doi:10.11887/j.cn.202201017 http://journal.nudt.edu.cn

无线自组织网络跨层攻击检测博弈模型*

王 剑,刘星彤,降 帅
(国防科技大学 电子科学学院,湖南 长沙 410073)

摘 要:无线自组织网络中的跨层攻击具有比单层攻击更强的隐蔽性、更好的攻击效果或更低的攻击成本。为了检测无线自组织网络中的跨层攻击,提出了一种基于博弈论的攻击检测模型。由于攻击不可避免地会对各协议层的参数造成影响,因此模型从协议层攻防博弈的角度,建立起相应的策略矩阵和支付矩阵,并通过均衡分析得到该模型的混合策略纳什均衡解。仿真结果表明,与传统的检测算法相比,采用混合策略的检测算法具有更优的检测性能并且能够显著降低节点能量消耗。

关键词:跨层攻击;无线自组织网络;博弈论
中图分类号:TN918 **文献标志码**:A **文章编号**:1001-2486(2022)01-114-08

Game model for detecting cross-layer attacks in wireless ad hoc networks

WANG Jian, LIU Xingtong, JIANG Shuai
(College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China)

Abstract: Compared with single-layer attacks, cross-layer attacks in wireless ad hoc networks can better conceal attack behavior, achieve better attack effects, or reduce the cost of attack. In order to detect cross-layer attacks in wireless ad hoc networks, a detection model based on game theory was proposed. As the attack will inevitably affect the parameters of each protocol layer, the corresponding strategy matrix and payoff matrix was built from the aspect of attack-defense game of protocol layer, and the mixed strategy Nash equilibrium solution was obtained by equilibrium analysis. Simulation experiments results show that the detection system adopting mixed strategy can achieve a better detection performance and save the energy consumption significantly, compared with the traditional detection system.

Keywords: cross-layer attack; wireless ad hoc networks; game theory

无线自组织网络是节点之间通过自组织方式互联而成的网络,具有分布式运行、拓扑动态变化等特点。无线传感器网络是一种应用非常广泛的无线自组织网络,在农业、环境、军事等领域具有非常广阔的应用前景。由于节点部署的开放性以及无线通信的开放性,传感器节点容易被恶意节点所操控,传输的敏感信息易被攻击者所窃取。攻击者可以在物理层阻塞传感器节点的信道或者直接俘获传感器节点以获取其中的秘密消息[1]。攻击者在数据链路层可以发起碰撞攻击、休眠剥夺攻击、退避时间操控攻击、保证时隙(Guaranteed Time Slot,GTS)攻击等[2-3],在网络层可发起黑洞攻击、虫洞攻击、槽洞攻击、女巫攻击、数据包选择转发攻击、Hello flood攻击等[4],在传输层可发起洪泛攻击、去同步攻击等[1]。

无线自组织网络中除了针对某一协议层的单层攻击之外,还存在与多个协议层相关的跨层攻击[5-11]。跨层攻击的目的是期望获得比单层攻击更好的攻击效果、更好地隐蔽攻击行为或者更低的攻击成本。Radosavac等提出了一种从介质访问控制(Medium Access Control,MAC)层发起攻击,并传播到网络层,造成路由破坏的MAC-Network跨层攻击方法[5]。在该方案中,攻击者利用在MAC层的合法通信,使得1个或多个邻居节点脱离网络,并提高了攻击者自己成为新路由的概率。Bian等提出了一种仍从MAC层发起攻击,但目标为破坏传输层端到端数据流传输的MAC-Transport跨层攻击方法[6]。攻击者通过使用小的竞争窗口(Contention Window,CW)值周期性地占用无线信道,使得传输控制协议(Transmission Control Protocol,TCP)流的往返时

* 收稿日期:2021-01-13
基金项目:教育部-中国移动科研基金资助项目(MCM20200103)
作者简介:王剑(1975—),男,湖南邵阳人,教授,博士,博士生导师,E-mail:jwang@nudt.edu.cn

延(Round-Trip Time,RTT)产生很大的抖动,并造成数据流的重传超时(Retransmission TimeOut,RTO)。根据 TCP 拥塞控制机制,拥塞窗口的值将设置为 1,从而导致端到端的吞吐量大大降低。此外,Nagireddygari 等针对认知无线网络提出了一种 MAC-Transport 跨层攻击方法[7]。Wang 等提出了一种物理层和 MAC 层协同配合的攻击方法,以增大攻击强度并降低被发现的风险[8]。Hossain 等利用认知无线网络中低层频谱感知机制的缺陷以及网络层的路由操控,提出了一种跨层攻击方法可将数据流传输给指定节点[9]。Hasan 等提出一种针对移动通信网络的跨层攻击方法,利用数据链路层和网络层的信息在物理层发起阻塞攻击,以破坏移动台与基站收发信台之间的通信[10]。

