进行量化,以准确刻画攻击者的行为.为了便于描述,定义 T_x 为发送节点,R_x 为接收节点.Xu 等人[2]给出了两种被广泛为采用的度量属性.

- 报文发送率(packet send ratio,简称 PSR)

报文发送率是指,在 MAC 层,节点 T_x 有 n 个报文需要发送,但由于受到干扰攻击的影响,最终只有 m 个报文被成功发送,则 PSR 为

$$PSR=\frac{m}{n} \tag{1}$$

PSR 的适用对象主要是采用了载波侦听(carrier sensing)策略的发送者 T_x.由于采用了载波侦听,干扰信号使得传输媒介一直处于忙碌状态,导致 T_x 的传输队列迅速填满.在这种情况下,T_x 需要发送的报文数不变,而成功发送报文数在一定时间内减少.即 PSR 值越小,则表示干扰效果越好.

- 报文接收率(packet delivery ratio,简称 PDR)

报文接收率是指,接收节点 R_x 收到从 T_x 传送过来的 m 个报文,但由于干扰信号的影响,只有 p 个报文通过了循环冗余码(cyclic redundancy codes,简称 CRC)校验.与 PSR 不同的是,PDR 代表了干扰攻击针对接收节点的干扰效果.

$$PDR=\frac{p}{m} \tag{2}$$

以上两种简单的度量属性主要在 MAC 层实现,另外一种适用于物理层干扰攻击的较复杂的度量方法是测量干扰信号比率[12,13]:

- 干扰信号比率(jamming to signal ratio,简称 JSR)

其定义如公式(3)所示:

$$JSR=\frac{P_jG_{jr}G_{rj}R_{tr}^2L_rB_r}{P_tG_{tr}G_{rt}R_{jr}^2L_jB_j} \tag{3}$$

其中,j 代表干扰源,r 代表接收节点,t 是发送节点,P_x 表示节点 x 的传输功率,G_{xy} 表示从节点 x 到 y 的天线增益,R_{xy} 表示节点 x 与 y 之间的距离,L_r 表示通信链路的信号损失,L_j 表示干扰信号损失,而 B_x 表示节点 x 的带宽.由公式(3)可以看出,JSR 值越大,表明干扰效果越好.因此,从减少干扰影响的角度分析,增大收发节点之间的信噪比,如缩短收发节点之间的距离、增大发送节点的功率等,都可以在一定程度上减少干扰攻击的影响.

另外,还有针对网络连通性的度量属性[13]等.传统的无线网络性能属性也可以作为干扰攻击的性能指标,如存在干扰攻击时网络吞吐量的变化等.

2.2 干扰攻击模型

当前,针对无线网络的干扰攻击,根据攻击者的能力或智能性,可分为基本攻击模型和智能攻击模型两种.

2.2.1 基本攻击模型

恶意节点为了干扰正常节点之间的通信,可以采取各种各样的策略.当前,研究工作主要基于两类具有代表性的基本的干扰攻击模型,这两类攻击模型已被证明可以有效地破坏无线网络的正常数据传输[2,14−16].

(1) 主动性干扰攻击

这一类攻击方式不考虑网络的信道状况,主要有:

- 持续性干扰源(constant jammer)[2]

持续性干扰源,顾名思义,即不间断地发射无线信号.这种攻击方式可以通过射频发射器持续发送信号实现(physical layer),或者通过网络中一般的节点在不遵循任何 MAC 层协议的情况下向信道发射随机无意义报文来实现(MAC layer)

- 欺骗性干扰源(deceptive jammer)[2]

这种攻击者具有欺骗性,不再发射随机无意义字节,而是持续地向网络信道中传送正常的数据包.这种攻击方式的好处在于,网络中的节点误以为是正常的数据包在传送,从而一直保持静默或者接收状态.

- 随机性干扰源(random jammer)[2]

不同于前两种主动性攻击方式,随机性干扰源在睡眠状态和干扰状态之间随机切换,比如,在对网络攻击 $T1$ 时间后关掉自己的射频模块,进入睡眠状态;在 $T2$ 时间之后,又重新发起攻击.$T1$ 和 $T2$ 可以随机设定也可以是固定的值.

(2) 按需干扰攻击(reactive jammer)[2]

以上提到的 3 种攻击方式,在具备主动性的同时,也由于其持续的“在线”特性,使其相对容易被检测到.而按需干扰攻击,是在信道空闲时保持静默,而一旦感知到信道忙碌则开始发起攻击.这种类型的攻击特别针对于报文接收方.

Xu 等人利用加州大学伯克利分校的 Mica 系列传感器节点实现了上述 4 种攻击模型[2].这几种攻击模型是基本的实现方式,恶意攻击节点可能通过将不同的攻击方式进行结合,实现更有效的攻击效果,比如将欺骗性干扰与按需性干扰相结合,在侦听到信道忙碌时,向网络信道传送正常数据包,一般的普通节点很难将其与网络拥塞区别开来,从而使攻击者取得更好的隐蔽效果.

2.2.2 智能型攻击模型

基本攻击模型的攻击策略主要适用于物理层和 MAC 层,方法简单且效果明显,但也存在能耗较大、易被检测等问题.因此,一些智能型攻击模型被相继提出来.这些模型从网络较高层(MAC 层及以上)考虑,如在无线自组织网络中的路由层,攻击者可以发送一些混乱的无意义信息,或者破坏正常的路由控制报文.这些智能型攻击模型以最大化攻击收益、有目的性选择攻击目标和减少被检测概率为主要目的.当前,主要的智能型攻击有:

(1) 跨层干扰攻击(layered jamming)

Brown 等人[17]提出了一种针对加密了的无线网络通信的跨层干扰攻击方法,该方法涉及到应用层、传输层和链路层这 3 个协议栈,每一层向其上层提供相关信息,且每一层包含两个模块:感知模块和干扰模块.主要的思想是,在链路层,感知模块侦听信道状况并记录报文传输开始时间和传输间隔,而干扰模块负责发起攻击.传输层的感知模块从链路层读取记录的信息,并使用统计算法对报文进行归类,根据归类结果,干扰模块在链路层针对特定节点发起攻击,以获取最大的干扰收益,并使被检测概率最小化.最后,应用层感知模块侦测网络会话(sessions),干扰模块则根据会话信息,设定何时发起干扰以最小化网络性能.具体实现细节可参考文献[17].

(2) 针对 802.11 协议的干扰攻击

这种类型的干扰攻击主要针对 802.11 协议标准[18].具体来说,依据 802.11 MAC 层通信协议中各种控制帧和数据帧的发送时间,进行有针对性的干扰攻击[19].

- CTS(clear to send)帧干扰

攻击者侦听信道,在发送节点广播 RTS(ready to send)帧后,继续等待 SIFS(short inter frame space)时间间隔,然后广播一个干扰脉冲信号.这将导致网络邻居节点的 CTS 帧损坏,发送者接收不到 CTS 帧.最坏情况下,网络

吞吐量为 0.

