广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):270~274
Vol. 23,No. 4 November 2007

移动 Ad Hoc 网络中一种匿名攻击及防御策略研究*
Research on a Kind of Anonymous Attack and Defence Strategies in Mobile Ad Hoc Network

沈岚岚,董荣胜
SHEN Lan-lan,DONG Rong-sheng

(桂林电子科技大学计算机与控制学院,广西桂林 541004)
(School of Computer Science and Control,Guilin University of Electronic Technology,Guilin,Guangxi,541004,China)

摘要:应用概率模型检测工具PRISM证实统计暴露攻击能够破坏ANODR协议的匿名性。为此改进ANODR协议的节点输出方式,提出全局同步发送策略和组同步发送策略。概率模型检测表明,组同步发送策略适应移动Ad Hoc网络匿名通信需求,可防范统计暴露攻击,并能提供低延迟,受节点移动影响小的匿名服务。

关键词:统计暴露攻击 匿名通信 移动Ad Hoc 概率模型检测
中图法分类号:TP393 **文献标识码**:A **文章编号**:1002-7378(2007)04-0270-05

Abstract: By using probabilistic model checking, this paper proves that anonymous protocol ANODR cannot provide anonymity under statistical disclosure attack. In light of this, the strategy for node output in ANODR is improved and global and grouped synchronization strategies are proposed. Checked by probabilistic model, the grouped synchronization strategy can meet the requirements of mobile ad hoc networks, defend statistical disclosure attack, provide low-latency communication immune to mobility.

Key words: statistical disclosure attack, anonymous communication, mobile Ad Hoc networks, probabilistic model checking

移动Ad Hoc网络匿名通信,因其无线传输、动态拓扑和资源受限等特点,易受匿名攻击尤其是被动匿名攻击威胁。统计暴露攻击[1]是2003年提出的一种被动攻击方式,它依据概率的观点,利用统计和排除的方法,通过计算出与目标节点通信的节点所接受消息的概率分布,而得出目标节点的通信对象。采用这种攻击方式的攻击者,无需主动发起攻击行为,也不需要知道消息内容,只需要进行窃听攻击和计算,容易实施且隐蔽性强。

ANODR协议[2]是移动Ad Hoc网络的一个典型的匿名路由协议。本文通过概率模型检测工具PRISM[3]证实统计暴露攻击能够破坏ANODR的匿名性。因此我们对ANODR的节点输出方式进行了改进,提出了同步发送的消息输出策略,概率模型验证表明改进的策略能在移动环境中抵御统计暴露攻击这种匿名攻击方式,增强了匿名性。

1 统计暴露攻击思想和步骤[1]

统计暴露攻击属于被动攻击,攻击目标是获取某个发送者A的通信对象。假设攻击者知道目标节点A的通信对象个数,有能力进行全局窃听,即能够观测到所有节点的所有的输入输出消息。攻击的基本思想和步骤如下[4]。

(1)记录观察目标A不发送消息时的接收向量和A发送消息时的接收向量。向量中的每个元素代表每个节点在第i轮中的接收概率,例如每轮发送消息数为b,若某接收者在第i轮接收到的消息数为1,则该向量中该接收者对应的值为$1/b$,没有收到则为0。

(2)计算接收向量的统计概率平均值,假设A

收稿日期:2007-09-20
作者简介:沈岚岚(1978-),女,硕士研究生,主要从事形式化方法,网络安全研究。
*广西研究生教育创新计划项目(2007105950812M17)资助。

不发送消息时观察了 t' 轮,A 发送消息时观察了 t 轮,计算公式如下:$\bar{U}=\frac{1}{t'}\sum_{i=1}^{t'}\vec{u}_i$,$\bar{O}=\frac{1}{t}\sum_{i=1}^{t}\vec{o}_i$。

(3) 假设 $\bar{m}$ 为每轮 A 平均发送的消息数,$\vec{v}$ 为 A 的接收者的接收概率向量。则根据大数定律有 $\bar{O}\approx\frac{\bar{m}\vec{v}+(b-\bar{m})\bar{U}}{b}$,求出 $\vec{v}\approx\frac{1}{\bar{m}}[b\cdot\bar{O}-(b-\bar{m})\bar{U}]$。

