移动自组织网络环境下的威胁建模与仿真研究

李冰心[1] 朱丽娜[1,2] 袁卫东[1]
(武汉数字工程研究所 武汉 430074)[1] (哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[2]

摘 要 相对于传统有线网络,移动自组织网络(Mobile Ad Hoc NETwork,MANET)容易遭受各种主动和被动攻击。研究MANET网络可能遭受的威胁与攻击方式,建立实用有效的异常行为研究平台,对将来验证各种检测和防御的方法有极大的帮助,对于构建安全、实用的MANET网络具有重要的理论与实践意义。使用OPNET网络建模和仿真工具对MANET网络环境中的异常行为进行了建模,对虫洞、黑洞以及网络拥塞3种典型的自组织网络环境下的异常行为进行了威胁建模,并进行了验证和测试。OPNET通过无线模块、WLAN模型和MANET模型为无线网络建模与仿真提供了丰富多层次的支持。详细阐述了这些异常行为对MANET网络的影响,结果表明该模型较好地刻画了相关威胁的行为。

关键词 移动自组织,威胁建模,仿真研究
中图法分类号 TP309 **文献标识码** A

Research on Modeling and Simulating the Threats in MANET Environment

LI Bing-xin[1] ZHU Li-na[1,2] YUAN Wei-dong[1]
(Wuhan Digital Engineering Institute, Wuhan 430074, China)[1]
(School of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)[2]

Abstract Comparing with the traditional network, the Mobile Ad Hoc NETwork(MANET) is more vulnerable to various proactive and passive attacks. Building an efficient and practical benchmark for researching anomaly behaviors through modeling the possible threats and ways of attacks in MANET environment is very beneficial for verifying and testing some proposed detection and provention related approaches. It also establishes a significative base for exploring a secure MANET environment. This paper presented some approaches of modeling and simulating some typical abnormal behaviors like Worm hole, Black hole and Routing Jams commonly occurred in MANET. Those approaches depict the abnormal behaviors exactly. The verification and tests in simulation scenarios were also conducted in experiments with better performance.

Keywords MANET, Threats modeling, Simulation research

1 概述

在一些特殊的应用场合中,比如野外考察、战场通信、临时组织的大型活动以及严重灾害后的救援活动等,不能依靠预先架设的网络基础设施进行通信,需要一种可以临时快速组网的移动通信技术提供通信服务。MANET网络就是可以满足这种需求的一种移动通信技术。

MANET网络的研究源于军事通信的需求,其前身是美国DARPA(Defense Advanced Research Project Agency)1972年启动的分组无线网(PRNET, Packet Radio Network)项目[1]。DARPA又分别于1983年和1994年启动了高存活性自适应网络(SURAN, Survivable Adaptive Network)和全球移动信息系统(GloMo, Global Mobile Information systems)项目,对这种可以满足军事需求、灵活的、自组织的网络进行全面深入的研究。IEEE802.11标准委员会使用"Ad Hoc网络"来命名这种特殊的无线通信网络。而IETF称这种网络为MANET网络,也就是移动Ad Hoc网络[2,3]。

与传统的有线和无线网络不同,MANET网络往往是为了完成某个特定的任务而临时组织起来的,没有网络基础设施可以利用。MANET网络是一种使用无线信道通信和多跳路由转发的自组织网络,由于移动终端的无线传输范围有限,无法直接通信的终端节点需要通过其它中间节点转发报文来互相通信,通信只能通过节点之间的互相协作来完成。MANET网络中每个终端节点兼有主机和路由器两种功能:作为主机,终端节点运行分布式应用,靠和其他节点协作来完成特定的任务;作为路由器,终端节点运行路由协议,负责协助其他节点完成通信任务。

由于MANET采用与传统的有线和无线网络不同的通

到稿日期:2008-11-04 返修日期:2009-03-01 本文受国防"十一五"预研计划(No. C0820061362-06, No. A1420080183),国家"863"高新技术计划信息安全主题(No. 2007AA01Z464)资助。
李冰心(1979—),男,工程师,主要研究方向为网络与信息安全;朱丽娜(1981—),女,博士研究生,主要研究方向为入侵检测与网络安全,E-mail:zhulina81@gmail.com;袁卫东(1974—),男,工程师,主要研究方向为软件工程与网络安全。

