移动自组网中基于声誉机制的安全路由协议设计与分析

王建新[1,2],张亚男[1],王伟平[1],卢锡城[2]
(1. 中南大学信息科学与工程学院,湖南长沙 410083;2. 国防科技大学计算机学院,湖南长沙 410073)

摘 要: 移动自组网是一种有特殊用途的对等式网络,具有无中心、自组织、可快速展开、可移动等特点,这些特点使得它在战场、救灾等特殊场合的应用日渐受到人们的重视. 由于在移动自组网络中每节点既是主机又是路由器,所以容易遭受基于路由信息的攻击,而现今的路由协议基本没有考虑到该问题. 本文在分析移动自组网络安全特性的基础上,综述了该方面的研究工作,建立了基于声誉机制评价体系,并给出了具体的评价方法和计算模型. 在此基础上,提出了基于声誉机制的安全路由协议 S-DSR. 仿真结果表明在存在攻击节点的情况下 S-DSR 协议比 DSR 协议具有更好的包传输率、包丢失率等属性.

关键词: 移动自组网; 网络安全; 安全协议; 声誉机制
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2005) 04-0596-06

A Security Routing Protocol Based on Reputation Systems in MANET

WANG Jian-xin[1,2], ZHANG Ya-nan[1], WANG Wei-ping[1], LU Xi-cheng[2]
(1. *School of Information Science and Technology, Central South University, Changsha, Hunan* 410083, *China*;
2. *School of Computer, National University of Defense Technology, Changsha, Hunan* 410073, *China*)

Abstract: Mobile Ad hoc network is a special peer-to-peer network that is infrastructureless, self-organizing, dynamically reconfiguration and mobile. And now people pay more attention to the using of ad hoc network in emergence area such as battle field and disaster rescue. Each node in mobile ad hoc network can be regarded as either a computer or a router, so it is very vulnerable to routing information attacks. However, little information about the security problem has been considered in the routing protocols that have been proposed. In this paper, an overview of the research about attacks against routing information is given firstly, and then we present that a security routing protocol S-DSR based on reputation systems can be used in ad hoc networks. The simulation environment and results is given and the simulation results show that S-DSR protocol can get better than DSR protocol while there exists attacking nodes.

Key words: mobile ad hoc network; network security; reputation systems; security protocol

1 引言

移动自组网(Mobile Ad Hoc Network)作为一种新型的无线移动网络,不像传统的无线网,它不依赖于任何固定设施,而是通过移动节点间的相互协作保持网络互联. 由于节点具有移动性,网络的拓扑环境是不断变化的[1]. 而在传统网络中,主机之间的连接是固定的,网络采用层次化的体系结构,并具有稳定的拓扑,提供了多种服务以充分利用网络的现有资源,包括路由器服务、命名服务、目录服务等. 并在此基础上提出了相关的安全策略,如加密、认证、访问控制和权限管理、防火墙等. 而在移动自组网中没有基站或中心节点,所有节点都是移动的,网络的拓扑结构动态变化,并且节点间通过无线信道相连,没有专门的路由器,由节点自身充当路由器,也没有命名服务、目录服务等网络功能. 这些特性导致了在传统网络中的安全机制不再适用于自组网.

使用无线信道使自组网很容易受到诸如被动窃听、主动入侵、信息阻塞、信息假冒等各种方式的攻击. 窃听可能使敌方获取保密信息,而主动攻击可能使敌方删除信息、插入错误信息、修改信息、或者冒充某一节点,从而破坏了可用性、完整性、安全认证和抗抵赖性. 由于节点的能源有限,并且 CPU 的计算能力较低,无法实现复杂的加密算法,这增加了被窃密的可能性. 当节点在战场上移动时,由于缺乏足够的保护,很有可能被占领. 由于节点的移动性,自组网的拓扑结构和成员处于动态的变化之中,节点之间的信任关系也在不断变化. 因此任何只具有静态配置的安全方案在自组网中是不可行的.

从总体上说,对移动自组网的攻击可分为主动攻击和被动攻击. 主动攻击则指主动入侵的攻击方式. 被动攻击是指只是消极窃听,而不主动入侵.

在移动自组网中存在各种攻击方式,无论是发送错误的路由包还是不转发数据包等攻击行为,它们的目的就是造成网络的不可用,因此可以把这些节点统称为不良节点,把他们的行为称为不良行为. 有些不良节点是进行主动性攻击. 而有些不良节点仅仅是为了保存自身能量和计算能力的问题不给

收稿日期:2004-05-08;修回日期:2004-12-08
基金项目:国家自然科学基金网络与信息安全重大研究计划(No. 90304010,90104028);湖南省自然科学基金(No. 03JJY5032)

其他节点转发信息,这种方式可以称之为自私性攻击.

