第 34 卷 第 18 期 计 算 机 工 程 2008 年 9 月
Vol.34 No.18 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)18—0157—04 文献标识码：A 中图分类号：TP309

MANET中MIX策略的分析与设计

沈岚岚，董荣胜
(桂林电子科技大学计算机与控制学院，桂林 541004)

摘 要：在 MANET 匿名通信中，使用加密等技术防止攻击者通过消息内容进行匿名攻击，并采用 MIX 输出策略防范攻击者根据通信模式进行的匿名攻击。基于概率模型检测方法，该文分析几种典型的 MIX 输出策略在 MANET 中的应用。结果显示，这几种策略无法防范统计暴露攻击等被动攻击，且防范攻击的能力、平均时延和开销等性能会受到移动性的影响。该文提出同步发送的 MIX 输出策略，能更好地防御匿名攻击，具有延迟低、受节点移动影响小的特点。
关键词：匿名通信；概率模型检验；MIX 策略

Analysis and Design of MIX Strategies in MANET

SHEN Lan-lan, DONG Rong-sheng
(School of Computer Science and Control, Guilin University of Electronic Technology, Guilin 541004)

【Abstract】 In anonymous communication of MANET, both encryption and MIX strategies are used to defend attacks according to contents and communication pattern. This paper analyzes several known MIX strategies in MANET by probabilistic model check. Results show that these strategies can not defend passive attacks as statistical disclosure attack. In addition, the anonymity, average delay and overhead provided by them would be affected by mobility. Synchronization strategy is proposed. The method has better anonymity, low-latency and little influence by mobility.
【Key words】 anonymous communication; probabilistic model check; MIX strategies

1 概述

匿名安全是MANET安全设计中的重要问题。MANET具有无线传送、节点自由移动和能量受限等缺点，且不能直接应用于传统的匿名技术。当前MANET的匿名协议(ANODR[1],ASR[2])采用逐跳加密和认证来改变消息输入/输出的位串形式，可抵制基于内容的路由追踪以及重放、n-1等匿名攻击。然而，仅靠加密技术不能完全保证通信匿名，攻击者还可通过分析时间、数量等信息来追踪路由，MIX输出策略可通过改变消息输出的顺序和时间，混淆攻击者的观测，达到隐藏通信流中的通信关系的目的，抵御此类攻击。

本文研究了 MIX 策略在 MANET 中的应用，使用概率模型检测技术来验证几种典型的 MIX 策略所提供的匿名性，分析节点密度变化的情况，移动性对这些策略的影响，提出适用于 MANET 的输出策略。

2 相关研究

2.1 典型的 MIX 输出策略

自从MIX技术提出以来，人们提出了许多MIX输出策略[3]，这些策略主要集中研究触发消息输出的条件和输出哪些消息。触发条件有阈值和定时 2 种；输出形式有确定性和不确定性 2 种。表 1 列出了几种典型的MIX输出策略。

表 1 几种典型 MIX 策略

编号	侧路名称	参数	策略说明
s1	阈值策略	(m)	若 n=m，发送 n 个消息
s2	阈值消息池策略	(m,f)	若 n=m，随机发送 m-f 个消息
s3	阈值二项式策略	(m,p)	若 n=m，对每个消息以概率 p 发送
s4	定时随机假消息策略	(m,t)	每隔时间 t 发送，若 n<m，填充 m-n 个假消息；若 n≥m，发送 n 个消息

s1～s3 为阈值触发；s2,s3 增加了消息输出的随机性；s4 为定时触发，是 MANET 匿名协议 ANODR 采用的策略。符号说明如下：n 为未发送消息数；m 为阈值；t 为定时周期；f 为消息池大小；p 为消息发送概率。

2.2 攻击模型

随着匿名技术的不断发展，针对它们的攻击方式也不断丰富。统计暴露攻击[4-5]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，通过计算与目标节点通信的节点所接收消息的概率分布，而得出目标节点的通信对象。这种攻击方式不必知道消息内容，只需窃听和进行一定的计算，在MANET这样一个开放的环境中，具有隐蔽的特点，且易于实现。