(4) 理论上只要能达到一定的统计量,$\vec{v}$ 中不为 0 的向量均可被判定为 A 的通信对象。

2 ANODR 对统计暴露攻击的匿名性验证

2.1 ANODR 的节点输出策略

由于实施统计暴露攻击时不需要知道消息内容,所以本文仅对消息的输出方式进行建模和分析。

为了防范时间攻击,ANODR 协议借鉴 MIX-NET 的方法,节点在输出时采用定时填充假消息策略,将其记为 sl (m,t),m 为阈值,t 为定时周期。节点每隔周期 t 发送一次消息。在定时周期 t 内,若节点需发送的消息数 $n<m$,则生成 $dm=m-n$ 个假消息随机发送给该节点的邻居节点,否则,不生成假消息,发送 n 个消息。用概率有限状态机表示 sl 如图 1 所示。

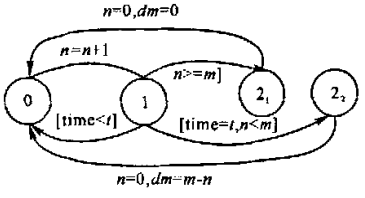

图 1 sl (m,t) 的有限状态机

0:接收;1:执行刷新策略;2_1:填充假消息发送,随机选择假消息的接收者;2_2:不填充假消息发送。

2.2 ANODR 匿明性验证

2.2.1 Ad Hoc 网络环境和参数设置

假设 Ad Hoc 网络满足下列条件:

(1)网络中各节点可独立地自由移动。

(2)网络信道是理想的,忽略相关延迟、拥塞、丢失等情况。

(3)节点通信模型为 Uniform,即各节点均匀的发送消息给所有接收者,但发送顺序随机。设在一个时间单位内,各节点发送 1 个消息。即 $\bar{U}=(1,1,1,\cdots,1)$。

(4)假设目标节点 A 的接收者个数为 1,设 $\vec{v}=(1,0,0,\cdots,0)$。

2.2.2 PRISM 建模

用 PRISM 语言描述图 1 的节点输出方法和攻击模型,建立离散时间马尔可夫链(DTMC)概率模型,性质规约为概率计算树逻辑(PCTL)[5]。

PRISM 系统由模块和变量组成,每个模块代表一个系统进程,模块间的通信通过全局变量或同步化的共同活动标记来完成。模块描述行为的语句根据有限状态机分析的状态转换来执行。PRISM 状态转换描述形式如下:

[sym] <guard> -> <command>

sym 是同步符号,<guard>是系统变量之上的谓词,若<guard>为 true,系统执行<command>命令。如果转换是带有概率选择的,离散概率的形式为:

[] <guard.> -> <prob1>: <command1> + … + <probN>: <commandN>

部分代码如下:

```
Probabilistic      //概率模型的类型是 DTMC
const int max;     //消息最大值
const int m=6;     //设置阈值
const int u1=1;    …     //设置向量 u
formula n=q0+q1+q2+q3+…;
formula finish = r=ROUNDS;     //结束条件

module Attacker     //攻击者行为模块
  a: [0..3];     //状态变量
  r: [0..ROUNDS];     //攻击轮数
  o0: [0..max];     //节点 A 发出的消息
  o1: [0..max];o2: [0..max];…     //向量 o 各分量
  v1: [0..max];v2: [0..max]; …     //向量 v 各分量
  [s0] a=0 -> o0'=min(o0+1,max);
  [s1] a=0 -> o1'=min(o1+1,max);
       …     //观测记录 o 的分量
  [fs] true -> a'=1 & r'=min(r+1,ROUNDS);//一轮消息发送完成
  []a=1-> a'=2 & v1'=max(o1+o0-u1*r,0) & v2'=max(o2-u2*r,0) …;     //计算向量 v
  []a=2 & finish ->a'=3;
  []a=2 & ! finish ->a'=0;
endmodule

module MIX     //节点输出行为模块
…     //图 1 中有限状态机模型的状态转换语句
```

```
endmodule

rewads "rounds"
  [fs] true: 1;      //一轮发送完成
endrewards
rewards "delay"
  [rcv] true: 1;     //一个定时周期
endrewards
rewards "overhead"
  [dm] true: 1/m;    //填充假消息比率
endrewards
```

2.2.3 ANODR 对统计暴露攻击的匿名性验证

采用探测率来衡量协议的匿名性。探测率定义为攻击者成功确立所观测的节点的输入输出关系的概率。当攻击成功时，向量 v 中应该只有 $v1$ 不为 0，其余分量均为 0。其 PCTL 描述如下：

P=? [true U a=3 & v1>0 & v2=0 & v3=0 & …]