针对移动自组网中的主动性攻击,本文给出了一个基于分级的节点声誉评价机制,用于判断节点的好坏,在此基础上提出了安全路由协议 S-DSR. 本文第二部分综述了移动自组网络中对网络中不良节点的评价方式以及安全防御措施的相关研究工作. 第三部分具体描述了声誉评价模型. 第四部分描述了基于 DSR 协议的安全路由协议 S-DSR. 第五部分给出模拟测试环境和模拟结果. 最后给出了结论.

2　相关工作

为减轻不良节点对网络的影响,文献[2]提出基于源路由协议的监测方法,用于检测包的传输情况,以此认证错误节点,但存在一定的检测错误概率(如把好节点认为是错误节点等);另一种路径分级方法用来从众多的路径中选择一条较好的、没有攻击节点的路由. 该方法采取的措施虽然没有惩罚攻击节点(不合作节点),但避免了这些节点出现在传输路径上.

针对有些节点只是转发路由包而不转发数据包,而有些自私节点既不转发路由包,也不转发数据包这种自私性攻击方式,文献[3]提出了一种基于计数器的节点合作机制,每个节点都有一个存储着计数器的安全模块. 当节点自己要传输数据包时,自己的计数器要相应减少;若为其他节点转发一个数据包则计数器加 1. 因此为保证自己数据包的传输则必须为其他节点转发数据包,从而提高了节点的合作性.

文献[4,5]提出了针对自私性攻击的一种基于 DSR[6]协议的反应式路由协议:CONFIDANT. 该协议主要包含以下组件:监测器,用于检测节点行为;声誉记录器,用于记录声誉信息;信任度管理器,用于控制发送、接收警告信息的情况;路径管理器,使节点根据声誉记录情况对行为做出调整. 模拟结果表明该方法可以保证即使网络中存在一半的自私攻击节点也能取得较好的性能.

Core[7]是针对自私性攻击提出的一种联合声誉机制. 该机制拥有一个监测器,另外还有一个声誉机制,包括:直接声誉值(由观察者提出),间接声誉值(由其他节点报告得知),以及功能声誉值(特殊的任务行为). 这些机制联合起来决定其节点的声誉值,以便决定是继续合作还是逐渐隔绝.

文献[8]提出了用于保护 AODV[9]协议中路由信息和数据报转发的安全协议. 它无需预先定义信任关系和节点间传输密钥. 在该协议中,每个节点都拥有全局密钥的一部分,每个节点由它的邻居节点联合监督. 另外,每个节点一个令牌,但很快会过期,必须从邻居节点重新申请,行为越好,令牌的有效期就越长,更新频率就越小. 该机制包括邻居验证、安全路由协议、邻居监测、入侵防御四部分,分别进行认证、监督、入侵检测等工作. 该机制可以抵抗一定数量的联合攻击节点,但增加了一定的计算开销.

SAR(Secure-Aware ad-hoc Routing)协议[10]用于保护路由发现过程,它使用类似于 QoS 路由算法的一种协议. 当节点进行路由发现时首先要确定一定的路由准绳,那么不是属于该路由准绳子网的节点则无法对路由包进行加密、解密或做出是否满足 QoS 指标的决定,只能抛弃. 该方法要求相同层次的节点要保持同步的加密、解密密钥. 这种方法对路由信息的传输(如完整性)提供了一定的保护.

在有线网中对实体的判断可以采取声誉评价机制 Reputation Systems[11]的方式. 该方式广泛应用于电子商务中,即买卖双方都拥有一定的声誉值. 交易后都会有一个反馈来评价声誉的好坏,声誉值将用于引导以后消费者的决定. 在这种方式中存在一个权威机构,该机构根据反馈信息对声誉值进行更新和发布. 例如,在 Amazon、Yahoo 网站上的交易中,Amazon、Yahoo 本身就是一个权威机构,给消费者提供消费引导. 这种拥有中心权威机制的评价方式对移动自组网来说并不适合,但可以引入对节点信任度的评价机制使之适合移动自组网.

移动自组网中声誉机制的方式与有线网中的不同,移动自组网不存在中心节点,所有节点都既是主机又是路由器,因此这种方式的监督反馈应该由整个网络中的所有节点来完成. 本文提出了一种全新的基于声誉机制的路由安全协议,用户可以自定义安全需求,并且通过对安全研究模型和安全协议的详细描述给出具体的邻居监控以及节点信息的交互方式.

