以网络性能为核心的移动自组网 Flooding 攻击防御技术

王 伟[1] 王嘉郡[2] 王明明[1] 张文静[2] 陈金广[1]
(西安工程大学计算机科学学院 西安 710048)[1] (厦门大学软件学院 厦门 361005)[2]

摘 要 移动自组网(Mobile Ad Hoc Networks,MANETs)所面临的 Flooding 攻击是一种严重 DOS 攻击行为。然而,现有的针对 Flooding 攻击的防范技术因不能较好地适应 MANETs 特性(如有限资源、动态拓扑等)而难以在 MANETs 网络性能和网络安全之间保持平衡。通过分析移动自组网的时空动态性、网络性能评估与 Flooding 安全威胁之间的内在关系,提出了一种基于性能评估的 Flooding 攻击防御技术。通过构建可量化的 MANETs 安全威胁、防御收益与代价的评估指标体系,实现了基于网络安全和性能平衡的防御及其性能优化方法。仿真实验结果表明,所提出的防御技术可有效地弥补现有移动自组网安全技术存在的一些缺陷,因而能够满足移动自组网特性且适合于实际应用。

关键词 移动自组网,Flooding 攻击,性能评估,时空动态性,安全威胁
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.01.031

Defense Technology Based on Dynamic Space-Time Performance for Flooding Attacks in Mobile Ad Hoc Networks

WANG Wei[1] WANG Jia-jun[2] WANG Ming-ming[1] ZHANG Wen-jing[2] CHEN Jin-guang[1]
(School of Computer Science,Xi'an Polytechnic University,Xi'an 710048,China)[1]
(School of Software,Xiamen University,Xiamen 361005,China)[2]

Abstract Flooding attacks is a kind of seriously harmful DOS attack in mobile Ad Hoc networks. However,the existing researches on security defense for flooding attacks are almost unfit for the characteristics (such as limited resource,dynamic topology) in Ad Hoc networks,and couldn't keep the balance between network performance and network security. On the basis of analysis of the inherent relations among space-time dynamic properties,network performance evaluation and security threatens,a defense technology based on performance evaluation for Flooding attacks in mobile Ad Hoc networks was presented. With the measurable system evaluation indexes for security threaten,defense income and cost,the mechanism of making defense policies and optimizing defense performance is achieved in the proposed system. Simulation results show that the proposed defense technology can overcome a good many drawbacks in the existing security technologies for mobile Ad Hoc networks. Consequently,the proposed technology can meet the network properties and actual application of mobile Ad Hoc networks.

Keywords Mobile Ad Hoc networks,Flooding attacks,Network performance evaluation,Space-time dynamics,Security threatens

1 前言

移动自组网(MANETs)可广泛地用于军事通信、灾难救助和临时紧急会议等领域。MANETs 没有基站或中心节点,其网络拓扑动态变化,节点间通过较差的无线信道相连,带宽、能源等网络资源有限,这些固有特性不但使 MANETs 无法应用有线网络中已有的一些安全机制(如访问控制、防火墙等),而且使 MANETs 更易遭受各种安全威胁。其中,Flooding攻击是 MANETs 面临的一种严重 DOS 攻击行为[1],它一般针对 MANETs 的按需路由协议(如 AODV,DSR 等)来实施,可导致 MANETs 网络性能显著下降。Li 等人[2]对 MANETs 中的 Flooding 攻击的研究显示,一个和多个攻击节点可分别使网络的丢包率达 25%和 60%以上。

在 MANETs 的按需路由协议 AODV[3]中,当源节点需要向目的节点发送数据但它们之间尚未建立路由时,源节点就向网络广播路由请求包 RREQ。尽管 AODV 可通过参数来限制 RREQ 数量,但恶意节点可突破该限制而产生 Flooding攻击:1)RREQ Flooding,攻击者随机选择 IP 作为路由查询地址,并连续发送大量 RREQ;2)DATA Flooding,通过建立到所有节点的路由,发送大量无用数据。Flooding 攻击不

到稿日期:2015-11-07 返修日期:2016-03-26 本文受陕西省教育厅专项科研计划(15JK1317),自然科学基金青年项目(61201118),自然科学基金面上项目(61175039)资助。

王 伟(1969-),男,博士后,主要研究方向为网络信息安全、移动自组网技术,E-mail:wangwxjt@xjtu.edu.cn;王嘉珺(1993-),女,硕士生,主要研究方向为并行算法与软件优化;王明明(1982-),男,博士,讲师,主要研究方向为量子密码;张文静(1989-),女,博士生,主要研究方向为无线网络安全;陈金广(1977-),男,博士,副教授,主要研究方向为目标跟踪等。

但使有限带宽被占用，还使受害节点疲于接收攻击报文，难以进行正常通信。

对此，尽管人们已提出了一些方案，但它们仍然存在一些缺点：1)大都专注于安全问题本身，缺乏对网络性能的有效评估；2)需要节点间进行大量协作，但过多地消耗资源以及系统自身缺乏量化的安全评估导致其难以在网络性能和网络安全间保持平衡[4]。网络性能(如时延、丢失率等)作为评估网络 QoS 和优化网络资源的依据，可为网络安全提供预警手段。近年国外学者提出了网络断层扫描(Network Tomography，NT)[5]理论，根据网络端到端(E2E)测量来推测网络内部链路性能，无需网络内部节点协作但能节约网络资源，这为资源有限的 MANETs 网络性能评估和安全监控提供了理论基础。

本文针对 MANETs 网络的 Flooding 攻击，在分析 MANETs 链路的时空动态性的基础上，应用 NT 技术理论框架，提出了网络性能与网络安全量化评估指标体系，实现了一种以网络性能为核心的移动自组网 Flooding 攻击防御技术。

2 相关工作

目前，国内外学者针对 MANETs 网络的 Flooding 攻击主要从安全路由协议设计、入侵检测与安全响应、安全防范 3 个方面进行了初步研究。

2.1 安全路由协议

针对现有 MANETs 路由协议缺陷，人们已进行大量研究[6]。Kataria 等人[7]针对 AODV 缺陷，从公平地转发真实 RREQ 包与虚假 RREQ 包的角度，提出抑制虚假 RREQ 包洪泛。Ahmad 等人[8]对 DSR 提出改进，通过延迟到源节点的 RREP 包，减少源于不同节点 RREP 包的洪泛。而 Gopalakrishnan 等人[9]对识别攻击节点的安全路由协议进行了研究，利用目的节点检查源节点的阈值是否变化，检测数据包在传输中是否被篡改。然而，这些研究仍有缺陷[6]：1)大都针对特定攻击场景或路由，仅在有限程度上抑制 Flooding，很难对攻击进行早期检测和隔离；2)需要引入复杂密钥管理机制、加解密算法或协议，但消耗过多网络资源；3)安全协议本身无法克服来自网络内部的攻击。