这里的"P=?"，可以得出满足规约的概率数值是多少。

移动 Ad Hoc 网络中节点的自由移动，会导致目标节点所处区域的节点密度也会有所改变，对节点处于不同密度的情况分别进行检验，当 $rx=6$，$t=1$ 时，检测结果如图 2 所示。从图 2 可以看出，在节点密度 $N>=4$ 时，探测率最终都能达到或收敛于 1，即攻击者能够达到攻击目的，找到目的节点的通信对象；随着节点密度的增大，探测率达到 1 所需要的攻击轮数也随之减少，这是由于 ANODR 协议中虽然考虑到移动性的影响，填充的假消息数量是动态的，但阈值 m 是固定值，随节点密度的增大，节点在给定周期内需转发的消息数 n 也增加了，当 $n>m$ 时，混淆策略不起作用，此时该协议无法提供匿名保护。

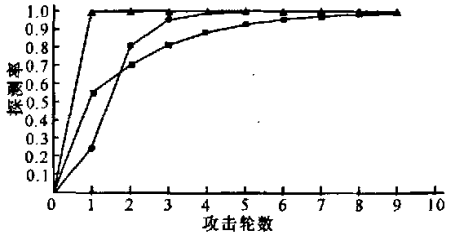

图 2 s1(6,1)的探测率

■：$N=4$；●：$N=5$；▲：$N>=6$。

3 统计暴露攻击的防御策略研究

假设各接收者的接收概率相同，此时攻击者无法通过统计方法排除背景，即可达到隐藏输入输出关系的目的。基于此设想，我们对 ANODR 协议的假消息的填充方式进行了改进，提出以下两种同步发送的输出策略 s2 和 s3。

3.1 同步发送策略

3.1.1 全局同步发送 s2(t)

全局同步发送策略 s2 的基本思想是对每一个邻居节点都同步发送消息，使接收向量中各个分量的值相等，即在给定时间 t 内节点的每一个邻居节点都接收相同数量的消息。

节点需对其所有邻居节点一一建立消息发送队列 $q_i(1\leqslant i\leqslant N-1)$，每隔周期 t 发送消息。发送时从 $i=1$ 开始顺序检查，若 $q_i>0$，发送此队列中的一个消息；若 $q_i=0$，填充一个假消息再发送。不断重复以上过程，直至发送队列全部为空。图 3 为 s2 策略的有限状态机模型。

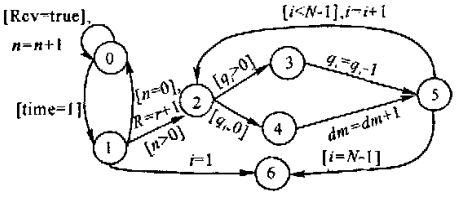

图 3 s2 (t) 的有限状态机模型

0：接收；1，2：执行刷新策略；3：不填充假消息发送；4：填充假消息发送；5，6：消息发送完成；i：相邻节点编号；dm：发送的假消息数量；q_i：接收节点为 i 的消息数量。

3.1.2 组同步发送 s3(g,t)

s2 在各邻居节点接收消息数量差异较大，只有极少的邻居节点接收消息等情况下，产生的假消息数额较大，会耗费大量网络资源，不利于在 Ad Hoc 网络环境中应用。我们对 s2 进行了改进，增加了邻居节点分组功能，g 为每组最小成员数。将邻居节点分成若干组，使各组成员数 $g\leqslant G_i<2g(1\leqslant i\leqslant j$，$j$ 为最大的组序列号)，发送时，查找接收节点所在组，在此组内实施 s2 策略。分组算法的有限状态机模型如图 4 所示。

图 4 中，当新的邻居节点的到来时(状态 2)，将其加入到最后一组 j 中。若 $G_j=2g$，则将 j 平均分为 2 组；反之若原有节点移出通信范围(状态 3)，假设此节点属于第 i 组，从第 j 组中随机选择 $g-G_i$ 节点并入 i 组(状态 3、7、8 和迁移)。如有 $G_j<g$(状态 6)，将第 j 组节点并入 $j-1$ 组。