跨层攻击中各个层次起到的作用可能会不一样。事实上,在当前针对无线网络的跨层攻击中,由于上层的路由策略、数据传输与下层的 MAC 协议有很大关联,因此很多跨层攻击都是从 MAC 层发起,进而影响协议的其他层次。将跨层攻击定义为:“综合考虑多层协议的漏洞或相关信息,通过在某一协议层发起攻击,或者在多个协议层协同攻击,以达到在单一协议层次难以实现的攻击目标[11]”。这里要注意的是,跨层攻击不同于多层攻击,多层攻击可以在多个协议层次实施,但是各层次之间的攻击通常是独立的,而跨层攻击通常则是为了达到某种特殊目的在多个层次发起协同攻击或者在某一层发起攻击但目标为破坏其他层次的功能。

目前的入侵监测系统主要有基于误用和基于异常两种类型。误用检测基于预先定义的规则能够很容易地检测到已知攻击,但对于未知攻击则无能为力。相较于误用检测,异常检测具有较高的检测率以及检测未知攻击的能力,但同时也带来了较高的误报率。异常检测的方法有很多,包括基于流量预测、统计方法、数据挖掘、博弈论、免疫理论、信任管理、人工智能等[12-23]。Han 等利用马尔可夫模型提出一种针对无线传感器网络的流量预测算法,并基于此算法设计了一种分布式异常检测方案,可有效检测影响网络数据流选择的前向攻击、拒绝服务攻击等[12]。Alaparthy 等基于免疫理论提出了一种多层入侵检测系统,通过监控节点能量、数据包传输数量、数据发送频率等参数,计算得到聚合输出,以此检测无线传感器网络中的黑洞攻击、虫洞攻击等[13]。Bao 等提出一种基于可信的无线传感器网络入侵检测方案,通过对节点的可信值进行统计分析来判断节点的恶意性[14]。Luo 等提出一种分簇无线传感器网络可信管理系统,该系统通过监控节点行为实现对节点可信值的动态管理,并基于可信评估模型来识别攻击行为[15]。Sandhya 等基于遗传 K 均值算法提出一种入侵检测框架,以识别无线传感器网络中的攻击行为和攻击节点[16]。Geetha 等基于决策树提出一种入侵检测算法,分析表明 Hoeffding 树最适合无线传感器网络中的数据流检测[17]。Otoum 等分析了深度学习应用于无线传感器网络入侵检测的可行性,提出了一种基于受限玻尔兹曼机的入侵监测系统[18]。

事实证明,博弈论在分析多人策略决策问题方面是一种非常有效的工具。无线网络中攻防对抗的本质完全可以用攻防双方相互作用的攻防策略来表示,而博弈论可用于描述理性判决者所采取策略之间的相互影响。Chen 等将异构网络中的入侵检测问题视为攻击者和入侵检测系统之间的非合作零和博弈进行了建模和分析[19]。Liu 等提出了一种贝叶斯博弈框架来分析无线 ad hoc 网络中攻击节点与防御节点之间的相互影响[20]。Moosavi 等设计了一种非零和鲁棒的随机博弈框架,分析了无线传感器网络中的入侵检测问题[21]。Guan 等基于多标准博弈提出了一种无线传感器网络入侵检测机制[22]。当前,大多数入侵检测方案的重点是检测典型的攻击行为,对于不同种类攻击方法同时实施或多层次协同配合的跨层攻击场景则较少考虑。由于攻击将不可避免地对多个协议层的参数造成影响,因此将多层协议参数的偏差作为可信度量参数,提出了一种基于可信模型的入侵检测方案[23]。

为检测跨层攻击,通常的方式是监测各层协议的参数变化,并进行综合研判。本文从攻防博弈的角度,在充分考虑协议层攻击方式的基础上,提出了一种针对无线自组织网络的博弈模型,并计算出该模型的支付函数,分析了模型的纳什均衡,得到了混合策略纳什均衡解。仿真结果表明,采用混合策略纳什均衡的检测系统具有较好的检测性能并且能有效节约节点的能量消耗。

1　跨层攻击检测博弈模型

1.1　博弈模型的建立

攻防博弈模型中包含攻击者和检测者,攻击

者用 A 表示,检测者用 D 表示。攻击者通过攻击网络来获取利益,而检测者通过发现攻击行为来保护网络。攻击者一旦发起攻击将支付一定代价,如果攻击成功将得到一定利益。检测系统一旦启动检测程序将消耗一定能量,如果成功检测到攻击也将获得一定利益。这是一种典型的相互对立的博弈过程,攻击者和检测者显然不可能合作,因此应采用非合作博弈模型。由于攻防双方不断重复攻防过程,因此该模型应为可重复博弈模型。此外,攻击者的行为和检测者的行为没有固定的先后顺序,他们可以同时或随机发起攻击或者检测,后者并没有前者所采取策略的相关信息,因此可以将该过程视为静态博弈过程。假设攻防双方对彼此的特性、策略空间和支付函数有着比较全面的了解,可以采用完全信息非合作静态博弈模型来分析攻防过程。攻击者和检测者的策略空间分别用 $\boldsymbol{SA}$ 和 $\boldsymbol{SD}$ 表示,支付函数分别用 $\boldsymbol{UA}$ 和 $\boldsymbol{UD}$ 表示,因此博弈模型可表示为 $\boldsymbol{G}=\{(A, D),(\boldsymbol{SA}, \boldsymbol{SD}),(\boldsymbol{UA}, \boldsymbol{UD})\}$。