- ACK 帧干扰

与 CTS 干扰类似,攻击者当侦听到数据帧 DATA 发送后,继续等待 SIFS 时间,然后发送干扰信号.这将使发送者接收不到 ACK 应答,导致发送者重传数据,直到发送者放弃发送,丢弃 MAC 层队列的帧数据.同样,最坏情况下,网络吞吐量为 0.

- DATA 帧干扰

与前两种攻击方式相似,攻击者侦听到CTS帧发送后,继续等待DIFS(DCF inter frame space)时间,然后进行干扰,使得 DATA 帧损坏.

- DIFS 帧等待干扰

这种攻击方式主要破坏协议中需要等待 DIFS 时间的帧,如 DATA 帧和 RTS 帧.

- 窄带干扰

Gummadi 等人[20]通过实验分析了 802.11 网络面对干扰的脆弱性,提出了一种窄带干扰(narrow-band jamming)方式,该攻击方式特别针对于 802.11 的动态区域选择(dynamic range selection)、PLCP(physical layer convergence procedure)帧头处理等机制,并证明,由于802.11物理层和MAC层的设计缺陷,即使用低于正常传送节点 1 000 倍的信号进行干扰,也可以破坏报文的接收.

- 贪婪行为

贪婪行为(greedy behavior)是指,网络中的个别自私节点为了提高自身的吞吐量,而争夺其他节点的通信时间[21−24].比如,他们可以在侦听信道后实施上文提到的 CTS 帧干扰、ACK 帧干扰或者 DATA 帧干扰等,使得网络中其他节点不能发送报文,只能保持等待或者静默状态,从而达到提高自身吞吐量的目的.

表 1 总结了各种干扰模型在实现复杂性、能耗、稳定性等方面的表现.

Table 1 Comparison of characteristics of various jamming models

表 1 各种干扰模型的特征比较

Jammin ; model	Implementation omplexity	Energ efficiency	tealthiness	Level of DOS	Anti-Jamming resistance
Constant[2]	Low	Low	Low	High	Medium
Deceptive[2]	Low	Low	Low	High	Medium
Random[2]	Low	Adjustable	Medium	Adjustable	Medium
Reactive[2]	High	High	Medium	High	Low
Packet corruption[11,19]	Average	High	Average	High	Low
Narrow-Band[20]	High	High	High	High	Average
DIFS waiting[11,19]	Medium	Medium	Medium	High	Low
Layered attacks[17]	High	Low	Average	High	Medium

3 干扰攻击检测机制

3.1 检测机制概述

由于干扰攻击的危害性,及时、有效的检测算法对于恢复网络正常操作和安全性至关重要.当前,检测机制的总体思路是,依据发送节点或者接收节点各层(物理层及以上层)的多种属性(如信号强度、侦听时间、报文接收率等)在受到干扰攻击前后的变化进行判断,并最终决策是否受到干扰攻击.最具代表性的工作是 Xu 等人发表于无线领域顶级会议 MobiHoc 2005 的文章[2].在本节以下部分,我们将阐述当前检测机制的代表性工作,并在最后加以归纳总结.

另一方面,多种攻击模型的存在也为干扰攻击的检测带来巨大挑战.攻击检测算法应当具备准确性、及时性、可扩展性、分布性以及误判率低(false positive)等特点[25].这也是区分检测方法优劣的主要标准.

3.2 底层检测机制

底层检测机制主要依靠物理层和 MAC 层中某些属性的变化进行检测.基本思想是,攻击者干扰信号的存

在势必会影响到接收节点端信号强度的变化.基于此,主要有以下几种检测方法.

(1) 信号强度测量(signal strength)

这是一种最直观的检测方法,但 Xu 等人[2,26]通过实验证明,只使用简单的统计方法,比如统计接收节点平均的信号强度,并不能区分干扰攻击和正常的网络状态.难点还有如何选择合适的判断门限值,以及如何区分正常的网络拥塞以及干扰攻击等.因此,Xu 等人[2,26]使用了一种频谱差分(spectral discrimination)的方法,用该方法可以检测出持续性干扰攻击和欺骗性干扰攻击,但不能用于随机性干扰和按需性干扰的检测.

(2) 载波侦听时间(carrier sensing time)

这种检测方式主要适用于采用了载波侦听多路访问(carrier sense multiple access,简称 CSMA)的网络,如 802.11MAC 协议.主要的思想是,在没有干扰攻击的情况下,普通节点通过历史记录或者理论分析,可以获取载波侦听时间的分布特性,一旦存在有意干扰,侦听时间的分布特性必然受影响,从而用于干扰攻击的检测[2,26].但与信号强度测量方法相同的是,这种方法也只能用于持续性干扰攻击和欺骗性干扰攻击的检测,而无法判断随机性干扰和按需性干扰的检测.

(3) PDR 测量

Xu 等人[2,26]在 Mica2 系列节点平台上的实验结果表明,通过测量 PDR 值,可以有效检测各种基本的干扰攻击.实验结果表明:即使在一个高度拥塞的网络环境下,PDR 值依然可以达到 78%;而在有干扰攻击情况下,PDR 值锐减.因此,为了区分拥塞状态和干扰攻击,可以设定一个 PDR 值门限,从而达到检测目的.但 PDR 值测量方法对于某些网络场景依然无能为力,如节点电池耗尽,或者链路质量差(信噪比小于特定值).

表 2 给出了 3 种单独的检测方法对基本类型的干扰攻击的有效性[2].

Table 2 Comparison of efficiency of different detection methods

表 2 检测方法的有效性对比

Jamming model	Carrier sensing time	Signal strength		PDR
		Average	Spectral discrimination	
Constant[2]	√	√	√	√
Deceptive[2]	×	√	√	√
Random[2]	×	×	×	√
Reactive[2]	×	×	×	√

(4) 一致性检测

为了克服以上 3 种检测方法的不足之处,Xu 等人[2,26]提出了两种一致性检测方法.

- 信号强度一致性检测

其基本思想是,同时测量信号强度值和 PDR 值,如果 PDR 值低,而信号强度值高,则很有可能存在干扰攻击;如果 PDR 值低,同时信号强度值也很低,则很可能是因为网络链路质量差或者节点失效.其判断依据见表 3.

Table 3 PDR vs. signal strength

表 3 报文接收率 vs. 信号强度

PDR	Signal strength	Typical scenarios
PDR=0 (no preamble is received)	Low	Non jammed: Neighbor failure, neighbor absence, neighbors being blocked, etc.
PDR=0 (no preamble is received)	Low	Node jammed
PDR low (packets are corrupted)	Low	Non jammed: Neighbor being faraway
PDR low (packets are corrupted)	High	Node jammed

- 位置一致性检测

与信号强度一致性检测相似,其主要思想是在记录 PDR 值的同时,将邻居通信节点的位置考虑在内.如果 PDR 值低,而与邻居通信节点的距离近,则很有可能存在干扰攻击;如果 PDR 值低,但两者距离也较大,则有可能是因为脱离了无线通信范围导致的网络链路质量差或者失效.