信方式，没有中心节点并且没有网络基础设施可以依靠，因此难以将用于传统网络环境中的安全检测防范技术直接运用到MANET网络中。另外，由于MANET使用无线信道、节点间通信通过多个中间节点路由转发完成、各节点地位对等独立自主工作、各移动节点所具有的资源(包括电源、计算能力、存贮容量等)相当有限，因此MANET在各个工作阶段极易遭受各种主动和被动攻击。研究MANET网络可能面临的各种攻击和异常行为并对其建立仿真模型，对于发现相应的检测和防御方法有很大的帮助，也可以为各种异常行为检测和防御方法提供验证和评估环境。我们选用的建模工具是OPNET Modeler网络建模与仿真软件。OPNET Modeler采用面向对象建模方式，可以很方便地继承和扩展已有模型。OPNET将建模工作划分为3个层次，分别为(1)网络层：从高层设备(即节点和通信链路)对系统进行规范；(2)节点层：从应用、进程、队列和通信接口对节点的功能进行规范；(3)进程层：对系统内节点所含进程的行为进行规范，包括决策进程和算法。在这些层次上可以分别定义系统的网络模型、节点模型和进程模型，描述系统的拓扑结构、数据流(系统结构)和控制流(行为逻辑)。OPNET Modeler的进程编辑器通过有限状态机来支持各种协议、应用、资源和算法。

OPNET通过无线模块、WLAN模型和MANET模型为无线网络建模与仿真提供了丰富的、多层次的支持。无线模块支持节点移动性的模拟，并通过收发信机管道来模拟无线信道。WLAN(Wireless LAN)模型主要用于模拟无线网络的MAC层，支持IEEE802.11和IEEE802.11b无线局域网标准，并支持Ad Hoc网络模式。MANET模型提供了包括DSR(动态源路由协议，Dynamic Source Routing)协议在内的多种MANET路由协议进程模型，用来刻画MANET网络中移动节点的协作与路由转发行为。

2 无线移动自组织网络下的威胁建模与仿真

现将在如图1所示的仿真场景对虫洞、黑洞以及路由拥塞等移动自组织网络中的异常行为模型进行测试。在这个仿真网络场景中，节点之间的直接通信距离拟被限制为200m。节点mobile_server_0上将运行FTP和HTTP服务，节点mobile_client_0将定时向服务器mobile_server_0请求FTP和HTTP服务。由于节点mobile_client_0和节点mobile_server_0之间距离太远，这两个节点将借助中间的5个节点完成数据通信任务。

为了观察异常行为对移动自组织网络的影响，将这个场景作为基本场景，然后在这个场景基础上对每种异常行为模型建立了相应的网络场景。

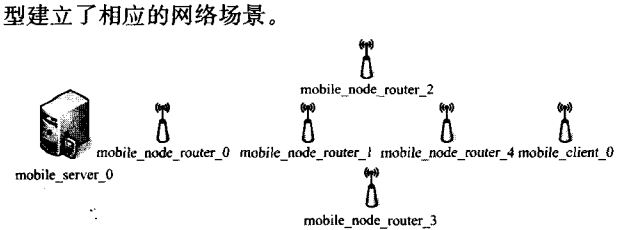

图1 移动自组织网络异常行为基础仿真场景

2.1 虫洞行为模型的建立与仿真

2.1.1 行为模型

移动自组织网络中的虫洞攻击是指这样的一些行为，攻击者在网络中一个地方记录下接收到的数据包，然后将这个数据包通过隧道传送到位于网络中另外一个地方的共谋节点，并且由这个共谋节点将包重放到网络中。在移动自组织网络中可以使用以下4种方式产生虫洞：