2.2 入侵检测与安全响应

国内外学者也对 MANETs 的入侵检测与安全响应进行了初步研究[10]，它们可分为以下两种类型。

2.2.1 分布式协作 IDS

这种 IDS 适用于平面结构的 MANETs，网络中的每个节点都部署了 IDS Agent，不但要进行本地检测，还要参与网络全局检测。Zhang 等人[11]首先提出了基于 Agent 分布式协作的入侵检测框架，每个节点的 IDS Agent 独立完成本地检测，全局检测由各节点的 Agent 协作完成。而 Leila 等人[12]采用移动 Agent 技术来构建分布式协作的 IDS 框架，通过各节点的 IDS 进行本地检测，通过相互协作实现全局检测。其不足在于每个网络节点都要运行 Agent，开销大，扩展性差。Wang 等人[13]利用社会网络分析法构建了一种分布式协作 IDS，相对于异常检测它在计算复杂度上有优势，但节点间交换审计数据导致通信负载增大。张晓宁等人[14]提出基于模糊行为分析的 IDS，引入模糊路由行为分析方法降低误报率，但负载较大，且仅适用于 DSR。

2.2.2 分层 IDS

这种 IDS 适用于分层结构的 MANETs，是对分布式协作 IDS 的扩展。Yi 等人[15]提出一种分布式入侵检测方法，它将整个网络划分为若干区域，各区域随机且周期性地选出簇首进行监视并收集簇内节点信息，利用时间自动机确定入侵者。尽管它能实时检测入侵，但仅适于 AODV 协议。Marchang 等人[16]提出独立于任何路由协议的 IDS，簇内节点相互监听对方，利用协作消息传递机制将监听结果发送给检测节点，由簇首诊断入侵者。类似地，Otrok 等人[17]提出基于博弈论的分级 IDS。这些方案可检测到簇首的恶意行为，但簇首的产生和维护会带来额外负载。Manousakis 等人[18]提出了一种基于动态树结构的分级 IDS，检测信息是根节点聚合了源于各叶节点的审计信息，这在高度动态环境下具有鲁棒性，也可提高检测准确性，但构建和维持树结构会增加额外处理和通信负载。此外，如果簇首被攻陷，将给系统带来致命的安全威胁。

2.3 Flooding 攻击的防范

对于 Flooding 攻击的防御，存在以下 3 种方法。

2.3.1 基于速率限制的方法

EU Zhiang 等人[19]对 AODV 中的 Flooding 攻击提出了防御机制，网络各节点监视并计算其邻居 RREQ 发送速率，一旦发现其超过阈值，就将它加入黑名单，并丢弃其数据包。类似地，Yi 等人[20]针对 AODV 协议中的 Flooding 提出了缓解方法，利用统计分析检测并阻止 RREQ Flooding 攻击。这些方法存在缺点：1)不能阻止低于阈值的攻击；2)若攻击者冒充合法节点，会导致后者被误认为是攻击者。

2.3.2 基于信任或信誉值的方法

Shandilya 等人[21]提出一种基于节点间友好程度的信任方法，让节点进行协作并阻止 RREQ Flooding。由于信誉值是按照节点参与网络协作的程度来估计的，这在一些特定场景(如“孤岛”)下易造成误报。

2.3.3 基于节点行为的方法

Bhuvaneshwari 等人[22]提出一种基于流量模式的动态轮廓检测技术，通过检测引擎来检测 Flooding 攻击行为，攻击者会被其一跳邻居节点隔离。但该方法从训练数据所得到的节点流量轮廓往往是静态的，在动态的网络环境下会出现较大误差。

3 Flooding 攻击防御系统

本系统包括网络性能评估、Flooding 攻击检测和防御 3 部分，分别采用 NT Agent、攻击检测 Agent 和攻击防御 Agent 来实现，如图 1 所示。

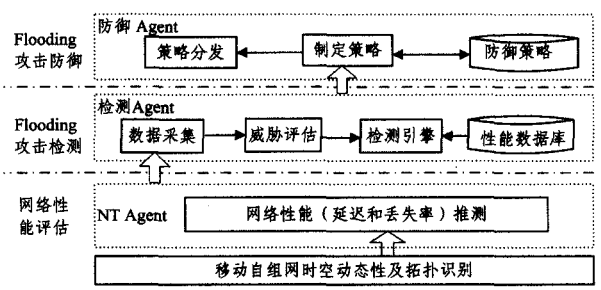

图 1 系统模型

上述 Agent 实现的系统功能分别包括：依据网络时空动态特性识别网络拓扑；采用网络外部测量机制，评估移动自组网内部链路性能参数；建立基于网络性能的分布式入侵检测及防御系统。其中，检测 Agent 和防御 Agent 驻留在每个节点，默认处于睡眠状态，检测和防御时由 NT Agent 唤醒。

3.1 系统假设

系统假设：1)网络是由 N 个移动节点($n_1, n_2, \cdots, n_N$)组成，它们具有相同无线覆盖半径 r_n，并按照移动模型在一个有限二维矩形区域 Ω 内移动；2)在系统运行中，正常节点都能够保持时钟同步，这可利用 GPS 和 CDMA 等外部时钟源实现；3)系统自身安全可使用现有认证机制[23]，无论新节点加入还是 Agent 执行，都要先经过认证；4)为增强攻击效果，攻击节点在靠近 Ω 中心的区域移动，因为这样可与更多节点建立连接。

3.2 MANETs 时空动态性及其识别

依据报文在网络中传输的逻辑关系，本文用逻辑拓扑 $\Psi(t)$来揭示 MANETs 在任意时刻 t 的时空动态性。本质上，如果一个源节点向多个目的节点发送数据包，$\Psi(t)$就是一个倒立树，数据包从根节点到达 $\Psi(t)$内分叉节点时分离，并沿各自的路径到达叶子节点。而 $\Psi(t)$是由逻辑链路(即 $\Psi(t)$中两个相邻节点在逻辑上是连通的)组成的。$\Psi(t)$在 t 时刻的逻辑链路集合用 $L(t)$表示，其中任一逻辑链路可包含多条物理链路。逻辑链路在空间上体现了 $\Psi(t)$逻辑连通性，在时间上则表现为网络拓扑的生存期[24]，即网络拓扑在时刻 t 具有逻辑上的相对稳定期(即 $LT(t)$)。因此，MANETs 的时空动态特性可用式(1)描述。

$$\Psi(t)=\tau(V,L(t),LT(t)) \tag{1}$$

其中，V 表示网络节点集。如果不考虑节点电能、环境等物理因素，$\Psi(t)$的时空连通性主要由节点间的时空动态邻接关系决定。显然，MANETs 在时刻 t 的网络拓扑识别就是获得网络节点在时刻 t 的空间邻接关系。