假设攻击者有能力进行全局窃听，即能够观测到所有节点的输入/输出消息。攻击思想和步骤如下：

(1)记录观察目标A不发送消息时的接收向量$\boldsymbol{u}_i$和A发送消息时的接收向量$\boldsymbol{o}_i$。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 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：

$$\overline{\boldsymbol{U}}=\frac{1}{t'}\sum_{t'=1}^{t'}\boldsymbol{u}_i,\quad \overline{\boldsymbol{O}}=\frac{1}{t}\sum_{t=1}^{t}\boldsymbol{o}_i$$

(3)假设 $\bar{m}$ 为每轮 A 平均发送的消息数，$\boldsymbol{v}$ 为 A 的接收者的接收概率向量。则根据大数定律有

基金项目：广西自然科学基金资助项目(0542052)
作者简介：沈岚岚(1978－)，女，硕士研究生，主研方向：形式化方法，网络安全；董荣胜，教授
收稿日期：2007-10-25 **E-mail：**shenll@mails.guet.edu.cn

$$\overline{\boldsymbol{O}} \approx \frac{\bar{m}\boldsymbol{v} + (b-\bar{m})\overline{\boldsymbol{U}}}{b}$$

求出

$$\boldsymbol{v} \approx \frac{1}{\bar{m}}[b\cdot\overline{\boldsymbol{O}} - (b-\bar{m})\overline{\boldsymbol{U}}]$$

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

3 概率模型检验和结果分析

3.1 环境和参数设置

(1)网络中各节点可独立地自由移动。

(2)网络信道是理想的，可以忽略相关延迟、拥塞、丢失等情况。

(3)节点通信模型为 Uniform，即各节点均匀地发送消息给所有接收者。设在一个时间单位内，$\overline{\boldsymbol{U}} = (1,1,\cdots,1)$，即各节点都发送 1 个消息。

(4)设目标节点 A 的接收者个数为 1，设 $\boldsymbol{v} = (1,0,0,\cdots,0)$。MANET 为了能够最大限度地利用资源，当有多对节点进行通信时，会尽量选择不相交的路由，因此，该设想可成立。

3.2 PRISM 建模

概率模型检测是一种可以验证存在随机行为系统的正确性、可靠性和系统性能的形式化分析技术，其检测结果不是简单地标识转换存在与否，而是对状态间转换的概率进行编码，对转换的可能性进行数值计算。PRISM 是目前较为成功的概率模型检测工具，已成功地应用于多个案例分析中，包括网络协议、无线通信终端、轮询系统、分布算法、工作站集群等。用 PRISM 对 2.2 节的攻击模型和表 1 的 MIX 输出策略建模，模型为离散时间马尔可夫链(DTMC)，性质用概率时序逻辑(PCTL)进行描述。

PRISM系统由模块和变量组成，变量有全局变量和模块内的局部变量，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。对攻击者行为和节点执行输出策略行为建立模块，分别用变量a和m表示模块内的状态，$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots$为向量$\boldsymbol{v}$的各分量，$\boldsymbol{o}_1,\boldsymbol{o}_2,\cdots$为向量$\boldsymbol{o}$的各分量。

PRISM 描述形式为：[sym] <guard> -> <command>。sym 是同步符号。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>

rewards 语句可以为相应转换设置权，形式为

[action] <guard>: <reward>

当转换为 action 且<guard>为 true，可获得<reward>值。通过 R{}=? [F <prop>]，计算满足性质 prop 时所经历的路径的权的数学期望值。

3.3 性质规约和结果分析

性质 1 匿名性

(1)探测率(p)

衡量各策略的匿名性，探测率定义为攻击者成功确立节点的输入/输出关系的概率。PCTL 规约为

P=? [true U v1>0 & v2=0 & v3=0 & …]