攻击者可以选择在物理层、*MAC* 层、网络层、传输层、应用层等各个层次发起攻击,可以发起 *MAC-Network*、*MAC-Transport*、*Network-Application* 等跨层攻击,也可以选择不发起攻击。为简化模型,将攻击者的策略空间定义为 $\boldsymbol{SA}=\{A_{\mathrm{SL}}, A_{\mathrm{CL}}, A_0\}$,其中 A_{SL} 表示单层攻击,A_{CL} 表示跨层攻击,A_0 表示不攻击。同样地,检测者可以选择单层检测、跨层检测和不检测,因此检测者的策略空间可表示为 $\boldsymbol{SD}=\{D_{\mathrm{SL}}, D_{\mathrm{CL}}, D_0\}$,其中 D_{SL} 表示单层检测,D_{CL} 表示跨层检测,D_0 表示不检测。策略矩阵 $\boldsymbol{S}$ 可以表示为:

$$\boldsymbol{S}=\begin{bmatrix}(A_{\mathrm{CL}},D_{\mathrm{CL}}) & (A_{\mathrm{CL}},D_{\mathrm{SL}}) & (A_{\mathrm{CL}},D_0)\\ (A_{\mathrm{SL}},D_{\mathrm{CL}}) & (A_{\mathrm{SL}},D_{\mathrm{SL}}) & (A_{\mathrm{SL}},D_0)\\ (A_0,D_{\mathrm{CL}}) & (A_0,D_{\mathrm{SL}}) & (A_0,D_0)\end{bmatrix} \tag{1}$$

矩阵中的元素表示攻防双方采取的策略。例如矩阵的第一个元素 S_{11} 表示攻击者采用跨层攻击策略,同时检测者采用跨层检测策略。在这种情况下,攻击者的攻击行为将以很大的概率被检测者检测到,因此检测者会得到一定的收益,而对于攻击者将造成一定的损失。如果攻击者发起跨层攻击,而检测者实施的是单层检测,则检测者可能很难发现攻击者的攻击行为,因此攻击者将获得一定的利益。如果攻击者选择不攻击而检测者仍实施检测策略,虽然攻击者不能得到收益,但检测者会消耗一定的能量。攻击者和检测者的支付矩阵可分别表示为:

$$\boldsymbol{UA}=\begin{bmatrix}UA_{11} & UA_{12} & UA_{13}\\ UA_{21} & UA_{22} & UA_{23}\\ UA_{31} & UA_{32} & UA_{33}\end{bmatrix} \tag{2}$$

$$\boldsymbol{UD}=\begin{bmatrix}UD_{11} & UD_{12} & UD_{13}\\ UD_{21} & UD_{22} & UD_{23}\\ UD_{31} & UD_{32} & UD_{33}\end{bmatrix} \tag{3}$$

式中,矩阵中的元素表示攻击者和检测者的支付函数。例如,$\boldsymbol{UA}$ 的第 1 个元素 UA_{11} 表示当攻击者发起跨层攻击且检测者实施跨层检测时攻击者的支付函数。

1.2 博弈模型的支付函数

博弈双方倾向于选择能够最大化各自利益的策略。为便于描述模型的支付函数,定义了相应的参数,如表 1 所示。

表 1 支付函数参数

Tab. 1 Parameters of payoff functions

参数名称	含义	参数名称	含义
g_{AS}	发起单层攻击收益	c_{AS}	发起单层攻击成本
g_{AC}	发起跨层攻击收益	c_{AC}	发起跨层攻击成本
g_{DS}	成功检测单层攻击收益	c_{DS}	检测单层攻击成本
g_{DC}	成功检测跨层攻击收益	c_{DC}	检测跨层攻击成本
a_{SS}	单层检测单层攻击成功率	a_{SC}	单层检测跨层攻击成功率
a_{CC}	跨层检测跨层攻击成功率	a_{CS}	跨层检测单层攻击成功率

根据定义的参数可以描述在不同策略下的支付函数。例如,策略 $S_{11}=(A_{\mathrm{CL}}, D_{\mathrm{CL}})$,表示攻击者选择跨层攻击,同时检测者选择跨层检测的策略。在这种情况下,攻击行为被检测到的概率为 a_{CC},攻击者和检测者的支付函数可分别表示为:

$$UA_{11}=(1-a_{\mathrm{CC}})g_{\mathrm{AC}}-a_{\mathrm{CC}}g_{\mathrm{DC}}-c_{\mathrm{AC}} \tag{4}$$

$$UD_{11}=a_{\mathrm{CC}}g_{\mathrm{DC}}-(1-a_{\mathrm{CC}})g_{\mathrm{AC}}-c_{\mathrm{DC}} \tag{5}$$