对于任意节点 n_i 和 n_j，假设它们在 t 时刻的坐标分别为 $(x_i(t), y_i(t))$和$(x_j(t), y_j(t))$，当其欧氏距离 $d_{ij}(t)=\sqrt{(x_i(t)-x_j(t))^2+(y_i(t)-y_j(t))^2}\leqslant r_n$ 时，它们就可建立无线链路 $l_{ij}(t)(l_{ij}(t)\in L(t))$，它们在空间邻接关系上互为一阶邻居。因此，$n_i$ 的一阶邻居节点集表示为：

$$V_{n_i}^1(t)=\{n_j\in V\}_{i\neq j;(i,j)\in N} \tag{2}$$

不失一般性，假设节点 $n_k(i\neq j\neq k$ 且$(i,j,k)\in V)$满足 $n_k\in V_{n_j}^1(t)$，则 n_k 是 n_i 的二阶邻居节点，即 $n_k\in V_{n_i}^2(t)$。同理，可得在 t 时刻 n_i 的所有不同阶邻居节点集：

$$V_{n_i}^{\theta}(t)=\{n_k\in V\backslash\bigcup_{\mu=1}^{\theta-1}V_{n_i}^{\mu}(t)\} \tag{3}$$

其中，θ 和 μ 均为正整数，且 $1\leqslant\mu<\theta<N$。因此，MANETs 网络拓扑 $\Psi(t)$的时空动态连通性可表示为：

$$V_{(*)}(t)=\{\bigcup_{i}^{N}V_{n_i}^{\theta}(t)\} \tag{4}$$

3.3 MANETs 性能评估指标

这里将数据包从 $\Psi(t)$根节点到达各叶子节点所经路由矩阵表示为 $A_{\Psi(t)}=(a_{ij}^{\Psi(t)})_{m\times n}$，其中 $a_{ij}^{\Psi(t)}\in\{0,1\}$表示数据包所经路径和链路在 $\Psi(t)$中的逻辑关系。若数据包所经路径 i 包含链路 j，$a_{ij}^{\Psi(t)}=1$；否则，$a_{ij}^{\Psi(t)}=0$。显然，数据包从根节点到达叶节点的路径性能(丢失率和延迟)是由其所含链路性能累积而成。

根据识别的 $\Psi(t)$，在 $LT(t)$期间，从 $\Psi(t)$根节点沿路径 i 向叶节点发送 N 个数据包，如果用 Y_i 表示该路径丢失或延迟性能参数，用 X_j 表示链路 j 丢失或延迟指标，则有：

$$Y_i=\sum_{j\in i}X_j \tag{5}$$

文献[25,26]提出利用累积生成函数(CGF)数学方法对传感器网络和有线网络链路性能进行估计。本文将 CGF 扩展到 MANETs 性能估计中，但与上述文献存在根本不同：1)将时空动态性分析技术与 CGF 数学方法相结合，把 CGF 从简单的宏观应用扩展到复杂的微观应用领域；2)将延迟和丢失率结合起来应用 CGF，实现了从一维性能空间扩展到多维性能空间，因而可对网络性能进行更全面的评估。

假设 $\Psi(t)$中各链路丢失率和延迟相独立，类似的假设见文献[27]。不失一般性，定义 $\Psi(t)$中 E2E 路径 i 的性能 CGF 为：

$$K_{Y_i}^{\Psi(t)}=\log E[e^{sY_i}] \tag{6}$$

其中，参数 $s\in(-\infty,+\infty)$。路径 i 中链路 j 的性能 CGF 为：

$$K_{X_{j(i)}}^{\Psi(t)}=\log E[e^{sX_{j(i)}}] \tag{7}$$

事实上，由于路径 i 往往是由一系列链路 j 组成的(即 $j\in i$)，结合式(6)、式(7)可得：

$$\begin{aligned}K_{Y_i}^{\Psi(t)}&=\log E[e^{sY_i}]=\log E[e^{s(\sum_{j\in i}X_{j(i)})}]\\&=\log\{\prod_{j\in i}E[e^{sX_{j(i)}}]\}=\sum_{j\in i}\log E[e^{sX_{j(i)}}]\\&=\sum_{j=1}^{n}a_{ij}^{\Psi(t)}\cdot K_{X_{j(i)}}^{\Psi(t)}(s)=A_{\Psi(t)}^{(i)}\cdot K_{X(i)}^{\Psi(t)}(s)\end{aligned} \tag{8}$$

其中，$A_{\Psi(t)}^{(i)}$为矩阵 $A_{\Psi(t)}$的第 i 行，$K_{X(i)}^{\Psi(t)}(s)=[K_{X_1(i)}^{\Psi(t)}(s),K_{X_2(i)}^{\Psi(t)}(s),\cdots,K_{X_n(i)}^{\Psi(t)}(s)]^{\mathrm{T}}$。因此，$\Psi(t)$中根节点到所有叶节点的 E2E 路径 CGF 表示为向量 $K_Y^{\Psi(t)}(s)=[K_{Y_1}^{\Psi(t)}(s),K_{Y_2}^{\Psi(t)}(s),\cdots,K_{Y_n}^{\Psi(t)}(s)]^{\mathrm{T}}$，简化为：

$$K_Y^{\Psi(t)}(s)=A_{\Psi(t)}K_X^{\Psi(t)}(s) \tag{9}$$

在 $\Psi(t)$中，选取 n 个目的节点和 n 条链路，可使 $A_{\Psi(t)}$成为满秩矩阵。其中，$K_X^{\Psi(t)}(s)=\int_{-\infty}^{+\infty}e^{sx}p_X(x)\mathrm{d}x$ 与随机变量 X 的概率密度分布 $p_X(x)$一一对应。这样，通过 $K_Y^{\Psi(t)}(s)$来推断 $K_X^{\Psi(t)}(s)$可获得链路性能分布特征。这里，链路性能 CGF $K_X^{\Psi(t)}(s)$由 E2E 路径 CGF $K_Y^{\Psi(t)}(s)$确定，即：

$$K_X^{\Psi(t)}(s)=(A_{\Psi(t)}^{\mathrm{T}}A_{\Psi(t)})^{-1}K_Y^{\Psi(t)}(s) \tag{10}$$

令矩阵 $B^{\Psi(t)}=(A_{\Psi(t)}^{\mathrm{T}}A_{\Psi(t)})^{-1}A_{\Psi(t)}^{\mathrm{T}}$，则有：

$$K_{X_{j(i)}}^{\Psi(t)}(s)=\sum_{i=1}^{n}b_{ji}^{\Psi(t)}K_{Y_i}^{\Psi(t)}(s) \tag{11}$$

其中，$b_{ji}^{\Psi(t)}$表示矩阵 $B^{\Psi(t)}$的第 j 行的第 i 列元素。

由于上述链路性能的 CGF 保留了 MANETs 网络链路性能统计信息，因此可利用 CGF 估算性能参数分布的多项特性来推测该路径上的各链路延迟或丢失率分布特征，进一步可为异常检测和攻击定位提供依据。