3　声誉机制评价模型

针对移动自组网络的特点,建立无核心节点的声誉评价机制,如图 1 所示. 节点打开监控模式,通过监控可以获得邻居节点的信息. 若节点向下一邻居节点发送了包就开始对其进行监控,看该节点是否正常处理了传输过去的包. 监控时间为 ΔT,然后判断节点在这段时间内的行为好坏. 首先看是否有错误发生,若没有错误发生且节点被使用次数超过使用门限值则节点的主动观测值(SR, Subjective Rating)增加. 若有错误则需进行严重性评估,若在该时间段内发生的错误数小于错误门限值并且被使用次数大于使用门限则错误不够严重,SR 线性增加;若发生错误数大于错误门限则 SR 指数减少. 当节点收到其他节点发出的声誉值交换包(REP, Rating Exchange Packet)时,首先进行发送节点的信任度评价,若信任该节点才接受该节点的信息,进行间接观测值(IR, Indirect Rating)的更新.

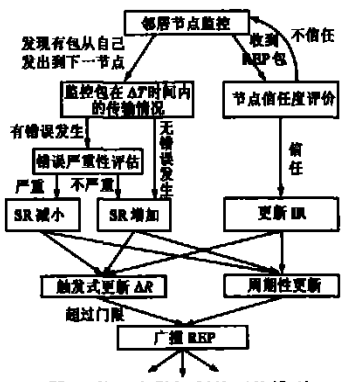


图 1　基于声誉机制的评价模型

3.1　节点声誉值评价方法

在移动自组网络中实现上述的声誉评价机制,就需一个分布式、交互系统,并且网络中每个节点都参与声誉值评价.

在该模型中,每个节点都拥有一个声誉值列表,保存着本节点对其他节点信任度的评价. 声誉值列表包括:NodeID、SR、IR,其中 NodeID 为节点编号;SR 为节点的主动观测值;IR 是从其他节点处获得的经验值,是通过信息的交换获得的.

节点对其他节点的信任度(CR, Combined Rating),即其他节点的声誉值,可以依据以下公式进行计算:

$CR = W_1 * SR + W_2 * IR$

$W_1 + W_2 = 1$

$W_1 > W_2$

(W_1、W_2 为权值,如 $W_1 = 0.7$, $W_2 = 0.3$)

一般取 W_1 大于 W_2,这是为防止敌人的恶意诋毁,因此 W_1 表示自己观测值 SR 的权值,W_2 代表对其他节点经验的权值.

3.2 SR的计算

每个节点对已知节点的 SR 的初始值为 0.5. SR 值是通过节点对邻居节点监控获得. 节点利用监测机制对邻居节点进行监控,得出节点对被监测节点的主动观测值. 该值可据不同的侧重点对不同功能进行检测(如对路由包、数据包的处理).

由于使用监听模式,向下一节点传输包时首先在自己的缓存中保存一份该包的副本,若收到下一跳已传输的报告则从缓存中删除掉副本. 若经过一段时间缓存中仍有副本认为发生错误.

从第一个监测到的错误包开始,统计 ΔT 时间. 若在 ΔT 内少于 L 个包发生错误则认为正常,可视为正常的网络拥挤、阻塞问题,否则不正常,具有攻击行为. 对不正常的惩罚比奖赏大(信誉建立难,失掉容易).

正常:ΔT 时间内发生的错误数少于门限值 L 且节点被使用的次数超过门限值 K,则 SR 线性增加,每次加一个变化值 ChangeValue1,即 SR = SR + ChangeValue1. 同时将攻击次数重置为 0.

不正常:监测错误若 ΔT 时间内超过 L 个错误门限值,记录攻击次数 n 为 1,之后累加;随着攻击次数的增加 SR 值呈指数下降. 使用指数函数描述,SR = SR-ChangValue2 $*2^{n-1}$ (n 为攻击次数的值). ChangeValue2 应适当大于 ChangeValue1. 若在 ΔT 时间内错误数小于 L 则重新计数. ΔT 和 L 的值视网络情况和包传输量而定. L 的取值要看实际情况而定,若 L 太大,攻击节点则有可能故意在 ΔT 内作 $L-1$ 个错误处理,若 L 太小,则误判攻击情况会增加. 所以 L 取值应综合考虑网络的实际情况而定.