(1)在网络层或其上层重新封装数据包并通过隧道传送。

(2)攻击节点通过使用更大功率的无线发射机将数据包传送到更远的地方。

(3)攻击节点和共谋节点通信时使用与其它节点不同的无线信道，这个信道具有更大的传输范围和传输速度。

(4)攻击节点和共谋节点之间通过有线网络连接，并使用有线网络建立隧道。

在第一种类型的虫洞中，恶意节点对接收到的数据包适当修改后，使用上层协议重新封装，再利用网络中其它节点提供的路由转发服务将数据包发送到共谋节点。共谋节点接收到数据包后，解开封装，并将包重放到网络中。其它3种类型的虫洞也按照类似的方式修改和重新封装接收到的数据包，不同的地方在于恶意节点直接将数据包发送给共谋节点而不借助于其它节点。

由于隧道的距离比一个单跳的正常无线传输距离要长，攻击者，可以很方便使得经过隧道的数据包比经过正常多跳路由的其他包更快到达目的地。我们拟通过包约束(Packets Leashes)来实现对虫洞的检测。包约束主要包括限制数据包最大传输距离、地理约束(Geographical Leashes)和时间约束(Temporal Leashes)等方法。

2.1.2 仿真建模

在针对虫洞异常行为的仿真场景中，将节点mobile_router_1和mobile_router_4作为虫洞的两个端点。这两个节点之间的距离大于直接通信的距离，并且拟从仿真时间500s起发起虫洞攻击。图2和图3分别是第495s和507s时从源节点mobile_client_0到目的节点mobile_server_0的路由路径。通过这两个图可以看出，在发起虫洞攻击之后，从源节点到目的节点形成了一条通过虫洞隧道的路由路径。

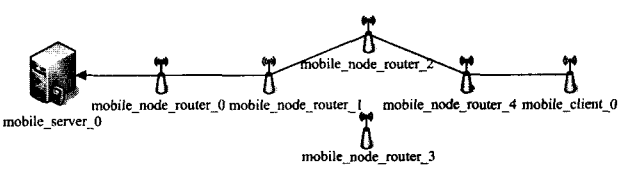

图2 正常场景中节点路由路径

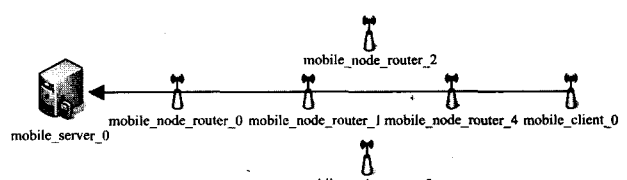

图3 虫洞异常场景中节点路由路径

2.2 黑洞行为模型的建立与仿真

2.2.1 行为模型

根据黑洞的工作原理，拟建立针对DSR协议的黑洞异常行为的进程模型。在这个进程模型中将按以下方式处理数据包：

(1)在DSR协议路由发现阶段，异常节点接收到路由请求消息后，将本节点地址和目的节点地址直接追加在路由请

求消息的路由记录后面，形成伪造的路由记录，并将这个路由记录作为路由回复，发给源请求节点。由于异常节点立即回复而不是继续将路由请求广播到目的节点，因此这种伪造的回复可以比其它节点的回复消息更早返回源请求节点。另外，这种回复消息中的路由记录忽略了从异常节点到目的节点之间的节点，因此可能比其它路径有更少的跳数。

(2)在 DSR 协议路由维护阶段，异常节点接收到路由维护确认请求消息后，向上一跳节点发送路由维护确认消息，以保持路径的有效性。

(3)在 DSR 协议数据包转发阶段，异常节点根据接收到的数据包目的地址判断数据包是否需要转发。如果目的地址不属于异常节点，则丢弃数据包。

(4)对于不属于以上情况的数据包，异常节点按照正常的 DSR 协议包处理流程进行处理。由于转发的数据包被丢弃，因此不会在处理转发的数据包时进行路由维护，也不会向前一跳节点发送路由错误消息，从而可以维持路径的有效性。