3.4 可量化的 Flooding 攻击威胁评估指标

本系统从局部节点和全局网络两个层次对 Flooding 攻击进行全面的量化评估，以获得准确的安全威胁程度。

3.4.1 局部节点的安全威胁指数

在 MANETs 中，$\Psi(t)$中任意节点 n_i 因资源消耗、主动或被动的攻击都可使 n_i 所在链路的性能产生威胁，其程度的大小用 $I_{n_i_ST}(t)$表示。对于 n_i，在 t 时刻的安全威胁程度由式(12)量化评估：

$$I_{n_i\_ST}(t)=f(\vec{P}_i(t),W_i(t))=W_i(t)\cdot\vec{P}_i(t) \tag{12}$$

其中，$\vec{P}_i(t)$是 n_i 所在链路对网络的威胁向量；$W_i(t)$是 n_i 在 t 时刻对网络连通的权重，即 n_i 越靠近 Ω 中心，会以更大的概率与其他节点建立连接，从而对网络连通性有更大贡献。$I_{n_i_ST}(t)$值表明了 n_i 所在链路安全威胁程度的大小。

如果用 O 表示 Ω 的中心，Ω 的 4 个顶点距离 O 的半径用 R 表示，将 t 时刻 n_i 到 O 的欧氏距离 $d_i(t)=\sqrt{x_i^2(t)+y_i^2(t)}$ 在 R 上归一化，以量化 n_i 的权重 $W_i(t)$。当发生 Flooding 攻击时，$\vec{P}_i(t)$量化评估如下：

$$\vec{P}_i(t)=\vec{\sigma}_i\cdot f(\vec{D}_i(t),\vec{L}_i(t))=\vec{\sigma}_i\cdot(u\vec{D}_i(t)+v\vec{L}_i(t)) \tag{13}$$

其中，$\vec{\sigma}_i=(\sigma_{i1},\sigma_{i2},\cdots,\sigma_{ik})$是 $\Psi(t)$中 n_i 转发的业务流；向量 $\vec{D}_i(t)=(d_{i1},d_{i2},\cdots,d_{ik})$和$\vec{L}_i(t)=(l_{i1},l_{i2},\cdots,l_{ik})$分别表示 n_i 所在链路给不同目的节点转发业务数据流的性能量化值，其大小由网络性能推测获得；u 和 v 分别表示该链路性能的归一化指标，取决于实际应用中不同业务数据流对不同性能参数的敏感程度。

3.4.2 全局网络的安全威胁指数

它描述了 MANETs 在 t 时刻受到 Flooding 攻击时$\Psi(t)$整体遭受的安全威胁程度，用 $I_{N_ST}(t)$表示。注意，$I_{N_ST}(t)$和 $I_{n_i_ST}(t)$分别是从网络全局和链路局部来量化安全状况，二者的关系密切，即前者随后者的增大而增大。

在任意时刻 t，系统以 $LT(t)$作为评估的时间窗口来量化 $\Psi(t)$在此期间遭受 Flooding 攻击的威胁程度：

$$\begin{aligned}I_{N\_ST}(t)&=f(\vec{I}_{n_i\_ST}(t),\vec{W}_{n_i}(t))\\&=\vec{W}_{n_i}(t)\cdot\vec{I}_{n_i\_ST}(t)\\&=\sum_i^N W_i(t)\cdot\vec{P}_i(t)\end{aligned} \tag{14}$$

其中，$I_{n_i_ST}(t)$由式(12)确定，$\vec{W}_n(t)=(W_1(t),W_2(t),\cdots,W_N(t))$是 t 时刻各节点在 Ω 内的位置权重指数。

3.5 Flooding 攻击的检测和定位机制

3.5.1 链路性能特征轮廓的学习算法

系统综合延迟和丢失率两个性能指标对 Flooding 攻击进行检测和防御。为此，先建立网络内部链路性能特征的活动轮廓。在链路性能分布特征推测的基础上，采用 SOM[28] 神经网络方法，通过输入移动节点的日志数据来学习链路性能特征，并训练 SOM 网络神经元，以捕获链路性能的分布特征，从而构建与链路性能分布一致的性能权重向量空间。算法如下：

(1)初始化。为 SOM 输出层的每个神经元权重 w_{ij} 赋初值，$w_{ij}\in[0,1]$表示 SOM 中第 j 个神经元在第 i 个链路性能向量中的映射位置；给定学习速率初始值 $\varphi(0)$；确定学习次数 S。

(2)输入 t 时刻 $\Psi(t)$中链路 $\ell_i(\ell_i\in L(t))$的一组性能数据样本 $X_{\ell_i}=[x_1,x_2,\cdots,x_n]^T$，其中 x_i 介于 0 和 1 之间，依赖于链路性能数据的观测样本中第 i 个数据样本。

(3)计算神经元权重 w_{ij} 和权重向量 $W_j=[w_{j1},x_{j2},\cdots,x_{jn}]^T$ 之间的欧氏距离，寻找权重向量与输入向量最近的神经元，竞争获胜神经元通过式(15)获得：

$$d_j=\arg\min\|X-W_j\| \tag{15}$$

其中，$j=1,2,\cdots,n$(n 是神经元的所有邻居节点数)。

(4)按照式(16)所示函数对所有获胜神经元及其邻居神经元的权重进行调整：

$$w_{ji}(\delta+1)=\begin{cases}w_{ji}(\delta)+\varphi(\delta)[x_i(\delta)-w_{ji}(\delta)], & \text{for each } j\in N_c(\delta)\\ w_{ji}(\delta), & \text{otherwise}\end{cases} \tag{16}$$

其中，δ 是网络链路性能测量的时间窗口值 $LT(t)$，它在每个学习过程中按照递增规律变化；$N_c(\delta)$为迭代期间邻居节点之间的半径；$x_i(\delta)$代表第 τ 个迭代期间选定的输入向量；$w_{ji}(\delta)$和 $w_{ji}(\delta+1)$分别是 δ 和 $\delta+1$ 两个迭代期间以获胜神经元为中心的权重调整范围；$\varphi(\delta)$是学习速率。

(5)重复步骤(2)—步骤(4)，直到 $\delta=S$ 为止，得到 S 批次学习的 SOM 网络。

3.5.2 异常链路的检测和定位

得到 $\Psi(t)$各链路性能轮廓后，就可将推测的链路延迟和丢失率($X_{LT(t)}$)分别与其对应的性能轮廓相比较：若超出阈值，则该链路是异常链路。由于一条逻辑链路往往包含多条物理链路，还需要对异常节点进行准确定位。为提高算法性能，先对性能数据进行量化处理：在 τ 时间窗口，假设链路 ℓ_i^τ 性能参数值在性能量化空间$\{0,u,2u,\cdots,ju,\cdots,Bu\}$($u$ 表示性能单位值，B 是性能最大量化值)中属于 ju 的概率是 $X_{i(j)}^\tau$，而该链路性能分布概率估计值是$\hat{X}_{i(j)}^\tau$，如图 2 所示。