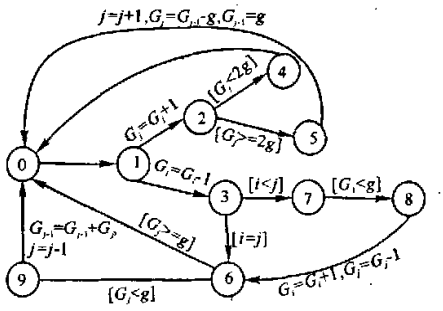

图 4 s3 (g,t) 的有限状态机模型

0:静止;1:执行分组策略;2:增加新节点;3:第 i 组节点减少;4:不分组;5,6,7,8,9:分组。

3.2 同步发送策略匿名性的模型验证

同步发送使各接收概率向量中的各分量值相等,攻击者使用统计暴露攻击得到的概率向量中的各分量要么全为 0,要么全不为 0,且各分量值相等。当概率向量不为 0 时,攻击者只能随机判断观测目标节点 A 的通信对象。图 5 显示了 s2 和 s3 这两种策略的探测率,可以看出,随着节点密度的增大,s2 和 s3 的探测率都不会达到 1。

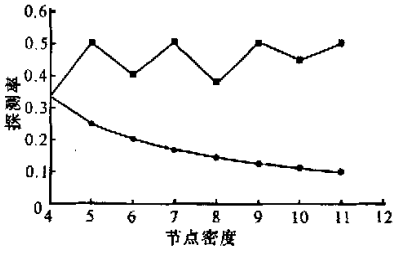

图 5 同步发送略的探测率

●:s2(1);■:s3(2,1)。

3.3 网络性能的检测评估

安全性和网络性能的折衷是移动 Ad Hoc 网络的安全设计的一个基本原则,匿名技术也要遵循这一原则。移动 Ad Hoc 网络中,平均时延是一必须考虑的因素。由于动态拓扑结构,若时间延迟过大,会使建立好的路由在会话完成前失效。此外,节点资源受限需要节约资源,减少假消息等额外开销。因此,下面将对平均时延与额外开销这两项性能指标进行分析。

3.3.1 平均时延

定义为当 A 的接收者收到 A 所发送的消息时所经历的时间。此时结束条件为:finish= o 0=1。其 PCTL 描述为:R{"delay"}=? [Fa =3]。在 Rewards 中为响应的状态设立了权值,"R=? [F<prop>]",可以得出满足 prop 时所经历的状态的权的平均期望值。检验结果如图6。由于策略 s2、s3与 s1一样采用定时触发机制,故它们的平均时延只与定时周期的设置相关,定时周期越大,时间延迟也就越大。

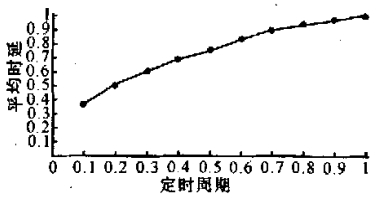

图6 平均时延

3.3.2 额外开销

定义为节点发送的假消息占其发送的所有消息的比率。结束条件为:finish= $v1$ > 0&$v2$ = 0&$v3$ = 0 & …。其 PCTL 描述为:R{"overhead"}=?[Fa = 3]。

验证取不同定时周期 t 的值的结果如图7~9。可以看出,s1产生的额外开销最小,s2的较大,s3对此有所改进,因此我们选择 s3作为 Ad Hoc 网络中防御统计暴露攻击的策略。

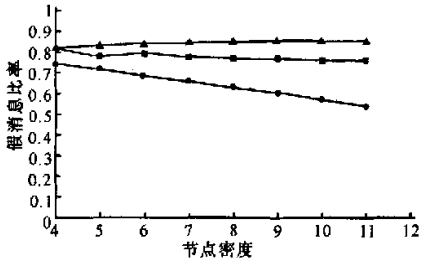

图7 额外开销 (t =0.2)

●:s1(6,0.2);▲:s2(0.2);■:s3(2,0.2)。

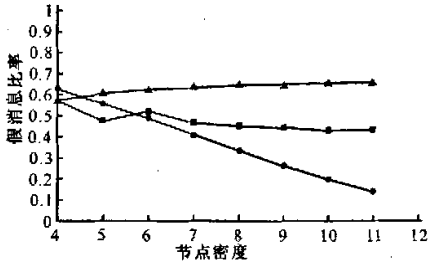

图8 额外开销 (t =0.5)

●:s1(6,0.5);▲:s2(0.5);■:s3(2,0.5)。

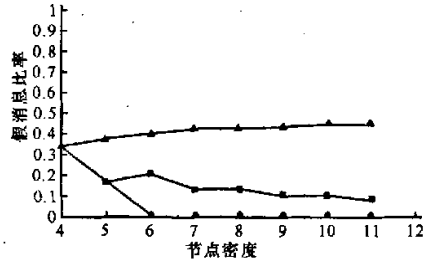

图9 额外开销 (t =1)