如果攻击者发起跨层攻击而检测者采取单层检测策略,则攻击者和检测者的支付函数分别为:

$$UA_{12}=(1-a_{\mathrm{SC}})g_{\mathrm{AC}}-a_{\mathrm{SC}}g_{\mathrm{DC}}-c_{\mathrm{AC}} \tag{6}$$

$$UD_{12}=a_{\mathrm{SC}}g_{\mathrm{DC}}-(1-a_{\mathrm{SC}})g_{\mathrm{AC}}-c_{\mathrm{DS}} \tag{7}$$

如果攻防双方选择 S_{13},即攻击者发起跨层攻

击但检测者选择不进行检测,显然攻击者能攻击成功,相应的支付函数可分别表示为:

$$UA_{13} = g_{AC} - c_{AC} \tag{8}$$

$$UD_{13} = -g_{AC} \tag{9}$$

类似地,攻击者和检测者的支付函数矩阵可分别表示为:

$$\boldsymbol{UA} = \begin{bmatrix} (1-a_{CC})g_{AC} - a_{CC}g_{DC} - c_{AC} & (1-a_{SC})g_{AC} - a_{SC}g_{DC} - c_{AC} & g_{AC} - c_{AC} \\ (1-a_{CS})g_{AS} - a_{CS}g_{DS} - c_{AS} & (1-a_{SS})g_{AS} - a_{SS}g_{DS} - c_{AS} & g_{AS} - c_{AS} \\ 0 & 0 & 0 \end{bmatrix} \tag{10}$$

$$\boldsymbol{UD} = \begin{bmatrix} a_{CC}g_{DC} - (1-a_{CC})g_{AC} - c_{DC} & a_{SC}g_{DC} - (1-a_{SC})g_{AC} - c_{DC} & -g_{AC} \\ a_{CS}g_{DS} - (1-a_{CS})g_{AS} - c_{DC} & a_{SS}g_{DS} - (1-a_{SS})g_{AS} - c_{DS} & -g_{AS} \\ -c_{DC} & -c_{DS} & 0 \end{bmatrix} \tag{11}$$

1.3　纳什均衡分析

纳什均衡即寻求非合作博弈中的最优解,在纳什均衡的情况下,攻防双方的策略对于对方来说都是最优反应。在本文的纯策略博弈模型中,对支付函数的参数有一些限制。首先,收益一定大于成本,否则相应的策略为无效策略,不会被博弈双方所选择。由此可得到 $g_{AS} > c_{AS}$、$g_{AC} > c_{AC}$、$g_{DS} > c_{DS}$、$g_{DC} > c_{DC}$。其次,跨层攻击的收益应大于单层攻击,跨层检测要比单层检测复杂,因此有 $g_{AS} < g_{AC}$、$c_{DC} > c_{DS}$。

纯策略能为博弈双方提供最大收益或者最佳结果。因此,它对于博弈双方而言都是最佳策略。通过分析支付矩阵可以很容易得到纯策略纳什均衡。可以圈出 $\boldsymbol{UA}$ 矩阵中每一列的最大值以及 $\boldsymbol{UD}$ 矩阵中每一行的最大值,如果有一个元素在 $\boldsymbol{UA}$ 和 $\boldsymbol{UD}$ 矩阵中都被圈出了,则找到了纯策略纳什均衡解。根据支付函数参数的定义,可以得到 $\boldsymbol{UA}$ 矩阵中每一列的最大值分别是 UA_{31}、UA_{12}、UA_{13},$\boldsymbol{UD}$ 矩阵中每一行的最大值分别为 UD_{11}、UD_{22}、UD_{33},因此该模型没有纯策略纳什均衡解。事实上,得出这个结论是合理的,因为如果检测者实施了相应的检测策略,则攻击者倾向于不攻击;如果检测者知道攻击者采取的攻击策略,则检测者将采用相应的检测策略。

在混合策略博弈模型中,至少一方以一定概率去选择相应的纯策略。假设攻击者分别以概率 p_1、p_2 和 $(1-p_1-p_2)$ 选择攻击策略 A_{SL}、A_{CL} 和 A_0,检测者分别以概率 q_1、q_2 和 $(1-q_1-q_2)$ 选择检测策略 D_{SL}、D_{CL} 和 D_0,因此攻击者和检测者总的支付函数可分别表示为:

$$\begin{aligned} \boldsymbol{UA} = {} & p_1q_1UA_{11} + p_1q_2UA_{12} + p_1(1-q_1-q_2)UA_{13} + \\ & p_2q_1UA_{21} + p_2q_2UA_{22} + p_2(1-q_1-q_2)UA_{23} + \\ & (1-p_1-p_2)q_1UA_{31} + (1-p_1-p_2)q_2UA_{32} + \\ & (1-p_1-p_2)(1-q_1-q_2)UA_{33} \end{aligned} \tag{12}$$

$$\begin{aligned} \boldsymbol{UD} = {} & p_1q_1UD_{11} + p_1q_2UD_{12} + p_1(1-q_1-q_2) \\ & UD_{13} + p_2q_1UD_{21} + p_2q_2UD_{22} + p_2(1-q_1 \\ & -q_2)UD_{23} + (1-p_1-p_2)q_1UD_{31} + (1 \\ & -p_1-p_2)q_2UD_{32} + (1-p_1-p_2)(1-q_1 \\ & -q_2)UD_{33} \end{aligned} \tag{13}$$