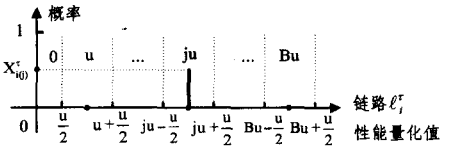

图 2 链路性能参数值在其量化空间上的概率

则 ℓ_i^τ 的性能参数在量化空间上的总估计误差 E_i^τ 为：

$$E_i^\tau=\sum_j^B|X_{i(j)}^\tau-\hat{X}_{i(j)}^\tau| \tag{17}$$

如果 $E_i^\tau>E_i^{th}$(E_i^{th} 是 ℓ_i^τ 上的性能误差阈值)，则 ℓ_i^τ 就是异常链路，ℓ_i^τ 上所有节点均为可疑节点(包含了正常节点和攻击节点)，其原因在于：根据 3.2 节的定义，ℓ_i^τ 可能包含多个物理链路(节点)，因此可用集合 $N_i^{pro}(t)$表示，其中真正的攻击节点用集合 $N_i^{atk}(t)$来表示($N_i^{atk}(t)\subseteq N_i^{pro}(t)\subset V$)。同理，对于 $\psi(t)$中所有异常链路上的可疑节点而言，对它们同时进行交集运算来进行攻击节点的判定，因为所有 Flooding 攻击节点的共性就是它们所在的链路充斥了大量攻击报文，即所有攻击节点所在的链路均存在性能异常的特点。如果用集合 $N^{atk}(t)$来表示 t 时刻检测到的所有攻击节点，则有：

$$N^{atk}(t)=\bigcap_{i=0}^N N_i^{pro}(t) \tag{18}$$

将式(17)、式(18)相结合，就可检测到网络在 t 时刻的所有攻击节点。接着，系统对不同时刻 t 所检测到的攻击节点进行并集运算，可在 MANETs 整个运行期间 T 检测到进行 Flooding 攻击的节点，用集合 N^{atk} 表示，那么：

$$N^{atk}=\bigcup_{t=0}^T N^{atk}(t) \tag{19}$$

由于系统对网络链路性能和安全威胁评估前就利用了 3.2 节的方法对网络所有节点的时空动态性进行了识别，因此由式(19)所得的攻击节点就可被准确地定位。

3.6 Flooding 攻击的防御及其优化方法

考虑到攻击节点的移动性，利用防御 Agent 的移动性实行黑名单操作，达到全网隔离。具体地，对 Flooding 攻击的

防御就是在攻击节点 n_i 的一阶邻居节点集 $V_{n_i}^1(t)$ 上实施阻拦和隔离。在一跳范围内对攻击节点进行防御，可以有效地阻止攻击流量在网络范围内扩散[19,22]。相对于电能、CPU 等资源，$\Psi(t)$ 对无线链路带宽消耗更敏感[29]，因此防御策略以消耗带宽作为衡量对攻击防御的代价，以提高全局网络吞吐量作为对攻击进行防御的收益。

从局部链路看，部署防御策略后该链路的性能可能有所下降，但从全局看，需要提高整个网络吞吐量。因此，有效的安全防御应以较小的代价（安全系统通信量）来获取较高的收益（网络业务吞吐量）。为此，提出防御的收益-代价比 $I_{G\_C}(t)$ 来量化评估系统对 Flooding 攻击的防御效果。

$$I_{G\_C}(t)=f(Th(t),Th^*(t),\delta_{sys}(t))$$
$$=(Th^*(t)-Th(t))/\delta_{sys}(t) \quad (20)$$

其中，$Th(t)$ 和 $Th^*(t)$ 分别表示防御策略实施前、后 $\Psi(t)$ 的吞吐量，可由网络所有节点成功接收的数据包统计获得；$\delta_{sys}(t)$ 表示某一防御策略实施后在 $\Psi(t)$ 中产生的通信流量，由所有节点上 Agent 间的通信统计获取。显然，收益-代价比值越大，防御策略所产生的防御效果越好。

在理想情况下，系统对 Flooding 攻击的防御应以最小代价（即 $\delta_{sys}(t)$ 最小，但总大于 0）使网络整体的安全威胁降到最低（即式(14)中的 $I_{N\_ST}(t)$ 最小，其理想值为 0）。然而，由于 MANETs 自身的复杂特性，这种理想目标在实际应用中一般很难达到。为此，从优化角度考虑，本系统在防御 Flooding 攻击时使得 $\delta_{sys}(t)$ 最小（即 $I_{G\_C}(t)$ 最大），同时使得 $I_{N\_ST}(t)$ 尽可能小（实际难以保证网络绝对安全）。这样，系统在防御 MANETs 的 Flooding 攻击时可实现 MANETs 网络安全和网络性能之间的平衡。

4　实验结果及其分析

4.1　仿真实验环境

实验平台为 Pentium4 1.8GHz，512MB RAM，操作系统为 Windows XP，并采用 NS2[30] 作为仿真实验的工具，基本的仿真环境及其相关参数如表 1 所列。

表 1　仿真环境和参数设置

参数	取值	
	场景 1	场景 2
Channel	Wireless Channel	
Mac	802.11	
Antenna	OmniAntenna	
IFQ Length	50	
Route Protocol	AODV(DSR)	
Nodes	30	200
Speed (m/s)	2～12	
Pause time (s)	1～5	
Mobility model	Random Waypoint	
Movement area (m^2)	1000 * 1000	

本系统提出的网络链路性能特性的评测及 Flooding 攻击检测和防御集成在 NS-2 中进行实验。需要注意，系统本身与具体路由协议无关[31]，因而可适用于任何路由协议下的 Flooding 攻击。限于篇幅，实验以最常用的 AODV 为例。

通过修改 AODV，两种场景分别选择 2 个和 44 个 Flooding攻击节点。为加大检测和防御难度，随机选择攻击节点、受害节点、数据包大小及发送时间。攻击每秒发送 10 个 RREQ 包或 DATA 包。

4.2　实验结果及其分析

4.2.1 网络性能的评估

Flooding 攻击节点的存在必然导致 MANETs 网络性能显著恶化。为了对攻击进行检测和防御，本系统首先获得网络链路性能参数的分布函数。这里分别以两种场景下的攻击节点所在链路 l_{13} 和 l_{53} 为例，采用仿真统计直接计算 l_{13} 与 l_{53} 的延迟 CGF 和丢失率 CGF，同时应用 E2E 统计数据分别推测它们相应的性能 CGF，结果如图 3、图 4 所示。

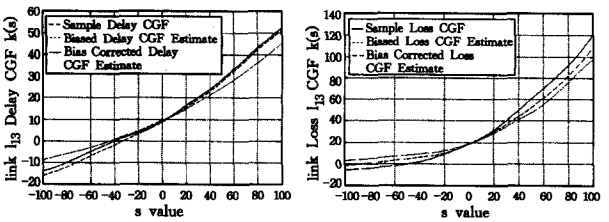

图 3　场景 1 中异常链路 l_{13} 的延迟（左图）和丢失率（右图）CGF

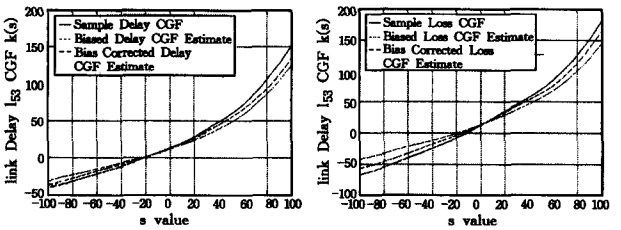

图 4　场景 2 中异常链路 l_{53} 的延迟（左图）和丢失率（右图）CGF

从图 3、图 4 可看出，系统在不同场景下推测的 CGF 与实际 CGF 很接近。相对于有偏估计，无偏估计明显更精确。因此，本文提出的链路性能推测算法所得结果能够较好地与实际性能保持一致。