其中，“ P=? ”表示满足规约的概率数值。根据 2.2 节中的描述，当攻击成功时，应该只有$\boldsymbol{v}_1$不为 0，其余分量均为 0。

当节点密度 N=5 时，验证结果见图 1。探测率随攻击轮数 r 的增加，都能达到或收敛于 1，即攻击者能够达到攻击目的，正确确立目的节点的通信对象。

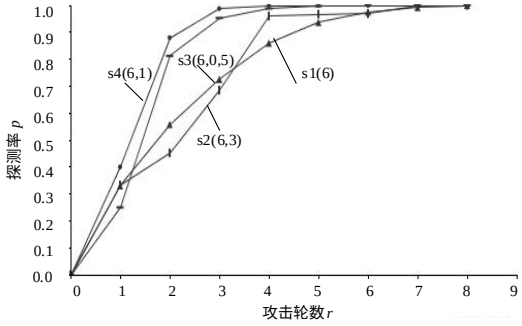

图 1 节点密度 N=5 时的探测率

(2)平均攻击轮数(r)

当各策略探测率相同时，可用平均攻击轮数衡量其抵御攻击的能力。这里将平均攻击轮数定义为当探测率达到或近似 1 时，攻击轮数的数学期望值。将结束条件设置为

finish= v1>0 & v2=0 & v3=0 & …

平均攻击轮数的 PCTL 表示为

R{“r”}=? [F a=finish]

由于节点自由移动会导致目标节点所处区域的节点密度不同，因此图 2 验证了不同节点密度时的情况，并用以分析移动性对各策略的影响。s2,s3 的攻击轮数与节点密度成正比。在 s1 中，节点密度接近阈值时，匿名性较差。而在 s4 中，当节点密度大于等于阈值时，几乎不能抵挡攻击。

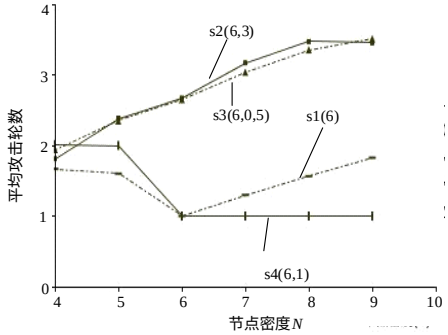

图 2 m=6 时的平均攻击轮数

性质 2 时间延迟(d)

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

其中，$\boldsymbol{o}_0$为A的接收者实际收到的从A发出的消息数量。PCTL 表示为

R{“d”}=? [F a=finish]

结果见图 3。可以看出，s4 对消息的延迟最少，且不受节点移动的影响。

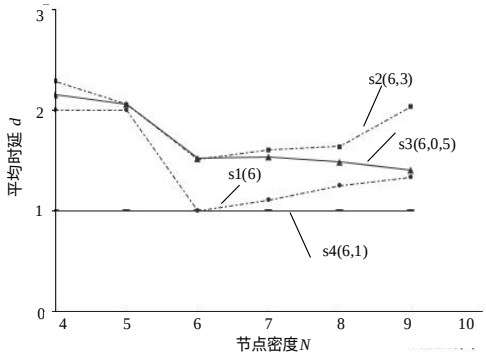

图 3 m=6 时的平均时延

性质 3 额外开销(*oh*)

MIX 节点发送的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 & …

PCTL 为

R{“oh”}=? [F a=finish]

在 s1～s4 中，只有 s4 采用填充假消息的方法，结果见表 2。

表 2　s4(6)的额外开销

节点密度 *N*	额外开销 *oh*
4	0.333
5	0.167
6	0.000
7	0.000
8	0.000
9	0.000

从以上结果可以看出，这几种 MIX 输出策略均不能抵御统计暴露攻击，而且随着节点密度的变化，对攻击的抵御能力及网络性能的影响也有不同。s1～s3 策略的匿名性的获取是以时间为代价的，s2,s3 的匿名性最好，但消息延迟也最大，s4 的匿名性则是靠牺牲部分系统资源获得，因此，时间延迟最少，且不受节点移动的影响。

4　同步发送的 MIX 策略

MANET 的动态拓扑决定通信时延不能太大，否则会导致传送路径在对话未完成之前失效。因此，可以考虑使用 s4 的定时触发方式，但对其假消息的填充方式进行改进。

当各接收者的接收概率相同时，攻击者无法通过统计方法排除背景，找出接收概率高的某个节点，就可以达到隐藏输入/输出关系的目的。基于此思想，笔者提出以下 2 种同步发送策略：s5,s6。

4.1　全局同步发送策略 s5(*t*)