对式(12)~(13)求偏导,可得:

$$\begin{cases} \dfrac{\partial \boldsymbol{UA}}{\partial p_1} = 0 \\ \dfrac{\partial \boldsymbol{UA}}{\partial p_2} = 0 \\ \dfrac{\partial \boldsymbol{UA}}{\partial q_1} = 0 \\ \dfrac{\partial \boldsymbol{UA}}{\partial q_2} = 0 \end{cases} \tag{14}$$

由式(14)可得:

$$\begin{cases} q_1^* = \dfrac{1}{a_{CC}a_{SS} - a_{CS}a_{SC}}\left[\dfrac{a_{SS}(g_{AC} - c_{AC})}{g_{AC} + g_{DC}} - \dfrac{a_{SC}(g_{AS} - c_{AS})}{g_{AS} + g_{DS}}\right] \\ q_2^* = \dfrac{1}{a_{CS}a_{SC} - a_{CC}a_{SS}}\left[\dfrac{a_{CS}(g_{AC} - c_{AC})}{g_{AC} + g_{DC}} - \dfrac{a_{CC}(g_{AS} - c_{AS})}{g_{AS} + g_{DS}}\right] \end{cases} \tag{15}$$

$$\begin{cases} p_1^* = \dfrac{1}{a_{CC}a_{SS} - a_{CS}a_{SC}} \cdot \dfrac{a_{SS}c_{DC} - a_{CS}c_{DS}}{g_{AC} + g_{DC}} \\ p_2^* = \dfrac{1}{a_{CC}a_{SS} - a_{CS}a_{SC}} \cdot \dfrac{a_{CC}c_{DS} - a_{SC}c_{DC}}{g_{AS} + g_{DS}} \end{cases} \tag{16}$$

当攻击者以概率$\{p_1^*, p_2^*, 1 - p_1^* - p_2^*\}$、检测者以概率$\{q_1^*, q_2^*, 1 - q_1^* - q_2^*\}$实施混合策略时,攻防双方的支付函数是最优的。

2　仿真分析

2.1　仿真参数

采用 MATLAB 作为仿真工具,考虑在 100 m × 100 m 范围内,随机部署 50 个节点,构成一个无线自组织网络。节点的发射功率为2 mW,通信频率为 2.4 GHz。详细的仿真参数如表 2 所示。

表2 仿真参数

Tab. 2 Simulation parameters

参数	取值或种类	参数	取值或种类
网络大小	100 m×100 m	短帧间间隔	10 μs
簇头数	1	分布协调功能帧间间隔	50 μs
节点数	49	时隙	20 μs
路由协议	按需距离向量路由协议	路由请求包大小	176 bits
MAC 协议	802.11 分布式协调功能	路由响应包大小	176 bits

考虑在窃听网络数据流、破坏网络可用性和消耗节点能量三个攻击场景下,对博弈模型的性能进行仿真分析,仿真场景的详细描述如表3所示。

表3 仿真场景

Tab. 3 Simulation scene

场景	单层攻击策略	跨层攻击策略	单层检测策略	跨层检测策略
窃听网络数据流	槽洞攻击	MAC-Network(吸引网络数据流)	跳数监控	可信模型
破坏网络可用性	退避时间攻击	MAC-Network(丢弃网络数据流)	退避窗口检测	可信模型
消耗节点能量	剥夺休眠攻击	MAC-Network(发送无用数据包)	请求发送数据帧统计	可信模型

在窃听网络数据流场景中,攻击者选择槽洞攻击作为单层攻击策略,采用 MAC-Network 攻击作为跨层攻击策略。检测者则采用跳数监控方法来检测单层攻击[24],采用基于可信的检测方法来检测跨层攻击[23]。在槽洞攻击中,攻击者尝试通过发送伪造的路由响应包(Route REPly,RREP)来吸引网络流量。在 MAC-Network 攻击中,攻击者通过减小 CW 值来获取信道,并发送包含极小跳数的伪造路由消息,使得周围节点都选择攻击者作为路由,从而达到数据流窃听的目的。对应的单层检测方案主要通过监测跳数的变化来实现,跨层检测方案通过检测 MAC 层和网络层可信值的变化来实现。仿真观测周期为800次、间隔时间为5 s、仿真时间约为70 min,通过统计计算可得到不同攻击和检测策略下的成功率。仿真结果表明,单层检测单层攻击的成功率 $a_{SS}=0.91$、单层检测跨层攻击的成功率 $a_{SC}=0.72$、跨层检测跨层攻击的成功率 $a_{CC}=0.97$、跨层检测单层攻击成功率 $a_{CS}=0.88$。