4.2.2　攻击节点的检测和识别

系统对网络异常节点的检测和识别是通过链路性能的推测值与 SOM 算法学习得到的真值的比较来实现的，即二者之差是否超过事先设定的阈值 E_T^{th}（取 0.9）。算法在每个时间窗口下将收集的数据包进行预处理，采用简化的五元组{根节点 *ID*，源节点 *ID*，接收节点 *ID*，延迟，丢失率}作为特征向量，并输入给 SOM 分类器。对链路性能特性的学习的初始值 $\varphi(0)=0.8$，学习次数 $S=100$。图 5、图 6 分别示出了两种场景下链路性能的推测值与 SOM 真值的比较。

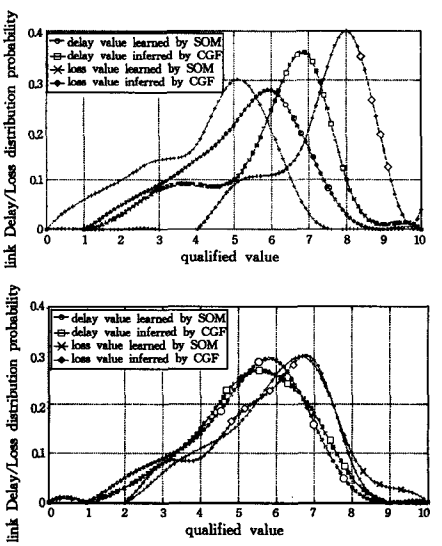

图 5　场景 1 中异常链路 l_{13}（上图）和正常链路 l_{30}（下图）性能推测值与 SOM 真值的比较

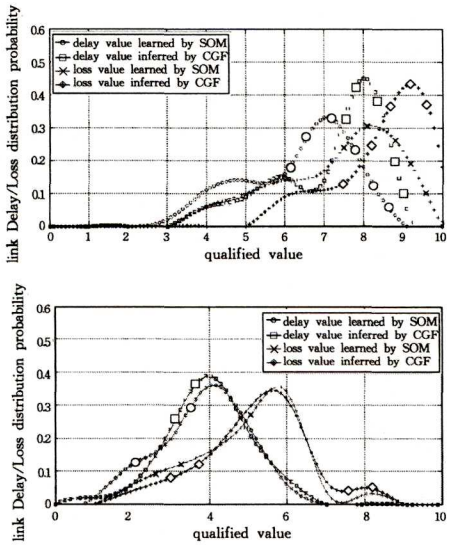

图 6 场景 2 中异常链路 l_{53}(上图)和正常链路 l_{31}(下图)性能推测值与 SOM 真值比较

在两种场景中,异常链路的延迟和丢失率分布状况与其对应的性能轮廓存在显著不同,其相应之差均超过阈值 0.9,显然是由于 l_{13}、l_{53}所包含的异常节点所致。而其中的正常链路 l_{30}和 l_{31}的延迟和丢失率分别与其对应的真值分布状况几乎保持一致。

为进一步说明异常节点对其所在路径性能的影响,以上述链路 l_{13}和 l_{53}为例进行实验,图 7、图 8 反映了仿真统计所得的性能真值与性能 CGF 的推测值分别占它们所在路径性能值的百分比。

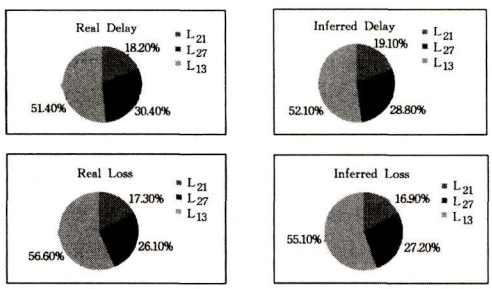

图 7 l_{13}所在路径的延迟(上图)和丢失率(下图)真值与相应的 CGF 推测值分别占其所在路径性能值的百分比

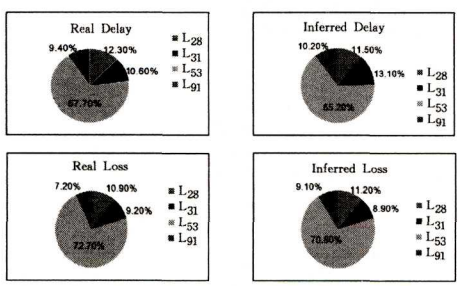

图 8 l_{53}所在路径的延迟(上图)和丢失率(下图)真值与相应的 CGF 推测值分别占其所在路径性能值的百分比

可以看出:一方面,各链路性能的真值与对应推测值之间的误差均很小(<2%);另一方面,网络 E2E 路径的性能恶化主要由其中的异常链路(Flooding 攻击节点)所决定。

检测到异常链路后,就可利用 3.5.2 节的攻击节点进行定位,两种场景下的攻击节点集 $N^{atk}(t)$如表 2 所列。

表 2 攻击节点集

场景	$N^{atk}(t)$
N=30	n_2、n_{17}
N=200	n_{31}、n_{62}、n_8、n_{46}

4.2.3 安全威胁评估和防御策略实施

限于篇幅,局部节点的安全威胁评估主要针对两种场景下的网络中间节点(包括攻击节点),并对式(13)中的 u 和 v 均取值 0.5。图 9 显示了两种场景下局部节点安全威胁评估结果。

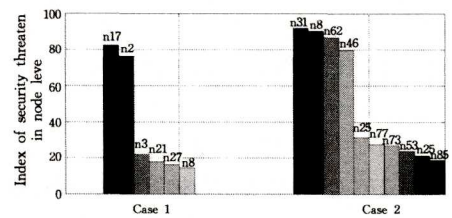

图 9 节点级的安全威胁评估

可以看出:在场景 1 中,n_2 和 n_{17}对网络安全威胁量化值达到 80 左右,而其他节点安全威胁量化值大都仅为 20 左右;在场景 2 中,n_{31}、n_{62}、n_8 和 n_{46}的安全威胁量化值超过 80,而其余节点安全威胁量化值最大不超过 30。这充分说明了 Flooding 攻击节点对网络造成的危害程度。

图 10 显示了两种场景下攻击给网络全局造成的安全威胁状况,网络安全威胁呈现出显著加剧趋势。这是由于随着攻击节点向移动区域中心移动,其向网络倾泻了更多攻击数据包。此外,场景 2 中网络面临的安全威胁更为严重。