其算法描述如图 2 所示.

```
Open Monitor Function
Begin monitor if node be used
If Monitor Time > ΔT then
    If Error < L then //L represents error threshold
      If the times node be use exceed K then
        SR = SR + ChangValue1;//IncreaseSR
        If SR > = 1 Then SR = 1;
      Endif
      n - - ;//n represents attacking times
      If n < 0 Then n = 0
    Else
      n ++
      SR = SR - ChangValue2 *2^(n-1);//DecreaseSR
      If SR < = 0 Then SR = 0
    Endif
Endif
```

图 2 SR 值的计算过程

3.3 IR的计算

IR 为节点从其他节点获得的声誉值,即网络中通过交换获得的信息. 每个节点对已知节点的 IR 值初始化为 0.5. IR 的更新和对信息来源节点的信任度 CR 相关,信任度高则更新幅度较大,若信任度低则更新较小. IR 的更新有两种方式:触发式更新和周期性更新.

触发式更新:若节点对某节点的节点信任度值的改变(通过 SR 的改变或 IR 的更新算得)超过某个门限值 ΔR 时,广播该信息(仅广播一条即节点对某节点声誉值). 此方法需在声誉值列表中增加 ΔR 字段,$\Delta R = \sum \Delta R_i$ (ΔR_i 为每次的变化值),该字段用于描述声誉值的变化情况. 若该值超过某个门限值时广播信息包 REP,广播后该项置 0. 收到信息的节点按如下公式进行更新:

$$IR_{ik} = IR_{ik} + (CR_{jk} - IR_{ik}) * CR_{ij}$$

其中:i 为待更新 IR 的节点,j 为发送更新信息的节点,k 为 i 节点要更新相应 IR 的节点. CR_{ji} 表示节点 i 对节点 j 的声誉评价值,IR_{ij} 表示节点 i 从其他节点处获得的关于节点 j 的评价值. 如节点 2 发送对节点 3 的声誉更新信息 R_{23},节点 1 收到该信息,则根据收到的 2 对 3 的声誉信息 R_{23} 和自己列表中对节点 3 R_{IR13} 的比较差值乘以对节点 2 的 R_{12} 作为更新值. 即为:

$$IR_{13} = IR_{13} + (CR_{23} - IR_{13}) * CR_{12}$$

周期性更新:周期性更新则每隔一定时间广播所有的信息,不需 ΔR 字段. 某节点对其 IR 的更新如下(节点根据所有信息的更新求平均):

$$IR_{ik} = IR_{ik} + \frac{\sum_{j=1, j\neq i, j\neq k}^{n} (CR_{jk} - IR_{ik}) * CR_{ij}}{n}$$

其中,n 为收到的信息包的个数.

4 基于声誉机制的安全路由协议 S-DSR

我们在源路由协议 DSR 的基础上增加了声誉判断机制,并且用户可以根据自己的需要来变更安全系数以增加安全性,并由此提出了基于声誉机制的安全路由协议 S-DSR.

4.1 DSR协议

DSR(Dynamic Source Routing Protocol)是一种源选路由协议[7]. 该协议分为两个阶段:路由发现阶段和路由保持阶段. 当源节点(S)想要和目的节点(D)通信,但并不知道到 D 的路径时就唤醒路由发现功能. S 首先向它的邻居发送一条含有目的节点 D 地址的 RREQ 包. 中间节点收到该包时检查自己是否有路到达目的节点 D,如果有则向 S 发送 RREP;没有则在包内加入自己的地址并继续广播. 该过程一直持续到找到目的节点为止. 当目的节点收到该包时,向 S 发送 RREP. 该路由发现过程完毕. 如果多次重发 RREQ 并经过一段特定时间,S 一直没有收到 RREP 则放弃寻路. 路由保持阶段是在链路断裂后使用的. 当链路断开时,首先由断裂链路的源节点来抢救包,即检测该节点本身是否有到达目的节点的路径,有则抢救,并向源节点 S 发送 RERR,表示链路断链,数据传输失败.

4.2 S-DSR协议

S-DSR 协议是在 DSR 协议的基础上进行的改进. 源节点(S)若需要发送数据到目的节点(D)首先要选择一个自己要求的安全系数,要求传送路径的声誉值要大于某个值,称之为请求声誉值(Require Rating). 某路径 P 的声誉值 PathRating 是指该路径上所有节点声誉值的最小值,即:

$$\text{PathRating}(P) = \min\{CR_{si}, i \in P\}$$

节点首先检查自己的路由信息表是否存在满足请求声誉值的路径,即路径声誉值比请求声誉值大的路径. 具体做法是针对路由信息表中的路径,在声誉值列表(Rating List)中取出路径上每个节点的声誉值,计算出路径声誉值. 在所有满足路径声誉值大于请求声誉值的路径中,取出路径声誉值最高,跳数最小的路径作为传输路径. 若没有合适的路径,节点就启动路由发现过程. 首先创建一个 RREQ,和其他协议不同的是该 RREQ 要携带一个请求声誉值和一个黑名单. 黑名单中记录着声誉值列表中声誉值小于请求声誉值的节点,即不符合要求的节点,这样可以避免这些不合节点参与路由发现过程.