在该场景中,攻击者的收益主要由其获得的数据包数量来决定,如槽洞攻击中,攻击者获取的网络流量越大,攻击收益就越大。攻击者的成本主要由其发起攻击的次数来衡量,如在 MAC 层违规抢占信道的次数、在网络层发布虚假路由信息的次数等。检测者的收益与攻击者的收益成正比,也就是说成功攻击造成的损失越大,则成功检测此次攻击带来的收益越大。检测的成本由采集的数据量以及计算复杂度决定。因此,在该场景的仿真中,以攻击者"吸引"收到的数据包数量来衡量攻击者的收益。仿真表明,攻击者在实施单层攻击与跨层攻击时接收到的数据包数量之比约为4∶5。单层攻击的代价根据攻击者发布虚假路由的次数来衡量,跨层攻击的代价根据攻击者在 MAC 层违规占用信道以及发布虚假路由的次数来衡量。经仿真得到,这两种非正常行为的次数之比约为5∶7。此外,根据收益大于成本的原则,将两种检测成功的收益定义为检测成本的2倍。基于以上考虑,博弈双方支付函数的参数值可设置为:$g_{AS}=2$、$c_{AS}=1$、$g_{AC}=2.5$、$c_{AC}=1.4$、$g_{DS}=2$、$c_{DS}=1$、$g_{DC}=2.5$、$c_{DC}=1.2$。

在破坏网络可用性场景中,攻击者选择 MAC 层的退避时间控制攻击作为单层攻击策略,通过缩短退避时间以不断地占用信道,使得合法节点难以竞争到信道,从而无法使用网络。检测者则通过监测退避窗口值以发现此类攻击[25]。在跨层攻击中,攻击者采用 MAC-Network 攻击作为跨层攻击策略。攻击者首先通过减少 CW 值来获取信道,然后发送虚假路由信息以吸引网络数据流,最后将网络数据流丢弃以破坏网络的可用性。该场景中的跨层检测策略、观测周期、仿真时间与窃听网络数据流场景类似。通过仿真可计算得到 $a_{SS}=0.92$、$a_{SC}=0.58$、$a_{CC}=0.96$、$a_{CS}=0.68$。此场景中,攻击收益取决于攻击者占用信道和破坏正常传输的次数,攻击成本取决于攻击者发起攻击的次数。检测收益和成本的计算方法与上一个场景类似。在该场景的仿真中,支付函数的参数值可设置为:$g_{AS}=1.8$、$c_{AS}=1.2$、$g_{AC}=2$、$c_{AC}=1.4$、$g_{DS}=1.8$、$c_{DS}=0.9$、$g_{DC}=2$、$c_{DC}=1$。

在消耗节点能量场景中,攻击者采用 MAC 层

的剥夺休眠攻击作为单层攻击策略,通过发送无意义的控制帧,使得周围节点不断接收控制帧并作出响应,以消耗节点能量。检测者则通过监测节点发送的请求发送(Request To Send, RTS)帧数以检测此类攻击。在跨层攻击中,攻击者首先在 MAC 层采用小退避窗口攻击以优先占用信道,然后在网络层发送大量无用数据包以消耗节点能量。检测者同样采用基于可信模型的检测方法作为跨层攻击检测策略。通过仿真可得 $a_{SS}=0.91$、$a_{SC}=0.47$、$a_{CC}=0.93$、$a_{CS}=0.64$。攻击收益由因攻击行为引起其他节点额外发送和接收数据包的数量决定,攻击成本根据发起攻击的次数来衡量。在该场景中,同样设置 $g_{AS}=1.8$、$c_{AS}=1.2$、$g_{AC}=2$、$c_{AC}=1.4$、$g_{DS}=1.8$、$c_{DS}=0.9$、$g_{DC}=2$、$c_{DC}=1$。

2.2　仿真结果

在窃听网络数据流的场景中,由式(15)和式(16)计算得到攻击者的混合策略纳什均衡解为{0.170 2, 0.106 3, 0.723 5},检测者的混合策略纳什均衡解为 {0.050 9,0.196 3, 0.752 8}。在破坏网络可用性场景中,攻击者的混合策略纳什均衡解为 {0.157 5, 0.161 4, 0.681 1},检测者的混合策略纳什均衡解为{0.084 5,0.118 7, 0.796 8}。在消耗节点能量场景中,攻击者的混合策略纳什均衡解为 {0.153 1, 0.168 2, 0.678 7},检测者的混合策略纳什均衡解为 {0.106 6, 0.108 2, 0.785 2}。由于检测的准确率较高,攻击者发起攻击的风险较高。因此,在混合策略中攻击者大部分时间都将采取合作模式,而检测者为了节约能量大部分时间都不采取行动。

在窃听网络数据流的场景中,恶意节点分别以概率 0.170 2、0.106 3、0.723 5 发起跨层攻击、单层攻击或不攻击,检测者分别以概率 0.050 9、0.196 3、0.752 8 实施跨层检测、单层检测和不检测。图 1 给出了在使用混合策略、仅采取单层检测和仅采取跨层检测情况下的检测概率。仿真结果表明,当仿真时间超过 700 个观测周期时,检测者采用混合策略的检测率达到了 97%,高于仅采取单层检测或跨层检测的情况。破坏网络可用性和消耗节点能量等场景下的检测概率如图 2 和图 3 所示。同样地,采取混合策略时的检测概率要优于仅采取单层或跨层检测时的检测概率。