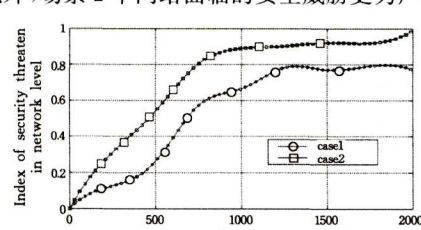

图 10 全局网络的安全威胁评估

4.2.4 系统性能的评估

根据安全威胁的评估结果,系统利用防御 Agent 产生相应的防御策略。为了评估系统在资源上的开销及获得的收益,实验采用 3.6 节提出的安全防御收益-代价评估指标 $I_{G_C}(t)$来检验不同场景下的 Flooding 攻击防御效果,如图 11 所示。

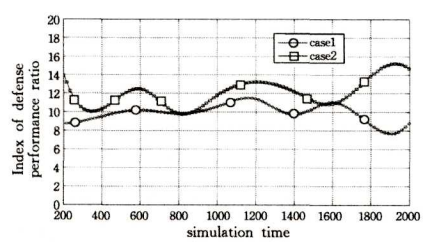

图 11 防御性能代价指标

可以看出,系统的防御收益-代价指标值在两种场景下均明显大于 1,这说明 MANETs 在遭受 Flooding 攻击时,采用本系统的安全防御策略能够显著遏制攻击并有效地维护网络性能(吞吐量),保持了网络的正常业务。

4.2.5 与现有防御方法的比较

将本系统与文献[19,22]所提出的 Flooding 攻击防御方

法的能量消耗、业务数据包从源端到目的端的成功交付率进行比较。

为评估能量消耗，本文假设各节点初始能量均为 100J。系统运行时，任一节点 n_i 的能量消耗采用文献[32]提出的能量模型 $E_i=a*Size+b$，a，b 和 $Size$ 分别表示每字节消耗的能量、字节数和每个报文消耗能量，它们分别取值如下：当 n_i 发送数据时，$a=0.4$，$b=0.8$；当 n_i 接受数据时，$a=0.3$，$b=0.6$；当 n_i 监听时，$a=0.2$，$b=0.4$。系统对能量消耗的评估采用网络所有节点剩余能量的平均极差 $\overline{E}_{remain}$（即节点剩余能量最大值与最小值之差除以节点数）作为衡量 MANETs 生存时间的重要依据[33]。图 12 显示了 3 种 Flooding 攻击的防御方法在不同场景下的能量消耗结果对比图。

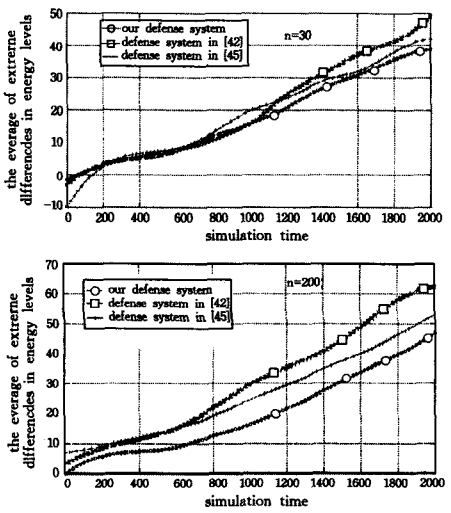

图 12　3 种防御系统的平均能量极差 $\overline{E}_{remain}$

可以看出，与其它两种系统相比，本系统的 $\overline{E}_{remain}$ 值随模拟时间趋于最小（在大规模场景中更明显），说明本系统可使 MANETs 保持更长的生存期。文献[19]采用简单的阈值法防御，造成节点能量的更大消耗：阈值偏小会导致大量攻击流量倾泻到网络；阈值偏大导致业务流量被阻拦而反复发送。文献[22]相对于文献[19]对攻击的防御是在恶意节点一跳范围内进行的，能量消耗较小，但因攻击检测在全网节点中进行，且防御未考虑网络性能，最终导致其能量消耗要比本系统大。

图 13 显示了 3 种防御系统中网络业务数据包成功交付率对比示意图。

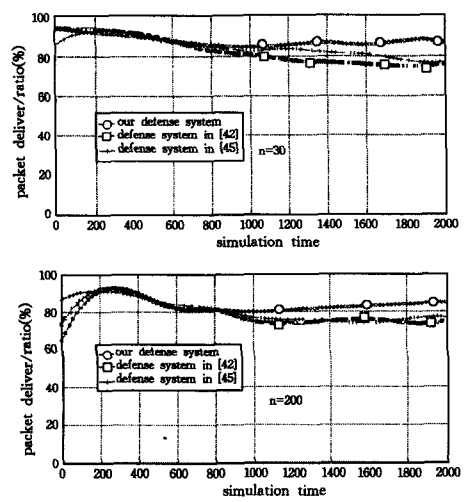

图 13　3 种防御系统下 MANETs 数据包的交付率

可以看出，随模拟时间的延长，本系统下数据包交付率明显大于其它两种系统。这是由于本系统防御 Flooding 攻击时采取了优化的防御策略，确保了网络性能和网络安全间的平衡。而其他两种防御系统则单纯地从安全角度进行防御，没有考虑网络的性能[34]。但在总体上文献[22]要比文献[19]的数据包交付率高，这是因为前者的防御在攻击节点的一跳范围内进行，较后者在全网范围内防御相对节约网络资源。

综上所述，本系统能够有效地对 MANETs 的 Flooding 攻击行为进行防御，并在性能上较现有一些防御系统更好。

结束语　Flooding 攻击是 MANETs 所面临的严重安全问题之一。现有安全解决方案未能有效适应这种网络特性，尤其是不能在网络性能和网络安全间保持平衡。本文通过对 MANETs 时空动态性、网络链路性能的推测、攻击的检测与防御进行分析，提出以网络性能为核心的 Flooding 攻击防御系统。仿真实验结果表明，本系统不但能够有效地适应 MANETs 特性，而且具有较强的灵活性和扩展性。下一步将从以下几点进行深入研究：1）从电能资源消耗的角度继续优化本系统；2）将现有一些安全认证机制集成到本系统；3）将本系统应用到真实网络环境中进行验证。

参 考 文 献

[1] MEHER R, LADHE S. Review Paper on Flooding Attack in MANET [J]. Journal of Engineering Research and Applications, 2014, 4(1): 39-46.

[2] LI F, JASSIM S. Malicious nodes seriously affect the performance of mobile ad hoc networks [EB/OL]. [2014-9-21]. http://spie.org/x8693.xml.

[3] HE Jin-lu, CHU Wei, LIU Hui-zhou. Research and Improvement of AODV Routing Protocol [J]. Computer Engineering, 2015, 41(1): 110-114. (in Chinese)
何绵禄，褚伟，刘辉舟. AODV 路由协议的研究和改进[J]. 计算机工程，2015，41(1)：110-114.

[4] DORRI A, KAMEL S R, KHEIRKHAH E. Security challenges in mobile ad hoc networks: a survey [J]. International Journal of Computer Science and Engineering Survey, 2015, 6(1): 15-29.