2.2.2 *仿真建模*

在针对黑洞异常行为的仿真网络场景中，节点 mobile_node_router_2 将被设定为从仿真时间第 600s 起发起黑洞攻击。

图 4 和图 5 分别是正常场景和黑洞异常场景中客户节点 mobile_client_0 接收到的 HTTP 流量统计图。对比这两个图可以看出，黑洞异常场景中客户节点 mobile_client_0 在第 10min(600s)后从服务器接收到的 HTTP 流量变为 0。这说明由于受黑洞节点 mobile_node_router_2 影响，其周围节点都将包发送给黑洞节点并被丢弃，因此客户节点 mobile_client_0 从第 600s 起无法从服务器接收到 HTTP 数据包。

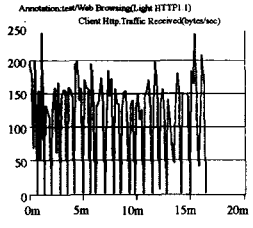

图 4 正常场景中节点接收的 HTTP 流量统计

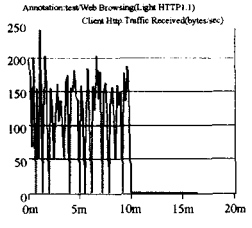

图 5 黑洞异常场景中节点接收的 HTTP 流量统计

2.3 路由拥塞行为模型的建立与仿真

2.3.1 *行为模型*

拟建立的针对 DSR 路由协议的路由拥塞攻击模型通过向指定节点不断发送无用的数据包来干扰网络。在这种模式的路由拥塞攻击下，如果路由协议没有防御路由拥塞攻击的能力，则会忠实地转发无用的数据包，使得从发起攻击的节点到指定节点的路由路径上的所有节点都忙于处理无用的数据包，无法进行正常的工作。在这种模型中，攻击节点可以在指定时间内发起若干次攻击，每次攻击持续一段时间。我们将为这种攻击模型提供以下属性：

(1)Start Time：发起路由拥塞攻击的时间。

(2)Stop Time：停止路由拥塞攻击的时间。

(3)Packet Size：数据包的大小，即攻击节点发出的无用数据包的大小。这个属性是一个分布函数，每次发送数据包时使用这个分布函数生成的整数值作为数据包的大小。

(4)Packet Inter-Arrival Time：在每次攻击中发送数据包的间隔时间。这个属性是一个分布函数，发送一个数据包后使用这个函数生成发送下一个数据包的时间。

(5)Duration：攻击的持续时间。这个属性是一个分布函数，用来生成每次攻击持续的时间。

(6)Inter-Repetition Time：两次攻击之间的间隔时间。这个属性是一个分布函数，一次攻击之后使用这个函数生成下一次攻击发起的时间。

(7)Destination IP Address：指定数据包发送的目的节点 IP 地址。

2.3.2 *仿真建模*

拟使用图 6 所示场景来测试路由拥塞异常模型。这个场景在图 1 所示场景中添加了一个路由拥塞异常节点 mobile_node_0。新增的节点位于节点 mobile_node_router_2 附近，并将向节点 mobile_node_router_1(ip 地址是 192.0.0.4)发送无用的数据包。异常节点的路由拥塞参数配置如图 7 所示。从仿真时间第 100s 起，异常节点间歇地向节点 mobile_node_router_1 发送大量无用的数据包，每次发送持续 200s。然后间隔 50s 后再发送，直至仿真结束。

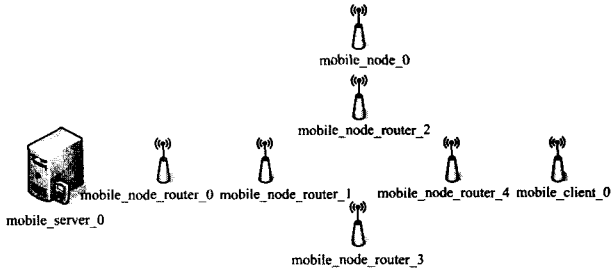

图 6 路由拥塞测试场景

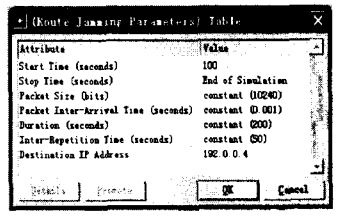

图 7 路由拥塞异常节点参数配置

图 8 和图 9 分别是正常和异常场景中 mobile_client_0 节点的 FTP 文件下载响应时间统计图。对比这两个图，可以看出由于路由拥塞异常节点不断向位于 FTP 客户机和服务器之间路由必经路径上的节点发送大量无用数据包，影响了正常的数据转发，使得客户机节点的 FTP 文件下载响应时间大大增加。