在采用混合策略、仅使用跨层检测或单层检测的情况下,以 800 个观测周期作为仿真时间,分析了节点的能量消耗。仿真表明,由混合

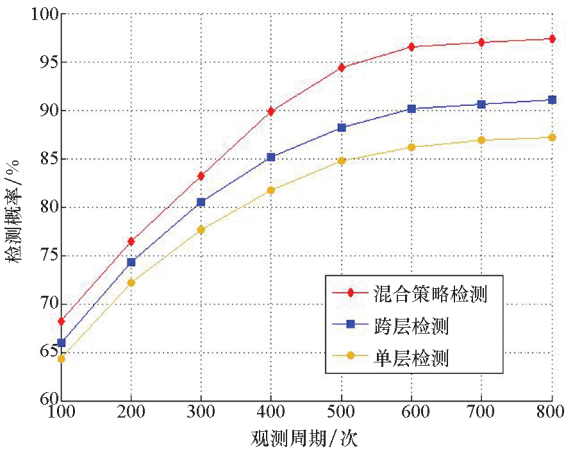

图 1　窃听网络数据流场景下的检测概率

Fig. 1　Detection probability in scenario of eavesdropping on network data stream

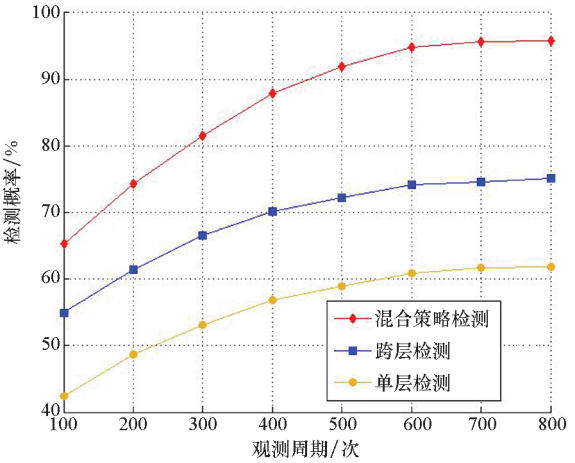

图 2　破坏网络可用性场景下的检测概率

Fig. 2　Detection probability in the scenario of destroying network availability

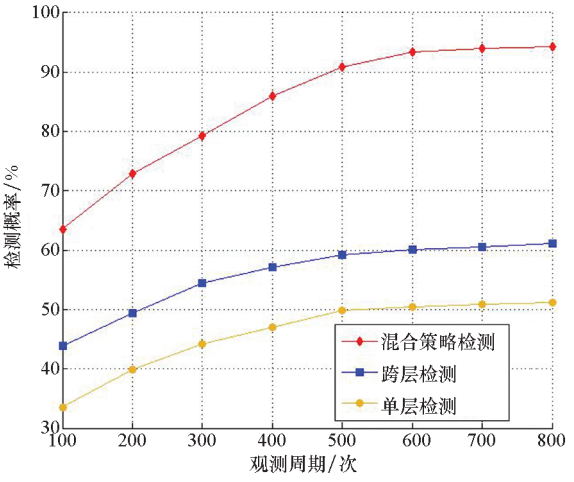

图 3　消耗节点能量场景下的检测概率

Fig. 3　Detection probability in the scenario of consuming energy of nodes

策略检测带来的能量消耗明显小于由仅进行跨层检测或单层检测带来的能量消耗，如图4所示。

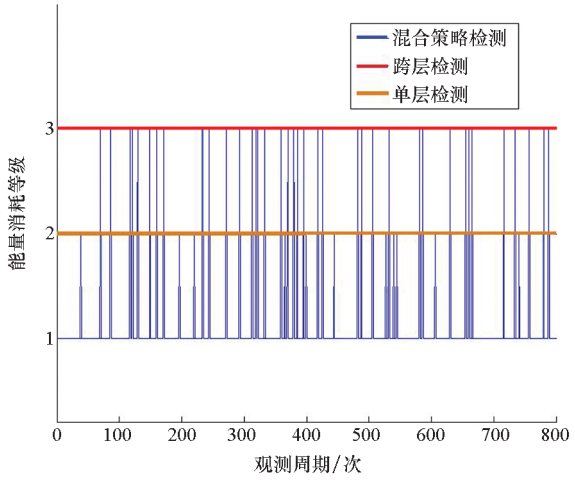

图4 能量消耗分析

Fig. 4 Analysis of energy consumption

3 结论

本文从协议层攻击的角度构建了非合作完全信息重复博弈模型，以检测无线自组织网络中的跨层攻击。在此模型的基础上，分析了博弈双方支付函数的策略空间，计算了混合策略纳什均衡解。在无线自组织网络仿真平台上对模型的性能进行了仿真分析。仿真结果表明，检测者在采用混合策略的情况下，其检测概率高于仅使用单层检测或跨层检测的情况，而且在采用混合策略情况下节点的能量消耗要显著低于仅使用单层检测或跨层检测的情况。下一步将在真实的无线自组织网络中开展实验，分析模型在实际环境中的性能。

参考文献(References)

[1] WOOD A D, STANKOVIC J A. Denial of service in sensor networks[J]. Computer, 2002, 35(10): 54 – 62.