●:s1(6,1);▲:s2(1);■:s3(2,1)。

4 结束语

在匿名通信中，当应用加密、认证等技术提供匿名服务，防止攻击者从传送的消息中直接获取通信主体信息或根据消息的位串形式进行路径追踪后，根据时间、数量等通信模式信息而进行的通信分析成为要防范的主要匿名攻击方式之一。本文介绍了一种基于通信分析的被动攻击——统计暴露攻击，概率模型检测表明，统计暴露攻击对典型匿名安全协议 ANODR 攻击有效。因此对 ANODR 的节点输出方式进行了改进，提出了同步发送策略并进行了验证，结果表明，组同步发送策略适应移动 Ad Hoc 网络匿名通信需求，可防范统计暴露攻击，并能提供低延迟，受节点移动影响小的匿名服务。

参考文献：

[1] DANEZIS G. Statistical disclosure attacks: traffic confirmation in open environments: Security and Privacy in the Age of Uncertainty, the 18th International Conference on Information Security (SEC2003)[C]. Athens, Greece, 2003: 421-426.

[2] KONG J, HONG X. ANODR: anonymous on demand routing with untraceable routes for mobile Ad Hoc networks: the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'03)[C]. Annapolis, Md, USA ACM, 2003: 291-302.

[3] Oxford University. PRISM [EB/OL]. [2007-08-20]. http://www.prismmodelchecker.org.

[4] 王伟平，皮润良，段桂华. 匿名系统中统计暴露攻击及防御策略研究[J]. 计算机工程，2006，32(22)：162-165.

[5] 陆天波，方滨兴，孙毓忠. 匿名协议 WonGoo 的概率模型验证分析[J]. 小型微型计算机系统，2006，27(4)：646-650.

（责任编辑：韦廷宗）

美国科学家用计算机成功模拟植物光合作用

美国伊利诺伊大学植物生物学和作物科学教授斯蒂夫·隆表示，他们在实验室成功地用计算机模拟了植物的光合作用，并据此培育出品种更加优良的植物。这种新植物不需要额外增加养份，就可以长出更茂盛枝叶和果实。

首先，研究人员建立了一个可靠的光合作用模型，以便精确模拟植物对环境变化的光合反应。研究人员使用了由美国国家超级电脑应用中心提供的计算资源，在确定光合作用中每种蛋白质的相对数量后，研究人员设计出了一系列连锁微分方程式，每个方程模拟了光合作用中的一个步骤。通过不断的测试和调整模型，研究小组最终成功预测了在真实叶片上进行实验的结果，其中包括叶片对环境变化的动态反应。接下来，研究人员们对模型进行编程，以随机改变光合作用过程中每种蛋白酶的含量水平。

模型运用"进化算法"搜寻各种酶，以提高植物的产量。一旦实验证明某种酶的相对高浓度可以提高光合作用的效率，该模型就会利用此实验结果进行下阶段的测试。研究人员通过这种方法确定了许多可以大大提高植物生产力的蛋白质。这个最新发现也印证了其他一些研究人员的研究结果，他们发现，在基因改造植物中，当这些蛋白质中某一种的含量得到增加，植物产量就会随之提高。斯蒂夫·隆教授说："通过改变氮的投入，我们几乎可以使光合作用效率提高两倍。然而，随之而来的一个显而易见的问题是，为何植物的生产力可以提高如此之多，为何植物还未能进化到可以自身进行如此高效的光合作用。这个问题的答案可能在于，进化的目的是生存和繁殖，而我们实验的目的是增加产量。模型中显示的变化很可能会破坏植物在野外的生存，因此这种模拟只适合在农民的农场中进行。"斯蒂夫·隆教授认为，目前全球每年通过光合作用能够固定2200亿吨生物质，相当于世界上所有能耗的10倍。要植物产生更多的生物质，就需要提高光合效率。通过高新技术转化，我们甚至可以让有些藻类在光合作用的调节与控制下直接产生氢。光合作用与农业的关系同样密切，水稻与小麦的高产品种的光合作用效率可以达到1%至1.5%，而甘蔗或者玉米的效率则可达到5%或者更高。如果人类可以人为地调控光能利用效率，农作物产量就会大幅度增加。要彻底揭开这一谜团，在很大程度上依赖于多学科的交差进行研究，依赖于高度纯化和稳定的捕光及反应中心复合物的获得，以及当代各种十分复杂的超快手段和物理及化学技术的应用与理论分析。事实上，当代几乎所有的物理、化学学科中，最先进的设备与技术都可以用到光合作用研究中来。

（据科学网）