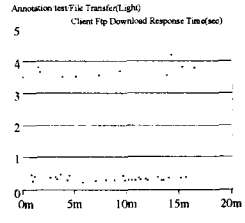

图 8 正常场景中节点 FTP 下载响应时间

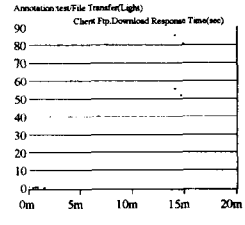

图 9 路由拥塞异常场景中节点 FTP 下载响应时间

结束语 本文使用 OPNET 网络建模和仿真工具对 MANET 网络环境中的异常行为进行了建模，对虫洞、黑洞以及网络拥塞 3 种典型的自组织网络环境下的异常行为进行了威胁建模，并进行了验证和测试。OPNET 通过无线模块、

WLAN 模型和 MANET 模型为无线网络建模与仿真提供了丰富的、多层次的支持。本文详细阐述了这些异常行为对 MANET 网络的影响。仿真实验结果表明本模型较好地刻画了相关威胁的行为。

将来的工作主要集中在进一步研究其他异常行为，如无线被动窃听以及网络灰洞等的建模和仿真；并力求把这些仿真的异常行为模块化，便于移植到真实的系统中应用。

参 考 文 献

[1] Johnson D B, Maltz D A. The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Mobile Ad Hoc Network(MANET) Working Group, IETF, Version 9, April 2003

[2] Maltz D A, Broch J, Johnson D B. Experiences designing and building a multi-hop wireless Ad hoc network testbed[R]. CMU-CS-99-116. CMU School of Computer Science, March 1999

[3] MANET. Mobile ad hoc networks (MANET) charter WG IETF, 2000

(上接第 90 页)

change 子协议，TTP 不需参与，协议支持离线 TTP。

公平性：以下分 3 种情况分析协议的公平性。

(1) 发方 O 和接收者 R_j 都诚实，则发方和收方都按照 Exchange 子协议交换消息，显然最后 R_j 得到 NRO，且 O 得到 NRR，协议公平。

(2) 发方 O 诚实而接收者 R_j 不诚实，即 R_j 不发送 EOR_j 给 O 或发送错误的 EOR_j 给 O。之后有两种可能：a) R_j 发送正确的 f_r 请求给 TTP，根据 Recovery 子协议，TTP 将发送 K_i' 给 R_j，发送 EOR_j 给 O，协议公平。b) R_j 发送伪造的 f_r 请求给 TTP，由于 EOR_j 中包含 $cert$，R_j 不可能伪造出 $cert$，因而不能发送伪造的 O，R 和 sid；又由于 EOR_j 是对 EOO 的签名，R_j 不可能伪造出 EOO，因而不能发送伪造的 $H(E_{K_i'}(M))$ 和 $H(K_i')$；若伪造 i，则会与 TTP 计算的 $H(K_i')$ 不符。因此，TTP 可以发现伪造的 f_r 请求，中止 Recovery 子协议运行，最终，由于 O 启动 Abort 子协议，R_j 得到 abrt，协议公平。