3.3 贪婪行为检测

这种检测机制主要针对网络内节点贪婪行为发起的干扰攻击.DOMINO(detection of greedy behavior in the

MAC layer of IEEE 802.11 network)[21]是其中最具代表性的检测系统.DOMINO 由 3 个模块组成.第 1 个模块负责网络流量 trace 的收集.这些 trace 被第 2 个模块,即测试模块作为输入,进行各种测试.当前,该系统支持 6 种测试方法,每一种测试都包含两种核心算法:一种是偏差估计算法,用于计算与期望模型之间的偏差;另一种是异常检测算法,用于判断之前的偏差是否超过指定门限,从而判断是否有干扰攻击存在.第 3 个模块负责决策,该模块收集测试模块得到的所有结果,并加于聚合判断,再对行为进行分类,以利于后续判断.

CMD(carrier sensing misbehavior detection)[24]是另一种检测方法.这种检测算法主要针对于有意调节 CCA (clear channel assessment)值以获取更多频段访问时间为目的的自私节点.其检测的基本思想是,网络中接收节点给发送者发送 CTS 或者 ACK 应答时,显示地告诉发送者下一次传输需要退避的时间(back off time).当发送者后一次传送所需的等待时间与该退避时间不匹配时,则怀疑有自私节点或干扰者的存在,具体可参考文献[24].

Radosavac 等人[27]提出了一种检测违背 back off 机制的自私节点的理论框架,并证明了最优的检测规则(detection rule)是序列概率比测试(sequential probability ratio test,简称 SPRT).该机制不需要更改已有的 802.11 协议,但需要精确地时间同步和连续的节点记录,部署实现难度大.

3.4 无线入侵检测系统(wireless intrusion detection system)

入侵检测系统(intrusion detection system,简称 IDS)一般是根据获取的历史信息以及按照一定的规则判断某一网络行为是否为攻击行为[28].无线网络,特别是无线自组织网络及无线传感器网络中的入侵检测系统近来得到广泛研究[29−34].

在无线网络中,单一节点有时不能单独判断是否受到干扰攻击还是发生网络拥塞.分布式的 IDS 通过节点之间共享的历史记录信息对网络中的数据进行判断,如包发送数、空闲等待时间、坏包数等,综合这些判断得出网络中是否存在干扰攻击[35].但这种系统的缺点也很明显,即需要节点之间进行信息共享.而一旦节点受到干扰攻击,节点将无法发送任何数据.因此,分布式 IDS 系统不是实时的检测系统;另外,分布式 IDS 系统还需要信任机制予以扶助,否则,如果存在恶意节点虚报信息,则将为 IDS 判断带来误差,甚至错误[36].

3.5 特别针对按需性干扰的检测机制

第 3.2 节~第 3.4 节剖析了当前已有的研究工作中针对干扰攻击的主要检测机制.对于周期性干扰,如持续性攻击、欺骗性攻击或者随机性攻击,攻击者不考虑网络本身特性(信道空闲或者忙碌).虽然发起攻击简单,但也容易被检测出来.而按需性干扰(reactive jamming)由于攻击者侦听信道,根据信道的忙闲情况发起攻击,隐蔽性强,检测难度大,也成为了当前研究的热点[37−39].

Shin 等人[37]提出一种利用识别触发节点(trigger node)进行按需性干扰检测的方法.这里的触发节点专指引起干扰源发起攻击的节点.他们使用组测试(group testing)技术进行触发节点的识别,并巧妙地利用这些触发节点对干扰源进行定位.Xuan 等人[38]进一步扩展了 Shin 等人的工作,采用随机非自适应组测试(randomized non-adaptive group testing)方法以及图论中的独立团(clique-independent set)理论,进一步降低了检测算法的复杂度.

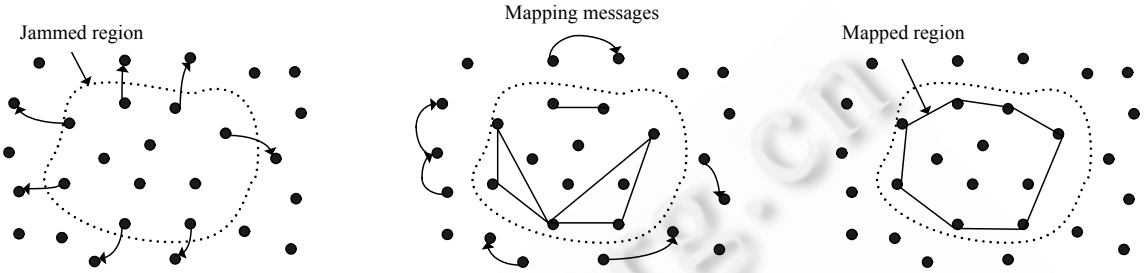
Strasser 等人[39]根据节点接收信号强度值(received signal strength,简称 RSS)来识别字节错误(bit error)的根源.其基本思想是:如果是无意的弱信号噪音或干扰,则 RSS 值较低;如果是干扰攻击,则 RSS 值会比较高.通过历史经验信息、错误纠正码以及有限的节点关联进行干扰攻击的检测.具体细节可参考文献[39].

4 干扰攻击防御

在存在干扰的网络环境下如何抵御攻击,以减少性能损失和降低安全威胁,是当前研究的另一个重点.与其他安全问题关注的角度类似,主要从主动防御和被动防御两个角度考虑.主动防御的思路是,做到有备无患,即使存在干扰攻击,也可以正常的进行网络操作.由于主动防御的难度较大,当前的研究工作较少,代表性的工作是时隙信道技术[40].被动防御则是指在检测到遭受干扰攻击时,从空间、时间或者频率等方面“避开”干扰攻击的影响,典型的防御方法包括 JAM[16]、信道切换[41−43]、空间退避[2,43]以及虫洞防御[44]等.本节重点介绍具有代表性的算法,并在最后给出分析与归纳.

4.1 干扰区域匹配服务[16]

针对无线传感器网络[45,46]中的干扰攻击,Wood 等人[16]提出了一种干扰区域匹配(jammed area mapping,简称 JAM)方法.其基本思想是,由于在干扰区域的边缘干扰信号相对较弱,边缘内节点发出 Jamming 信号,而在边缘外的节点则相互协同合作,交换接收到的 Jamming 信息,最后形成一个 Mapped Region,图 3 展示了一个具体的匹配过程.该方法可以为网络路由提供服务,即网络中节点一旦知道有这样的一个区域存在,则在下次信息转发过程中,将避开该区域,“绕道”而行.但 JAM 的缺陷在于需要修改网络底层相关通信协议,不能直接应用[16].