[2] RAYMOND D R, MARCHANY R C, BROWNFIELD M I, et al. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols [J]. IEEE Transactions on Vehicular Technology, 2009, 58(1): 367 – 380.

[3] RADOSAVAC S, CÁRDENAS A A, BARAS J S, et al. Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: robust strategies against individual and colluding attackers[J]. Journal of Computer Security, 2007, 15: 103 – 128.

[4] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: attacks and countermeasures [J]. Ad Hoc Networks, 2003, 1: 293 – 315.

[5] RADOSAVAC S, BENAMMAR N, BARAS J. Cross-layer attacks in wireless ad hoc networks [C]//Proceedings of Conference on Information Science and Systems, 2004: 1266 – 1271.

[6] BIAN K G, PARK J M, CHEN R L. Stasis trap: cross-layer stealthy attack in wireless ad hoc networks[C]//Proceedings of IEEE Global Telecommunications Conference, 2006.

[7] NAGIREDDYGARI D, THOMAS J. MAC-TCP cross-layer attack and its defense in cognitive radio networks [C]// Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 2014: 71 – 78.

[8] WANG W K, SUN Y, LI H S, et al. Cross-layer attack and defense in cognitive radio networks[C]//Proceedings of IEEE Global Telecommunications Conference, 2010.

[9] HOSSAIN M, XIE J. Off-sensing and route manipulation attack: a cross-layer attack in cognitive radio based wireless mesh networks [C]//Proceedings of IEEE Conference on Computer Communications, 2018: 1376 – 1384.

[10] HASAN K, SHETTY S, OYEDARE T. Cross layer attacks on GSM mobile networks using software defined radios [C]// Proceedings of 14th IEEE Annual Consumer Communications & Networking Conference, 2017: 357 – 360.

[11] WANG J, FAPOJUWO A O, ZHANG C, et al. UML modeling of cross-layer attack in wireless sensor networks [C]// Proceedings of Interoperability, Safety and Security in IoT, 2017: 104 – 155.

[12] HAN Z J, WANG R C. Intrusion detection for wireless sensor network based on traffic prediction model [J]. Physics Procedia, 2012, 25: 2072 – 2080.

[13] ALAPARTHY V T, MORGERA S D. A multi-level intrusion detection system for wireless sensor networks based on immune theory[J]. IEEE Access, 2018, 6: 47364 – 47373.

[14] BAO F Y, CHEN I R, CHANG M J, et al. Trust-based intrusion detection in wireless sensor networks [C]// Proceedings of IEEE International Conference on Communications, 2011.

[15] LUO W, MA W P, GAO Q. A dynamic trust management system for wireless sensor networks [J]. Security and Communication Networks, 2016, 9: 613 – 621.

[16] SANDHYA G, JULIAN A. Intrusion detection in wireless sensor network using genetic K-means algorithm [C]// Proceedings of IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014: 1791 – 1794.

[17] GEETHA S, DULHARE U N, SIVATHA SINDHU S S. Intrusion detection using NBHoeffding rule based decision tree for wireless sensor networks [C]//Proceedings of Second International Conference on Advances in Electronics, Computers and Communications, 2018.

[18] OTOUM S, KANTARCI B, MOUFTAH H T. On the feasibility of deep learning in sensor network intrusion detection [J]. IEEE Networking Letters, 2019, 1(2): 68 – 71.

[19] CHEN L, LENEUTRE J. A game theoretical framework on intrusion detection in heterogeneous networks [J]. IEEE Transactions on Information Forensics and Security, 2009,

4(2): 165 – 178.

[20] LIU Y, COMANICIU C, MAN H. A Bayesian game approach for intrusion detection in wireless ad hoc networks[C]// Proceedings of the Workshop on Game Theory for Communications and Networks, 2006.

[21] MOOSAVI H, BUI F M. A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(9): 1367 – 1379.

[22] GUAN S H, WANG J J, JIANG C X, et al. Intrusion detection for wireless sensor networks: a multi-criteria game approach[C]//Proceedings of IEEE Wireless Communications and Networking Conference, 2018.

[23] WANG J, JIANG S, FAPOJUWO A O. A protocol layer trust-based intrusion detection scheme for wireless sensor networks[J]. Sensors, 2017, 17(6): 1227.

[24] DALLAS D, LECKIE C, RAMAMOHANARAO K. Hop-count monitoring: detecting sinkhole attacks in wireless sensor networks[C]//Proceedings of 15th IEEE International Conference on Networks, 2007: 176 – 181.

[25] RADOSAVAC S, BARAS J S, KOUTSOPOULOS I. A framework for MAC protocol misbehavior detection in wireless networks[C]//Proceedings of the 4th ACM Workshop on Wireless Security, 2005: 33 – 42.