中间节点收到该 RREQ 后,首先看自己是否收到过该包,若收到过则抛弃;否则首先看自己的路由缓冲区中是否有合适的路径,若有则向源节点 S 发送 RREP,否则继续转发 RREQ,直到找到合适的路径为止. 若经过一段时间没有收到 RREP,节点就再次发送 RREQ 请求,若发送一定次数的 RREQ 仍没有收到 RREP 则放弃寻路,表示没有合适的路由. S-DSR 协议描述见图 3.

```
Source node:
If source S want to send packets to destination D then
    Define a Require Rating
    Find in its Route Cache whether there exists
    proper route (Route's rating > = Require Rating)
    If proper route exists then
    Send Packets
    Else
    broadcast RREQ with Require Rating and Black List
    End if
End if
Intermediate node:
If intermediate node receives the RREQ then
  Find in its Route Cache whether there exists proper route
  If route exists then
    Send back RREP
  Else
  Forward the RREQ until find a proper route or TTL is out
End if
```

图 3　S-DSR 协议

若数据包传输过程中出现断路的情况,拯救包时也要看节点是否有合适的路径,有才拯救,若没有能满足安全需求请求声誉值的路径则不拯救.

在该协议的路由发现过程中,由于设定了一个新的目标请求声誉值,可能存在从源到目的有路,但由于路径声誉值不满足需求而找不到合适路径的情况. 所以在这种情况下 S-DSR 协议发送的 RREQ 的数量可能要比以往的协议要多.

5 模拟环境及实验结果分析

5.1 模拟环境及性能参数

在对网络的性能影响评价中,我们所使用的模拟工具是 Glomosim2.03. Glomosim 是加州大学洛山矶分校并行计算实验室开发的类似于 NS2 和 OPENET 等的模拟工具,它主要是针对无线网络的模拟[12].

模拟的通信模型选用 CBR 流,每个 CBR 流包含 512 字节. 随机选择 3 个节点作为源节点,源节点不停的向目的节点发送 CBR 流,且每 1000 秒随机更新一次源节点. 移动模型采用 Random Waypoint 模型,节点的运动速度为 0～20m/s,节点间链路的带宽为 2Mbps. 模拟运动范围为 1800 * 1800. 测试节点数目分别为 10,主动性攻击节点数分别为 1、2、3 个. 总模拟时间为 9000s. 在模拟过程中 IR 的更新采用的是触发式模式.

在对 S-DSR 的模拟实验中我们通过增加不同数目的主动性攻击节点来为测试 S-DSR 协议对网络攻击的防御能力. 分别测试了请求声誉值为 0.1 和 0.2 情况下的网络性能. 通过分析主动性攻击模型的网络性能的影响以说明 S-DSR 协议的有效性. 主动性攻击模型的基本攻击方法是:(1)攻击节点本身不参与路由请求,不传送数据包.

(2)对收到的所有的 RREQ 都回复 RREP,告知"我有一条只要一跳就能到达目的节点的链路".

(3)转发所有的 RREP 和 RERR.

(4)凡是收到的数据包都抛弃,并且不发送 RERR.

(5)不抢救数据包和 RERR.

为有效比较存在主动攻击节点情况下 DSR 协议与 S-DSR 协议的性能,使用下列参数来进行评价.

(1)包传输率(Packet Delivery Ratio):即网络中所有目的节点收到的包与源节点发出包的比率.

(2)包丢失率(Drop Ratio):即不良节点(主动性攻击节点)丢弃的包与网络中所有节点总发出包的比率.

(3)网络吞吐量(Throughput):单位时间内应用层所有节点吞吐量之和.

(4)RREQ 比率(RREQ Ratio):网络中发出的 RREQ 占整个网络开销的比率.

5.2 模拟结果及性能分析

为了表示方便,在以下所有图中我们以 DSR(i)表示网络中存在 i 个主动攻击节点下 DSR 协议的性能曲线,以 S-DSR(i)表示网络中存在 i 个主动攻击节点下 S-DSR 协议的性能曲线.