(a) 当检测到干扰攻击时,边缘节点向邻居报告受干扰信息

(b) 收到信息的邻居节点相互交换接收到的受干扰节点信息

(c) 聚合成一个干扰区域

Fig.3 Process of jammed area mapping service

图 3 干扰区域匹配服务过程

4.2 信道切换[41−43]

信道切换(channel surfing)方法借鉴了物理层调频技术思想,将之应用到了链路层.即,网络中节点一旦检测到干扰攻击存在,则切换到另外的安全信道.Xu 等人[41−43]提出了两种信道切换方法.一种称为协同式信道切换(coordinated channel surfing).该方法的基本思想是,受干扰的节点会切换至新的通信信道,并在新的信道上广播 Beacon 报文;同样,干扰区域边缘外的节点(受干扰节点的邻居)会感知到这些节点的消失,也切换至新的信道.如果接收到 Beacon 报文,则再切换至原来的信道,通知网络内其他节点全部切换至新的信道.显然,该方法将使全网所有节点切换至新的信道,虽然简单但通信开销和网络延迟过大.另一种切换方式是频谱复用(spectral multiplexing).该方法与协同式信道切换策略不同的是,只有受干扰节点切换信道,受干扰节点的邻居充当中继节点,网络内其他节点保持原来的通信信道.

Navda 等人[47]提出一种主动的(伪)随机信道切换协议.通过设置最优的跳转参数,即使在有干扰者的情况下,依然可以达到 60%的正常吞吐量.而且在没有干扰者的情况下,性能也没有明显下降.Pelechrinis 等人[48]则研究了信道跳转对于防御干扰攻击的有效性,通过真实的实验测试表明,相邻正交信道之间依然可以相互干扰,即频段相邻的正交信道并不是完全隔离的.如果节点在相邻的正交信道上切换,则防御效果并不明显.

4.3 空间退避(spatial retreat)[2,43]

其基本思想很简单:一旦检测到干扰攻击的存在,则“逃离”受干扰区域[2,43].主要分为两个阶段:一是移动至干扰区域外(逃离阶段),二是保持与网络其他节点的连通性(重构阶段).该策略的关键在于如何设计一个检测算法,在移动的同时尽量不损害或者尽可能小地损害网络的连通性.

4.4 虫洞防御(wormhole based defense)[44]

虫洞攻击一直被视为无线网络中的一大威胁[40,49,50],但 Cagalj 等人[44]提出了一种使用虫洞防御无线传感器网络干扰攻击的机制.其基本思想是,利用信道的多样性,在受干扰节点与干扰区域外的节点建立虫洞.他们给出了 3 种理论实现方法:

- 基于有线的虫洞(wormhole via wired pairs of sensor)

顾名思义,该方法假设在传感网中部分节点之间在能够进行无线通信的同时存在有线连接.当干扰发生时,

节点之间就可以通过有线进行通信.但为了以高概率在受干扰节点和干扰区域外节点建立有线虫洞,网络中配置大量的有线对,这并不符合部署传感网的实际情况.

- 基于跳频的虫洞(wormhole via frequency hopping pairs)

在这种机制中,网络中同样存在两种类型的节点:一种是装配有一般的单信道射频的普通节点,一种是装配有两个射频设备(单信道射频、跳频射频)的高级节点.该方法的目标是,在存在干扰攻击的情形下,能够以高概率在受干扰节点和干扰区域外节点之间至少形成 1 个跳频对.该方法需要严格的时间同步机制.

- 基于非协作跳频的虫洞(wormhole via uncoordinated channel-hopping)

该方法仍然需要一定的时间同步.与前一种方法不同的是,该方法在单一射频的信道之间进行切换,信道一般具有较大的频带宽度.具体细节可参考文献[44].

4.5 时隙信道(timing channel)[40]

以上提到的防御策略都是试图"绕过"干扰信号,无论是从频率域[41−43,47]还是从空间域[2,16,43].Xu 等人[40]则提出了一种即使干扰攻击存在的情况下,受干扰节点依然可以通信的方法.该方法基于这样一个事实:在受干扰状态下,接收者虽然不能接收正确的报文,但依然可以检测到从发送者发送过来的已损坏的报文.这样,发送者和接收者之间就可以在报文传输之间的时间间隙建立一种低速率中继时隙信道(low-rate overlay timing channel).通过该隐蔽信道进行报文传输,达到"四两拨千斤"的效果[40].

4.6 小 结

本节主要介绍了当前针对干扰攻击的防御措施和方法.总体思路主要是从不同的维度,比如从空间上或者从频段上,避开干扰源,从而尽可能地减少性能损失和安全威胁.另一方面,则是在存在干扰攻击的环境中建立起新的时隙或者隐蔽信道,主动性的防御.表 4 给出了几种典型的防御方法的对比分析.

Table 4 Analysis of typical schemes of jamming defense

表 4 典型干扰攻击防御方法分析

Defense schemes	Active & passive	Hardware changes	Re istance to j imming	Energy efficiency	Implementation complexity
JAM[16]	Passive	Yes	Medium	Adjustable	High
Channel surfing[41−43]	Passive	No	High	Medium	Medium
Spatial retreat[2,43]	Passive	No	High	Low	High
Wormhole via wired pairs of sensors[44]	Passive	Yes	High	High	Low
Wormhole via frequency hopping pairs[44]	Passive	No	Medium	Medium	Medium
Wormhole via uncoordinated channel-hopping[44]	Passive	No	Medium	Low	High
Timing channel[40]	Active	Yes	High	High	High

5 干扰源定位

找到干扰源的位置对于恢复正常的网络通信和网络管理至关重要.一旦检测到干扰攻击,就必须尽可能地"逮住"该攻击者,对其进行定位,以利于下一步安全机制的实施和部署.干扰源的位置能够为网络不同协议层的操作提供重要信息,例如,一旦检测并定位到干扰源,在路由协议的设计上就可以避开被干扰区域,以尽可能地减少丢包率,节省宝贵的网络资源.但是,在无线网络中对干扰源进行定位并非易事:首先,干扰源不遵循现今已有的定位算法,而且当今大多数的定位协议需要特殊设备的支持;其次,缺乏区分干扰攻击与正常网络拥塞的可操作性技术;最后,由于无线网络节点大部分本身能量受限,可行的干扰源定位方法不应带来过多的通信和计算开销.

定位问题一直是无线网络研究的热点,一般分为基于测距(range-based)的定位和测距无关(range-free)的定位.基于测距的定位算法主要是测量节点各种不同的物理属性,如信号强度、到达时间差[49]等,然后根据这些测量值估算被定位节点与信标节点之间的距离;测距无关定位算法[50]则依靠尽可能少的信息,如节点转发跳数、已知的部分节点位置等进行节点定位.当前,针对干扰源的定位也是基于这两种思路展开研究:基于测距的干扰源定位算法强调如何选择合适的位置节点的物理属性建立起与干扰源的关系,从而依据信号传播模型进行定

位;测距无关定位则是根据干扰区域附近内外节点的位置信息,结合相关的几何数学知识进行干扰源位置的估计.本节分析几种干扰源定位的典型算法,并给出小结.