(3) 接收者 R_j 诚实而发方 O 不诚实。O 的目的是获取有效 NRR 而不提供 M，其可能的欺骗有 3 种：a) 伪造消息 1^e。若 O 伪造标识符 O，R 或 T，接收者将不会响应 O；若 O 伪造 $H(K_i')$，$H(E_{K_i'}(M))$，i 或 $cert$，由于 EOR_j 中包含这些信息，因此 O 得不到有效的接收证据。b) 伪造消息 3^e。由于消息 1^e 中有 $H(K_i')$，R_j 可以辨别出伪造的消息 3^e，转而通过 TTP 获得对称密钥 K_i'，协议公平。c) 不发送消息 3^e，并请求 TTP 中止与 R_j 的交换。根据 Abort 子协议，R_j 将得到 abrt，协议公平。

时限性：协议允许发方 O 启动 Abort 子协议中止交换，允许接收者 R_j 启动 Recovery 子协议通过 TTP 完成交换，且协议的各参与方在任何状态时中止协议运行都不影响协议公平性，因此协议满足时限性。

机密性：(1) Exchange 子协议使用群加密机制发送密钥 K_i'，Recovery 子协议使用接收者公钥加密 K_i' 后发送，所以监听者得不到 K_i'，不能获得 M。(2) 发方和收方与 TTP 通信时，仅发送 $H(E_{K_i'}(M))$ 而没有直接发送密文，虽然 TTP 可以计算出 K_i'，但由于 TTP 没有动机去监听获得的密文，因此 TTP 没有得到 M。(3) R 采用 $(P_{R_1}(R_1), P_{R_2}(R_2), \cdots)$ 的结构，已经获得 M 的 R_i 得不到其他参与方 R_j 的标识符，不能将 M 泄漏给 R_j。(4) 协议采用双密钥链结构，接收者得到第 i 轮交换的密钥 K_i'，不能计算出其它轮的密钥。因此，协议满足机密性。

结束语 本文提出了一种基于密钥链的多方非否认协议。协议采用双密钥链结构，支持离线 TTP，满足公平性、时效性和机密性。在同一组用户进行多轮信息交换时，协议可有效减轻 TTP 存储负担。本文对协议进行了非形式化的分析。下一步的研究，将考虑利用串空间理论或其它工具对非否认协议的安全属性进行形式化分析。

参 考 文 献

[1] Zhou J, Gollmann D. A fair non-repudiation protocol[C]// Proceedings of the 1996 IEEE Symposium on Security and Privacy. Oakland, 1996: 55-61

[2] Wang G. Generic non-repudiation protocols supporting transparent off-line TTP[J]. Journal of Computer Security, 2006, 14(5): 441-467

[3] Cederquist J, Dashti M T, Mauw S. A Certified Email Protocol Using Key Chains[C]// Advanced Information Networking and Applications Workshops(AINAW '07). 21st International Conference. 2007: 525-530

[4] Liang X, Cao Z, Lu R, et al. Efficient and secure protocol in fair document exchange[J]. Computer Standards & Interfaces, 2008, 30(3): 167-176

[5] Permpoontanalarp Y, Kanokkanjanapong J. Dynamic Undeniable Fair Certified Email with DDoS Protection[C]// Advanced Information Networking and Applications. Okinawa, 2008

[6] Kremer S, Markowitch O. A multi-party non-repudiation proto-co[C]//15th International Conference on Information Security. IFIP World Computer Congress. Beijing, China, 2000: 271-280

[7] Markowitch O, Kremer S. A Multi-party Optimistic Non-repudiation Protocol[C]// Information Security and Cryptology-ICISC 2000: Third International Conference. Seoul, Korea: Spinger-Verlag, 2001: 109-122

[8] Onieva J A, Zhou J, Lopez J. Non-repudiation protocols for multiple entities[J]. Computer Communications, 2004, 27(16): 1608-1616

[9] Zhou J, Onieva J, Lopez J. Optimized multi-party certified email protocols[J]. Information Management and Computer Security, 2005, 13(5): 350-366

[10] Wang H, Wang R. Improvement of a multi-party certified email protocol[J]. Chinese Journal of Electronics, 2007, 16(4): 613-616

[11] Gurgens S, Rudolph C, Vogt H. On the security of fair non-repudiation protocols[J]. International Journal of Information Security, 2005, 4(4): 253-262