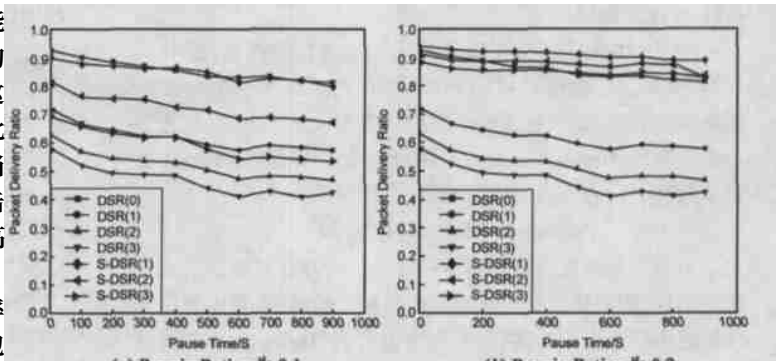
从图 4 可以看出,随着 Pause Time 的增加,DSR(0)的包传输率随之缓慢降低,在 81%～91%之间. 当存在主动攻击节点时,网络中包传输率明显降低,而且随着网络节点移动性的降低(Pause Time 增加),DSR 协议包传输率也随之降低. 这是因为主动攻击节点向其他节点发送了假的路由信息,一旦包传输到攻击节点就被抛弃. 当攻击节点数达到 3 个时,DSR 协议包传输率下降为 45%左右. 由于节点要寻找到合适的路径才进行包的传输,因此 S-DSR 协议传输率较高,甚至会超过没有

攻击节点的 DSR 原协议. 这是由于该防御模型可能会出现误判的情况,会把链路不稳定、移动性较强的节点误判为错误节点而不使用该节点传输数据,这样也可以使传输率上升,因此会出现 S-DSR 协议比原 DSR 协议结果要好的情况. 从图中可以看出,当请求声誉值较高时,包传输率较高. 在存在主动攻击节点时,S-DSR 协议比 DSR 协议在包传输率方面高大约 30 %左右.

如图 5 所示,随着攻击节点数的增加,包丢失率不断增大. 存在一个攻击节点时,攻击节点丢失的包占总发出包的 25 %～30 %. 当攻击节点个数达到 3 个时,主动性攻击节点由于发布假信息会吸引很多的数据包,因此 DSR 协议的包丢失率最高可达到将近 55 %. 在 Require Rating 为 0.1 时,S-DSR 协议出现一个攻击节点丢失的包只占总发出包的比率最高不到 15 %;当 Require Rating 为 0.2、攻击节点为 1 时,S-DRS 协议的包丢失率最高为 7 %. 当攻击节点数达到 3 个时,Require Rating 为 0.1 时 S-DSR 协议的包丢失率最高为 40 %,Require Rating 为 0.2 时 S-DSR 协议包丢失率最高为 15 %. 因此可以看出,在存在主动攻击节点时,S-DSR 协议的包丢失率比 DSR 协议要小的多,这是因为在 S-DSR 协议中对攻击节点的使用率明显减少.

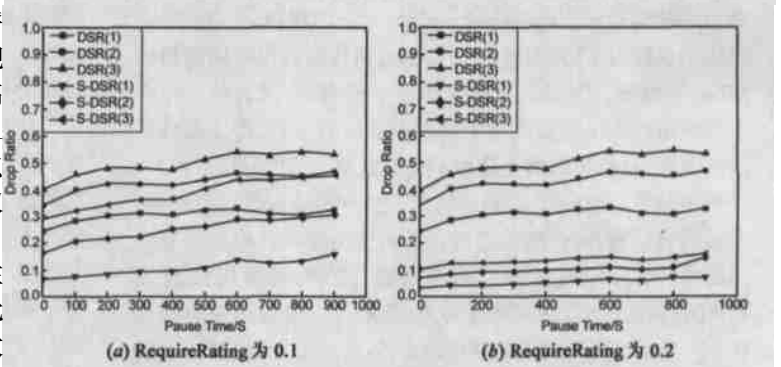
从图 6 可以看出,DSR 协议网络的吞吐量在没有攻击节点的情况下为 38000bps～43000bps 之间. 出现攻击节点后 DSR 协议的网络吞吐量明显下降,当攻击节点数为 3 个时 DSR 协议吞吐量最低下降为 20000bps. 而在 S-DSR 协议中,由于增加了请求声誉值的寻路指标造成面组请求的路减少,从而使得被正常传输得负荷相对于 DSR 来说要少,所以吞吐量有所下降. 如果降低 Require Rating 可以使网络吞吐量增高,但同时带来的就是网络包传输率的降低.