5.1 质心定位[51]

质心定位(centroid localization,简称 CL)利用位于目标节点(被定位节点)传输范围内的所有邻居节点的位置信息进行定位.例如,假设目标节点有 N 个邻居,且坐标分别为 $\{(X_1,Y_1),(X_2,Y_2),\ldots,(X_n,Y_n)\}$,则可估算目标节点位置如公式(4)所示.

$$(\bar{X}_{target},\bar{Y}_{target})=\left(\frac{\sum_{k=1}^{N}X_k}{N},\frac{\sum_{k=1}^{N}Y_k}{N}\right) \tag{4}$$

基于权重的质心定位(weighed centroid localization,简称 WCL)[51]是 CL 定位算法的改进版,在估算目标节点位置时加入了权重信息.例如,目标节点与其邻居节点之间的距离可以作为评价指标,距离目标节点越近的节点,赋予其越大的权重.这样,目标节点的位置可用公式(5)进行估算.

$$(\bar{X}_{target},\bar{Y}_{target})=\left(\frac{\sum_{k=1}^{N}w_kX_k}{\sum_{k=1}^{N}w_k},\frac{\sum_{k=1}^{N}w_kY_k}{\sum_{k=1}^{N}w_k}\right) \tag{5}$$

5.2 虚拟力迭代定位算法[52]

针对 CL[51]和 WCL[51]定位准确性的不足,Liu 等人[52]提出了一种虚拟力迭代定位算法(virtual force iterative localization,简称 VFIL).VFIL 利用网络拓扑对干扰者的位置进行迭代估计,首先,VFIL 对干扰者的位置进行一次粗略的估计,例如,可以使用 CL 算法估计其大致位置;然后,利用 VFIL 算法进行迭代估计,直到结果接近真实的位置.VFIL 的目标是搜寻到一个干扰区域,在该干扰区域内覆盖了所有的受干扰节点.为了达到这一目标,他们定义了两种虚拟力:一种是拉力(pull force) F_{pull}^{i},由干扰区域(估计范围)外的受干扰节点产生;一种是推力(push force) F_{push}^{j},由干扰区域(估计范围)内的边缘节点(boundary node)产生.如公式(6)及公式(7)所示,F_{pull}^{i} 和 F_{push}^{j} 都被定义为标准化向量(normalized vectors),以指向干扰源的估计位置:

$$F_{pull}^{i}=\left[\frac{X_i-\bar{X}_0}{\sqrt{(X_i-\bar{X}_0)^2+(Y_i-\bar{Y}_0)^2}},\frac{Y_i-\bar{Y}_0}{\sqrt{(X_i-\bar{X}_0)^2+(Y_i-\bar{Y}_0)^2}}\right] \tag{6}$$

$$F_{push}^{j}=\left[\frac{X_0-X_j}{\sqrt{(X_0-X_j)^2+(Y_0-Y_j)^2}},\frac{Y_0-Y_j}{\sqrt{(X_0-X_j)^2+(Y_0-Y_j)^2}}\right] \tag{7}$$

这里,$(\bar{X}_0,\bar{Y}_0)$ 是干扰源的估计位置,(X_i,Y_i)是被干扰节点的位置,(X_j,Y_j)是边缘节点的位置.如公式(8)所示,F_{pull}^{i} 和 F_{push}^{j} 的合力 F_{joint} 被定义为

$$F_{joint}=\frac{\sum_{i\in J}F_{pull}^{i}+\sum_{j\in B}F_{push}^{j}}{\left|\sum_{i\in J}F_{pull}^{i}+\sum_{j\in B}F_{push}^{j}\right|} \tag{8}$$

其中,J 是估计干扰区域(estimated jammed region)外的被干扰节点的集合,而 B 则是估计干扰区域内的边缘节点的集合.在每一次迭代过程中,F_{joint} 作为一个杠杆,指引 VFIL 算法达到目标估算值.

5.3 基于Hearing Range的干扰源定位[53]

Liu 等人[53]提出了 Hearing Range 的概念,将其定义为节点能够成功正确接收报文并解码的区域,并通过分析表明,干扰者可以缩减 Hearing Range 的面积,而且缩减的大小取决于干扰者的位置和干扰信号的强度.他们利用这种特性,将位置估计归结为最小二乘问题,在不需要迭代的情况下就可以估算干扰源的位置,降低了计算开销;同时,模拟实验表明,与已有定位算法 VFIL 相比,该方法具有更高的准确度.

5.4 基于PDR梯度的干扰源定位[54]

Pelechrinis等人[54]在无线网络中实现了一种分布式的轻量级干扰源定位算法.该方法依赖于报文传输速率PDR的值.其基本思想是,既然干扰信号会随着距离增大而减弱,那么距离干扰源较远的接收者的受干扰信号就会比较弱,从而会经常满足解码所需的SNR值要求,这将使接收者的PDR值增大.依据PDR的这个属性,他们设计了一种分布式的基于梯度递减最小化(gradient descent minimization)方法,并在原型网络环境下进行了实际测试,但并没有给出具体的性能分析.

5.5 基于几何覆盖的干扰源定位[55,56]

我们提出了一种基于几何覆盖理论的干扰源定位算法(geometry-covering based localization,简称GCL)[55,56].GCL算法利用计算几何中的凸壳理论,特别是最小包容圆方法,对攻击者进行定位.理论证明了该算法的正确性和较低的时间复杂度($O(n\log(n))$).我们通过模拟实验证明,该算法在攻击者攻击范围、网络节点密度以及攻击者位置等度量值变化的情况下,比已有算法(CL,WCL,VFIL)具有更好的定位准确度.

5.6 小 结

我们分析了本节提到的几种典型干扰源定位算法在准确性以及复杂度等方面的性能,见表5.

Table 5 Analysis of typical jammer localization schemes

表5 典型干扰源定位算法分析

Jammer localization schemes	Range-Free & range-based	Computation complexity	Accuracy	Sensitivity to network density	Scalability
CL[51]	Range-Free	Low	Low	Yes	Low
WCL[51]	Range-Free	Low	Low	Yes	Low
VFIL[52]	Range-Free	High	Medium	No	Medium
Hearing range[53]	Range-Based	Low	High	No	High
PDR-Based[54]	Range-Based	…	…	…	…
GCL[55,56]	Range-Free	Medium	High	No	High

总之,当前干扰源的定位问题研究得还比较少,是未来干扰攻击研究的重点和难点.当前的研究还主要是针对单一静态干扰源进行定位,与移动干扰源以及多干扰源定位问题相关的文献还很少.因此,这也将是未来研究的重要方向,我们将在下一节给出介绍和相关的研究建议.