[5] LIANG M, TING H, SWAMI A, et al. Node Failure Localization via Network Tomography [C]// Proc. of the 2014 Conference on Internet Measurement Conference. Vancouver, BC, Canada, 2014: 195-208.

[6] ZAMANI A T, ZUBAIR S. Security in Routing Protocol for Ad Hoc Networks [J]. International Journal of Science and Research, 2014, 3(4): 375-380.

[7] KATARIA J, DHEKNE P S, SANYAL S. A Scheme to Control Flooding of Fake Route Requests in Ad-hoc Networks [C]// Proc. of the 3rd International Conference on Computers and Devices for Communication. West, India, 2006: 198-201.

[8] AHMAD S, AWAAN I, WAQQAS A, et al. Performance Analysis of DSR & Extended DSR Protocols [C]// Proc. of the 2nd Asia International Conference on Modeling & Simulation. Kuala Lumpur, 2008: 191-196.

[9] GOPALAKRISHNAN S, GANESHKUMAR P. Intrusion De-

tection in Mobile Ad Hoc Network Using Secure Routing For Attacker Identification Protocol [J]. American Journal of Applied Sciences, 2014, 11(8): 1391-1397.

[10] ZISHAN N, CHOLE V. Intrusion Detection Systems and Security Aspects for Mobile Ad Hoc Networks [J]. International Journal on Recent and Innovation Trends in Computing and Communication, 2015, 3(2): 446- 448.

[11] ZHANG Y, LEE W. Intrusion Detection Techniques for Mobile MANET [J]. Wireless Networks Journal, 2003, 9(5): 545-556.

[12] LEILA M, DJEMILI T F, SALIM G. MASID: Multi-Agent System for Intrusion Detection in MANET [C]// Proc. of the Ninth International Conference on Information Technology: New Generations (ITNG). Las Vegas: IEEE Press, 2012: 65-70.

[13] WANG W, MAN H, LIU Y. A framework for intrusion detection systems by social network analysis methods in ad hoc networks [J]. Security Communication Networks, 2009, 2(6): 669-685.

[14] ZHANG Xiao-ning, FENG Deng-guo. Instrusion dectection for ad hoc routing based on fuzzy behavior analysis[J]. Journal of Computer Research and Development, 2006, 43(4): 621-626. (in Chinese)
张晓宁, 冯登国. 基于模糊行为分析的移动自组网入侵检测[J]. 计算机研究与发展, 2006, 43(4): 621-626.

[15] YI P, JIANG Xing-hao, WU Yue, et al. Distributed intrusion detection for mobile ad hoc networks [J]. Journal of Systems Engineering and Electronics, 2008, 19(4): 851-859.

[16] MARCHANG N, DATTA R. Collaborative techniques for intrusion detection in mobile ad-hoc networks [J]. Ad Hoc Networks, 2008, 6(2008): 508-523.

[17] OTROK H, MOHAMM N, WANG L, et al. A game-theoretic intrusion detection model for mobile ad hoc networks [J]. Computation Communication, 2008, 31(4): 708-721.

[18] MANOUSAKIS K, STERNE D, IVANIC N, et al. A stochastic approximation approach for improving intrusion detection data fusion structures [C]// Proc. of the IEEE Military Communications Conference. San Diego, CA, 2008: 1-7.

[19] EU Z A, KHOON W, SEAH G H. Mitigating Route Request Flooding Attacks in Mobile Ad hoc Networks [C]// Proc. of International Conferences on Information Networking. Sendai, Japan, 2006.

[20] YI S, KRAVETS R. Composite Key Management for Ad Hoc Networks [C]// Proc. of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services. 2004: 52-61.

[21] SHANDILYA S K, SAHU S. A trust based security scheme for RREQ flooding attack in MANET [J]. International Journal of Computer Applications, 2010, 5(12): 4-8.

[22] BHUVANESHWARI K, DEVARAJ A F S. PDS-A Profile based Detection Scheme for flooding attack in AODV based MANET [J]. International Journal of Security, Privacy and Trust Management, 2013, 2(3): 17-28

[23] GOLIĆ J D. A new authentication model for ad hoc networks [J]. International Journal of Information Security, 2012, 11(5): 333-347.

[24] WANG Wei, GUAN Xiao-hong, WANG Bei-zhan, et al. Evaluation method with measureable space-time dynamic properties for mobile ad hoc networks[J]. Journal of Software, 2011, 22(6): 1333-1349. (in Chinese)
王伟, 管晓宏, 王备战, 等. 可量化的移动 Ad Hoc 网络时空动态特性评估方法[J]. 软件学报, 2011, 22(6): 1333-1349.

[25] LI Y, CAI W, TIAN G I, et al. Loss Cumulant Generating Function Inference in Sensor Network[C]// Proc. of the International Conference on Wireless Communications, Networking and Mobile Computing. Wuhan, China, 2006: 1-4.

[26] JIAO Li, LIN Yu, WANG Wen-dong, et al. A novel algorithm for link delay inference in the neteorks with load-balance routing [J]. Journal of Software, 2005, 16(5): 886-893. (in Chinese)
焦利, 林宇, 王文东, 等. 一种负载均衡网络中内部链路时延推测算法[J]. 软件学报, 2005, 16(5): 886-893.

[27] YAO Y, CAI W. Ad Hoc Network Measurement Based on Network Tomography: Theory, Technique, and Application [J]. Journal of Networks, 2010, 5(6): 666-674.

[28] SHAH B, Trivedi B H. Artificial Neural Network based Intrusion Detection System: A Survey [J]. International Journal of Computer Applications, 2012, 39(6): 13-18.

[29] KAO B, TU N N, HWANG I, et al. Auction-Based Bandwidth Allocation in Multi-Hop Wireless Ad Hoc Networks [J]. Wireless Personal Communications, 2012, 66(2): 473-488.

[30] The network simulator—ns-2 [OL]. [2014-9-21] http://www.isi.edu/nsnam/ns.

[31] HU Xi, WANG Xin, ZHANG Bin. Stability-oriented adaptive routing overhead contral algorithm in MANETs [J]. Computer Science, 2014, 41(3): 100-104, 123. (in Chinese)
胡曦, 王鑫, 张斌. MANETs 面向稳定性的自适应路由开销控制算法[J]. 计算机科学, 2014, 41(3): 100-104, 123.

[32] FEENEY L M, NILSSON V. Investigating the energy consumption of a wireless network interface in an ad hoc networking environment [C]// Proc. of the IEEE INFOCOM, Anchorage. AK, USA, 2001.

[33] WANG Wei, WANG Hui-ran, WANG Bei-zhan, et al. Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks [J]. Information Sciences, 2013, 220(1): 580-602.

[34] JIANG Yi-bo, WANG Yu-chen, WANG Wan-liang, et al. Performance analysis method for instrusion detection in MANETs based on machine learning algorithms [J]. Computer Science, 2013, 40(11A): 170-191. (in Chinese)
蒋一波, 王鱼晨, 王万良, 等. 一种基于机器学习的 MANET 网络入侵检测性能评估方法研究[J]. 计算机科学, 2013, 40(11A): 170-191.