图 7 显示的是随着 Pause Time 的变化以及攻击节点数的不同,RREQ 占网络总开销的比率,体现了网络用于寻路的附加开销. 网络的总开销包括网络中所有的 RREQ、RREP 以及 RERR. 从图 7 中可以看出,当出现主动攻击节点时,DSR 协议中 RREQ 所占比率有所上升,但上升幅度不大. 这是由于出现了攻击节点,但由于没有错误报告节点认为寻路成功,在一定时间内都不会认为路由失败,直到从网络其他层获得链路不通的报告才会重新寻路. 因此 RREQ 比率会有一定上升,但幅度不大. 而在 S-DSR 协议中,根据节点声誉值的判断可以在较短的时间内就判断出哪些是不良节点,从而避免这些节点参与路由,但因此会使网络中的可用节点减少,从而增加了 RREQ 的发送. 而且当路由的安全需求有所变化时也会对 RREQ 的比率有所影响. 因为安全需求越高,满足需求的路径就越少,从而需要花费大量的 RREQ 用于寻找合适的路由. 因此在 S-DSR 中,RREQ 所占比率有很大的增加.



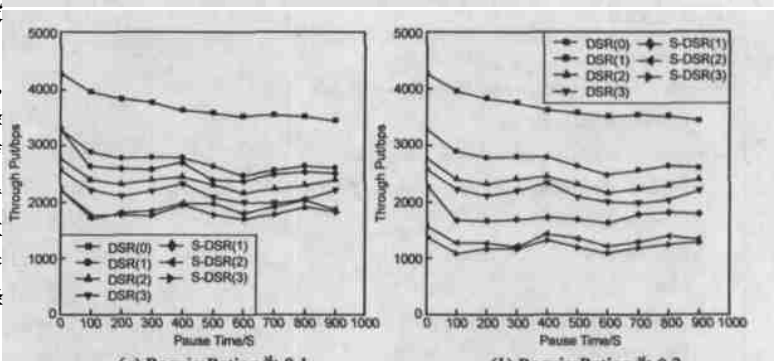
(a) RequireRating 为 0.1 (b) RequireRating 为 0.2

图 4 S-DSR 与 DSR 协议包传输率的比较



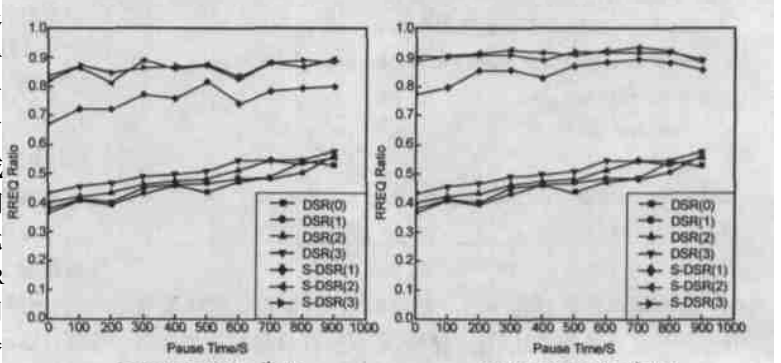
(a) RequireRating 为 0.1 (b) RequireRating 为 0.2

图 5 S-DSR 与 DSR 协议包丢失率的比较



(a) RequireRating 为 0.1 (b) RequireRating 为 0.2

图 6 S-DSR 与 DSR 协议吞吐率的比较



(a) RequireRating 为 0.1 (b) RequireRating 为 0.2

图 7 S-DSR 与 DSR 协议 RREQ 比率的比较

存在一个攻击节点时,S-DSR 中其他节点对攻击节点声誉值的平均值变化情况如图 8 所示,该曲线表示了网络中出现一个攻击节点时,请求声誉值为 0.2 的条件下 S-DSR 协议中其他节点对该攻击节点声誉值的平均值随时间的变化产生的结果. 从图 8 可以看出,攻击节点声誉值的初始值为 0.5,随着时间的变化,对该攻击节点平均声誉评价值不断降低. 声誉值下降的时间过程体现了声誉值传播更新的过程,到 2000s 时平均声誉值就下降到了 0.2 左右,因此表明 2000s 以后网络中其他节点很少会再使用该攻击节点,从而达到了防御的目的.