6 总结与展望

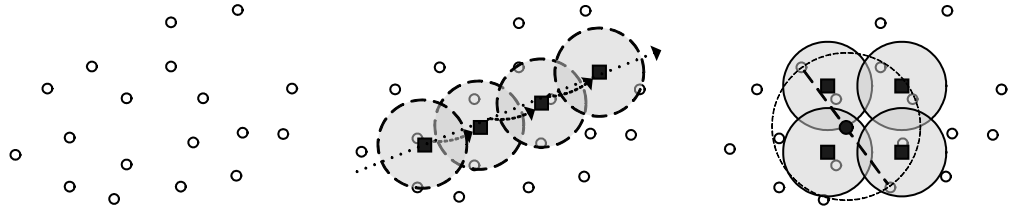
本文从攻击模型、攻击检测、防御以及干扰源定位这4个方面对无线网络中的干扰攻击进行了综述.由于无线网络媒介的广播、开放特性,干扰攻击容易实现,且攻击效果明显,严重影响着无线网络的安全和通信性能.虽然近年来干扰攻击的研究取得了一系列的研究成果,但随着各种新的攻击模型的出现以及攻击者能力的提高,无线网络依然饱受干扰的影响,不仅无意的网络拥塞影响着网络性能,有意的干扰攻击更是危害巨大.在分析了当前的研究现状、综述了已有的研究成果以后,依然有以下问题需要解决:

(1) 移动干扰攻击

如图4(a)及图4(b)所示,在一个分布式自组织网络或传感器网络中,攻击者可以发起移动干扰攻击,即干扰源具有从一个位置移动至其他位置的能力,使得干扰攻击的防御及干扰源定位难度大为增加.针对这种类型的干扰攻击,可能的解决策略就是实时跟踪干扰源的运动轨迹,并掌握其动态性和移动特征.

(2) 多干扰源攻击

在这种攻击情景中,攻击者在网络中部署多个干扰源,如图4(c)所示.当我们使用单干扰源攻击定位算法对进行定位时,如GCL[55],可能得到干扰源的估算位置.但实际上有4个干扰源在实施干扰攻击.因此,为了应对这种多个干扰源的协同攻击,需要提出新的解决方案.一种可行的策略是利用梯度信息(gradient information)[57],在全网建立基于可接收信号强度指示(received signal strength indicater,简称RSSI)[20]的势场梯度值,据此来发现可能的干扰源数量,并进一步对其进行防御或者定位.



(a) 随机部署的无线传感网 (b) 移动干扰源攻击 (c) 多干扰源攻击

Fig.4 Mobile jammer attack and multi-jammer attack

图 4 移动干扰与多干扰源协同攻击

(3) 考虑空间位置的干扰攻击研究

当前,针对干扰攻击的研究主要在时间域或者频率域上考虑,如基本的攻击模型[2]和信道跳转[41]等,都没有从空间位置上对干扰者可能发起的攻击进行考虑.如图 5 所示,将无线网络建模为最简单的 UDG(unit disc graph)模型,给定 3 个干扰源,且假定干扰源资源与普通网络节点相当(这一假设是合理的,因为这样的干扰源更具隐蔽性),则显然,在位置 1、位置 2 和位置 3 部署干扰源没有在位置 1′、位置 2′和位置 3′部署效果好.因此,位置相关的攻击模型研究无论从攻击的角度还是从防御的角度都具有十分重要的意义:对于攻击者,考虑在给定 K 个干扰源的条件下,如何最大化攻击效果(网络分割化);对于防御者,则必须在部署网络节点时考虑基于位置的干扰攻击可能带来的后果.

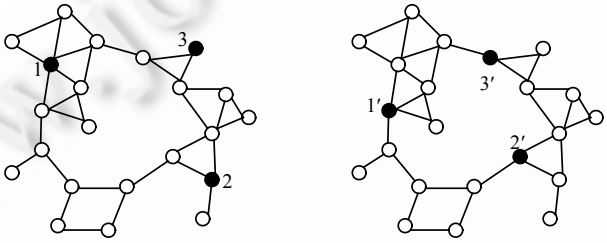


Fig.5 Impact of position on jamming attack

图 5 位置选择对干扰攻击的影响

(4) 具体检测、防御以及定位机制的实现

当前研究还主要停留在理论分析和模拟实验验证方面,缺乏相关的原型系统实现和应用.如何设计可用于现实无线网络环境中的检测算法、防御机制或者定位策略,是下一步需要考虑的又一问题.

总之,本文综述了当前无线网络中干扰攻击问题的主要研究进展,分析了干扰攻击的主要攻击模型,归纳了当前攻击的主要检测机制、防御策略和定位算法,并对未来值得研究的问题进行了展望.

致谢 在此,我们向对本文的工作给予支持和建议的同学和老师表示感谢.感谢上海交通大学 973 无线传感器网络培训项目.特别感谢国防科学技术大学并行与分布处理国防科技重点实验室无线与普适计算课题组的老师和同学的支持和鼓励.

References:

[1] Wood AD, Stankovic JA. Denial of service in sensor networks. IEEE Computer, 2002,35(10):54−62. http://dx.doi.org/10.1109/MC.2002.1039518 [doi: 10.1109/MC.2002.1039518]

[2] Xu WY, Trappe W, Zhang YY, Wood T. The feasibility of launching and detecting jamming attacks in wireless networks. In: Proc. of the ACM MobiHoc 2005. 2005. 46−57. [doi: 10.1145/1062689.1062697]

[3] Direct sequence spread spectrum. 2011. http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum

[4] Frequency hopping spread spectrum. 2011. http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

[5] Akyildiz IF, Su WL, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Communications Magazine, 2002, 40(8):102−114. [doi: 10.1109/MCOM.2002.1024422]

[6] Zhou Y, Fang YG, Zhang YC. Securing wireless sensor networks: A survey. IEEE Commun. Surveys and Tutorials, 2008,10(3): 6−28. [doi: 10.1109/COMST.2008.4625802]

[7] Abusalah L, Khokhar A, Guizani M. A survey of secure mobile ad hoc routing protocols. IEEE Commun. Surveys and Tutorials, 2008,10(4):78−93. [doi: 10.1109/SURV.2008.080407]

[8] System security group. 2011. http://www.syssec.ethz.ch/

[9] Data analysis and information security (DAIS). 2011. http://www.stevens.edu/daisy/

[10] ARENA. 2011. http://arena.cse.sc.edu/doku.php/

[11] Acharya M, Thuente D. Intelligent jamming attacks, counterattacks and (counter)^2 attacks in 802.11b wireless networks. In: Proc. of the Conf. on OPNETWORK 2005. Washington, 2005. http://www4.ncsu.edu/~mpachary/ docs/acharya_OPNETWORK05.pdf

[12] Pelechrinis K, Iliofotou M, Krishnamurthy SV. Denial of service attacks in wireless networks: The case of jammers. IEEE Communications Surveys and Tutorials, 2011,13(2):245−257. [doi: 10.1109/SURV.2011.041110.00022]

[13] Noubir G. On connectivity in ad hoc networks under jamming using directional antennas and mobility. In: Proc. of the Int'l Conf. on Wired/Wireless Internet Communications. LNCS 2957, Berlin, Heidelberg: Springer-Verlag, 2004. 521−532. [doi: 10.1007/978-3-540-24643-5_17]

[14] Law YW, Hartel P, den Hartog J, Havinga P. Link-Layer jamming attacks on S-MAC. In: Proc. of the 2nd European Workshop on WSN. 2005. 217−225. [doi: 10.1109/EWSN.2005.1462013]

[15] Law YW, van Hoesel L, Doumen J, Hartel P, Havinga P. Energy-Efficient link-layer jamming attacks against wireless sensor networks MAC protocols. In: Proc. of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks. 2005. 76−88. [doi: 10.1145/1102219.1102234]

[16] Wood AD, Stankovic JA, Son SH. JAM: A jammed-area mapping service for sensor networks. In: Proc. of the 24th IEEE Int'l Real-Time System Symp. Cancun, 2003. 286−297.

[17] Brown TX, James JE, Sethi A. Jamming and sensing of encrypted wireless ad hoc networks. In: Proc. of the 7th ACM Int'l Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc 2006). New York: ACM Press, 2006. 120−130. [doi: 10.1145/1132905.1132919]

[18] O'Hara B, Petrick AI.The IEEE 802.11 handbook: A designer's companion. Standards Information Network, IEEE Press, 1999.

[19] Acharya M, Sharma T, Thuente D, Sizemore D. Intelligent jamming attacks in 802.11b wireless networks. In: Proc. of the Conf. on OPNETWORK 2004. 2004. http://www4.ncsu.edu/~mpachary/docs/acharya_OPNETWORK04.pdf

[20] Gummadi R, Wetheral D, Greenstein B, Seshan S. Understanding and mitigating the impact of RF interference on 802.11 networks. In: Proc. of the ACM SIGCOMM 2007. 2007. http://nms.csail.mit.edu/~ramki/sigcomm07.pdf [doi: 10.1145/1282380.1282424]

[21] Raya M, Aad I, Hubaux JP, EI Fawal A. DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots. IEEE Trans. on Mobile Computing, 2006,5(12):1691−1705. [doi: 10.1109/TMC.2006.183]

[22] Kyasanur P, Vaidya NH. Selfish MAC layer misbehavior in wireless networks. IEEE Trans. on Mobile Computing, 2005,4(5): 502−516. http://dx.doi.org/10.1109/TMC.2005.71 [doi: 10.1109/TMC.2005.71]

[23] Kyasanur P, Vaidya NH. Detection and handling of MAC layer misbehavior in wireless networks. In: Proc. of the Int'l Conf. on Dependable Systems and Networks. 2003. 173−182. [doi: 10.1109/DSN.2003.1209928]

[24] Pelechrinis K, Yan GH, Eidenbenz S, Krishnamurthy SV. Detecting selfish exploitation of carrier sensing in 802.11 networks. In: Proc. of the INFOCOM 2009. 2009. 657−665. [doi: 10.1109/INFCOM.2009.5061973]

[25] Li MY, Koutsopoulos I, Poovendran R. Optimal jamming attack strategies and network defense policies in wireless sensor networks. IEEE Trans. on Mobile Computing, 2010,9(8):1119−1133. [doi: 10.1109/TMC.2010.75]

[26] Xu WY, Ma K, Trappe W, Zhang YY. Jamming sensor networks: Attack and defense strategies. IEEE Network, 2006,20(3):41−47. [doi: 10.1109/MNET.2006.1637931]

[27] Radosavac S, Barras JS, Koutsopoulos I. A framework for MAC protocol misbehavior detection in wireless networks. In: Proc. of the 4th ACM Workshop on Wireless Security (WiSe 2005). New York: ACM Press, 2005. 33−42. [doi: 10.1145/1080793.1080801]

[28] Intrusion detection system. 2011. http://en.wikipedia.org/wiki/Intrusion_detection_system

[29] Yi P, Jiang YC, Zhang SY, Zhong YP. A survey of security for mobile ad hoc networks. ACTA ELECTRONICA SINICA, 2005, 33(5):893−899 (in Chinese with English abstract).

[30] Kachirski O, Guha R. Intrusion detection using mobile agents in wireless ad hoc networks. In: Proc. of the IEEE Workshop on Knowledge Media Networking (KMN 2002). Washington: IEEE Computer Society, 2002. 153−158. [doi: 10.1109/KMN.2002.1115178]

[31] Zhang YG, Lee W. Intrusion detection in wireless ad-hoc networks. In: Proc. of the 6th Annual Int'l Conf. on Mobile Computing and Networking (MobiCom 2000). New York: ACM Press, 2000. 275−283. [doi: 10.1145/345910.345958]

[32] da Silva APR, Martins MHT, Rocha BPS, Loureiro AAF, Ruiz LB, Wong HC. Decentralized intrusion detection in wireless sensor networks. In: Proc. of the 1st ACM Int'l Workshop on Quality of Service & Security in Wireless and Mobile Networks (Q2SWinet 2005). New York: ACM Press, 2005. 16−23. http://doi.acm.org/10.1145/1089761.1089765 [doi: 10.1145/1089761.1089765]

[33] Huang YA, Lee W. A cooperative intrusion detection system for ad hoc networks. In: Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2003). New York: ACM Press, 2003. 135−147. http://doi.acm.org/10.1145/986858.986877 [doi: 10.1145/986858.986877]

[34] Mishra A, Nadkarni K, Patcha A. Intrusion detection in wireless ad hoc networks. IEEE Wireless Communications, 2004,11(1): 48−60. [doi: 10.1109/MWC.2004.1269717]

[35] Chatzigiannakis V, Androulidakis G, Pelechrinis K. Papavassiliou S, Maglaris V. Data fusion algorithms for network anomaly detection: Classification and evaluation. In: Proc. of the 3rd Int'l Conf. on Networking and Services (ICNS 2007). Washington: IEEE Computer Society, 2007. 50. http://dx.doi.org/10.1109/ICNS.2007.49 [doi: 10.1109/ICNS.2007.49]

[36] Aime MD, Calandriello G, Lioy A. A wireless distributed intrusion detection system and a new attack model. In: Proc. of the 11th IEEE Symp. on Computers and Communications. 2006. 35−40. [doi: 10.1109/ISCC.2006.22]