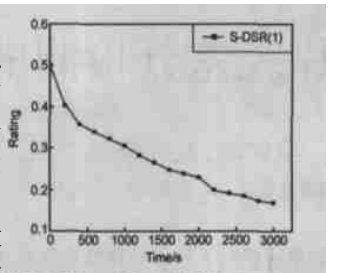


图 8　存在一个攻击节点时,S-DSR 中其他节点对攻击节点声誉值的平均值变化情况

6　结束语

本文在系统分析移动自组网络的攻击特点和目前针对网络攻击的主要防御技术的基础上,提出了基于声誉机制的防御模型,以提高网络的包传输率. 在以前的安全路由研究中,虽然大多采用邻居监控的方式进行对节点行为的评价,但多数只是给出监控框架模型,没有给出具体的评价方式例如如何邻居进行监控、怎样进行节点间的信息,而且不能根据用户自己的需求来定义安全级别.

本防御模型根据声誉监测的方式,根据邻居节点的监控和网络中节点信息的交换来更改节点的声誉值. 节点在寻路时首先确定自己的需求请求声誉值,在声誉值列表中查找声誉值小于请求声誉值的节点,并放入黑名单中,然后把请求声誉值和黑名单放入 RREQ 中寻路,这样就可以避免使用攻击节点,从而使之隔绝.

基于声誉机制的防御模型,本文提出了一种新的网络安全路由协议 S-DSR. 实验结果表明 S-DSR 协议在包传输率、包丢失率方面比攻击模型有很大的改进. 但由于增加了请求声誉值的寻路指标,使得网络中满足请求的路径减少是的吞吐量有所下降.

参考文献:

[1] 王建新,邓曙光,陈松乔,陈建二. 移动自组网络中一种基于选播策略的路由恢复方法[J]. 通信学报,2003,24(10):172 - 176.
Wang Jianxin, Deng Shuguang, Chen Songqiao, Chen Jianer. A route recovery method based on anycast policy in mobile ad hoc networks[J]. Journal of China Institute of Communications, 2003, 24(10): 172 - 176 (in Chinese).

[2] Sergio Marti, T J Giuli, Kevin Lai, Mary Baker. Mitigating routing misbehavor in mobile ad hoc networks[A]. In Proceedings of MOBICOM 2000[C]. Boston, 2000. 255 - 265.

[3] Levente Buttyan, Jean-Pierre Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks[R]. Technical Report DSC/2001/046, EPFL-DI-ICA, August 2001.

[4] S Buchegger, JL Boudec. Performance analysis of the CONFIDANT protocol: cooperation of nodes-fairness In dynamic ad-hoc networks[A]. In Proceeding of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)[C]. Lausanne, 2002. 226 - 236.

[5] S Buchegger, JL Boudec. Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks[A]. In Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing[C]. Canary Islands, Spain, 2002. 403 - 410.

[6] David B Johnson, David A Maltz, Yih-Chun Hu, Jorjeta G Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Network[S]. draft-ietf-manet-dsr-07.txt, 2002.

[7] Pietro Michiardi, Refik Molva. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile Ad hoc networks[A]. The Sixth IFIP Conference on Security Communications and Multimedia (CMS 2002)[C]. Portoroz, Slovenia, 2002. 107 - 121.

[8] Hao Yang, Xiaoqiao Meng, Songwu Lu. Self-organized network-layer security in mobile ad hoc networks[A]. Proceedings of the ACM Workshop on Wireless Security[C]. Atlanta, GA, USA, 2002. 11 - 20.

[9] C Perkins, E Royer, S Das. Ad Hoc on-Demand Distance Vector Routing[S]. Internet Draft, draft-ietf-manet-aodv-10.txt, 2002.

[10] S Yi, P Naldurg, R Kravets. Security-Aware Ad-Hoc Routing for Wireless Networks[R]. UIUCDCS-R-2001-2241 Technical Report, 2001.

[11] P Resnick, K Kuwabara, R Zeckhauser, E Friedman. Reputation systems[J]. Communications of the ACM, 2000, 43(12): 45 - 48.

[12] http://pcl.cs.ucla.edu/projects/glomosim[OL].

作者简介:

王建新　男,1969 年生于新疆托里,教授,博士生导师,主要研究领域为路由算法及网络性能评价. E-mail: jxwang@mail.csu.edu.cn

张亚男　女,1979 年生于河北石家庄,硕士研究生,主要研究移动自组网络中的路由协议和网络安全.

王伟平　女,1969 年生于江苏苏州,博士,副教授,主要研究领域为网络信息安全.

卢锡城　男,1946 年生于江苏靖江,中国工程院院士,教授,博士生导师,主要研究方向为 FGG 实现技术、并行与分布处理技术、网络与通信.