[37] Shin I, Shen YL, Xuan Y, Thai MT, Znati T. Reactive jamming attacks in multi-radio wireless sensor networks: An efficient mitigating measure by identifying trigger nodes. In: Proc. of the 2nd ACM Int'l Workshop on Foundations of Wireless Ad Hoc and Sensor Networking and Computing (FOWANC 2009). New York: ACM Press, 2009. 87−96. [doi: 10.1145/1540343.1540357]

[38] Xuan Y, Shen YL, Shin I, Thai MT. On trigger detection against reactive jamming attacks: A clique-independent set based approach. In: Proc. of the IPCCC 2009. 2009. 223−230. [doi: 10.1109/PCCC.2009.5403842]

[39] Strasser M, Danev B, Čapkun S. Detection of reactive jamming in sensor networks. ACM Trans. on Sensor Networks, 2010,7(2): 1−29. http://doi.acm.org/10.1145/1824766.1824772 [doi: 10.1145/1824766.1824772]

[40] Xu WY, Trappe W, Zhang YY. Anti-Jamming timing channels for wireless networks. In: Proc. of the ACM WiSec 2008. Alexandria, 2008. 203−213. [doi: 10.1145/1352533.1352567]

[41] Xu WY, Trappe W, Zhang Y. Channel surfing: Defending wireless sensor networks from interference. In: Proc. of the IPSN 2007. 2007. 499−508. [doi: 10.1109/IPSN.2007.4379710]

[42] Xu WY, Trappe W, Zhang YY. Channel surfing: Defending wireless sensor networks from jamming and interference. In: Proc. of the SenSys 2006. 2006. 403−404. [doi: 10.1145/1182807.1182877]

[43] Xu WY, Wood T, Trappe W, Zhang YY. Channel Surfing and Spatial Retreats Defenses Against Wireless Denial of Service. In: Proc. of the ACM Workshop on Wireless Security. 2004. 80−89. [doi: 10.1145/1023646.1023661]

[44] Cagalj M, Capkun S, Hubaux JP. Wormhole-Based antijamming techniques in sensor networks. IEEE Trans. on Mobile Computing, 2007,6(1):100−114. http://dx.doi.org/10.1109/TMC.2007.18 [doi: 10.1109/TMC.2007.18]

[45] Sun LM, Li JZ, Chen Y, Zhu HS. Wireless Sensor Network. Beijing: Tsinghua University Press, 2005 (in Chinese).

[46] Ren FY, Huang HN, Lin C. Wireless sensor network. Journal of Software, 2003,14(7):1282−1291 (in Chinese with English abstract). http://ww.jos.org.cn/1000-9825/20030713.htm

[47] Navda V, Bohra A, Ganguly S, Rubenstein D. Using channel hopping to increase 802.11 resilience to jamming attacks. In: Proc. of the INFOCOMM, Mini-Conf. 2007. 2526−2530.

[48] Pelechrinis K, Koufogiannakis C, Krishnamurthy SV. Gamming the jammer: Is frequency hopping effective?. In: Proc. of the 7th Int'l Symp. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks. 2009. 1−10.

[49] Girod L, Estrin D. Robust range estimation using acoustic and multimodal sensing. In: Proc. of the IEEE/RSJ Int'l Conf. on Intelligent Robots and Systems (IROS). Hawaii, 2001. 159−167. [doi: 10.1109/IROS.2001.977164]

[50] He T, Huang CD, Bium BM, Stankovic JA, Abdelzaher T. Range-Free localization schemes for large scale sensor networks. In: Proc. of the ACM MobiCom. San Diego, 2003. 354−365. [doi: 10.1145/938985.938995]

[51] Blumenthal J, Grossmann R, Golatowski F, Timmermann D. Weighted centroid localization in zigbee-based sensor networks. In: Proc. of the IEEE Int'l Symp. on Intelligent Signal Processing. Alcala de Henares, 2007. 1−6. [doi: 10.1109/WISP.2007.4447528]

[52] Liu HB, Xu WY, Chen YY, Liu ZH. Localizing jammers in wireless networks. In: Proc. of the PERCOM 2009. Washington: IEEE Computer Society, 2009. 1−6. http://dx.doi.org/10.1109/PERCOM.2009.4912878 [doi: 10.1109/PERCOM.2009.4912878]

[53] Liu ZH, Liu HB, Xu WY, Chen YY. Wireless jamming localization by exploiting nodes' hearing ranges. In: Proc. of the 6th IEEE Int'l Conf. on Distributed Computing in Sensor Systems (DCOSS 2010). Berlin, Heidelberg: Springer-Verlag. LNCS 6131, 2010. 348−361. [doi: 10.1007/978-3-642-13651-1_25]

[54] Pelechrinis K, Koutsopoulos I, Broustis I, Krishnamurthy SV. Lightweight jammer localization in wireless networks: System design and implementation. In: Proc. of the Globecom 2009. Hilton Hawallan Village, 2009. 204−208. [doi: 10.1109/GLOCOM.2009.5425405]

[55] Sun YQ, Wang XD, Zhou XM. Geometry-Covering based localization for jamming attack in wireless sensor networks. Journal on Communications, 2010,31(11):10−16 (in Chinese with English abstract).

[56] Sun YQ, Wang XD. Jammer localization in wireless sensor networks. In: Proc. of the 5th Int'l Conf. on Wireless Communications, Networking and Mobile Computing (WiCOM 2009). Piscataway: IEEE Press, 2009. 3113−3116. [doi: 10.1109/WICOM.2009.5302614]

[57] Lin HJ, Lu MH, Milosavljevic N, Gao J, Guibas LJ. Composable information gradients in wireless sensor networks. In: Proc. of the 7th Int'l Conf. on Information Processing in Sensor Networks (IPSN 2008). Washington: IEEE Computer Society, 2008. 121−132. http://dx.doi.org/10.1109/IPSN.2008.21 [doi: 10.1109/IPSN.2008.21]

附中文参考文献:

[29] 易平,蒋嶷川,张世永,钟亦平.移动 ad hoc 网络安全综述.电子学报,2005,33(5):893−899.

[45] 孙利民,李建中,陈渝,朱红松.无线传感器网络.北京:清华出版社,2005.

[46] 任丰原,黄海宁,林闯.无线传感器网络.软件学报,2003,14(7):1282−1291. http://ww.jos.org.cn/1000-9825/20030713.htm

[55] 孙言强,王晓东,周兴铭.无线传感器网络中基于几何覆盖的 Jamming 攻击定位算法.通信学报,2010,31(11):10−16.

孙言强(1985－),男,山东巨野人,博士生,主要研究领域为无线网络中的攻击检测.

王晓东(1973－),男,博士,研究员,CCF 高级会员,主要研究领域为无线网络,协同通信.

周兴铭(1938－),男,教授,博士生导师,中国科学院院士,CCF 高级会员,主要研究领域为移动计算与无线网络,高性能计算,并行处理.