全局同步发送策略 s5 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，即在给定时间周期 *t* 内，节点的每一个邻居节点都接收相同数量的消息。

节点需要对所有邻居节点建立消息发送队列$q_i(1\le i\le N\text{-}1)$，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 4 为该策略的有限状态机模型。

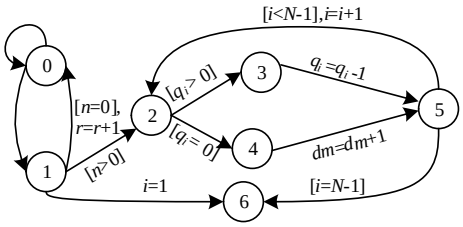

图 4　s5 的有限状态机模型

在图 4 中，0 表示接收；1,2 表示执行刷新策略；3 表示不填充假消息发送；4 表示填充假消息发送；5,6 表示消息发送完成；*i*表示相邻节点编号；*dm*表示发送的假消息数量；q_i 表示接收节点为*i*的消息数量。

4.2　组同步发送策略 s6(*g*,*t*)

组同步发送策略s6 是对s5 的改进，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$g\le G_i<2g(1\le i\le j$，*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s5 策略。分组算法的有限状态机模型如图 5。其中，0 表示静止；1 表示执行分组策略；2 表示增加新节点；3 表示第*i*组节点减少；4 表示不分组；5,6,7,8,9 表示分组。

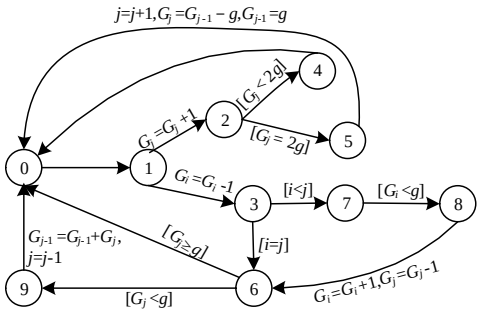

图 5　s6 的有限状态机模型

当新的邻居节点到来时(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$g\text{-}G_i$节点并入*i*组(状态 3、状态 7、状态 8 和迁移状态)。如有$G_j<g$(状态 6)，将第*j*组节点并入*j*-1 组。

4.3　性能分析与模型验证

根据图 4 和图 5，将有限状态机模型使用 PRISM 进行建模和验证，结果如下：

性质 4 匿名性

各接收概率向量中的各分量值相等，攻击者只能随机判断目标节点 A 的通信对象。在 s5 中，$p=1/(N\text{-}1)$；在 s6 中，$1/g\le p\le 1/(2g\text{-}1)$，均不到 1。表 3 显示了根据 3.1 节的设置所得到的验证结果。

表 3　探测率(*p*)

节点密度 *N*	s5(1)	s6(3,1)
4	0.333	0.333
5	0.250	0.250
6	0.200	0.200
7	0.167	0.333
8	0.143	0.286
9	0.125	0.250

性质 5 平均时延

s5 和 s6 都采用定时填充假消息发送机制，平均时延不会超过给定时间参数 t_o。

性质 6 额外开销

额外开销由在给定时间内收到的消息数量 *n*、节点密度 *N* 以及最小组成员数 *g* 决定。表 4 为根据 3.1 节的设置所得到的验证结果：s5 的开销与节点密度成正比；随节点密度增大，s6 的开销明显低于 s5。

表 4　额外开销(*oh*)

节点密度 *N*	s5(1)	s6(3,1)
4	0.333	0.333
5	0.375	0.375
6	0.400	0.400
7	0.417	0.222
8	0.429	0.236
9	0.428	0.245

5　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、数量等信息而进行的通信分析成为主要的匿名攻击方式之一，MIX 输出策略可通过改变消息发送的顺序等方式来抵御此类通信分析。本

文对 MIX 输出策略在 MANET 中的应用进行研究，采用概率模型检测技术验证了 MIX 输出策略的匿名性、平均时延、开销等性质。结果表明，MANET 匿名通信需要 MIX 输出策略提供匿名保护，而现有的策略无法抵御基于统计方法的被动攻击，且会受节点移动的影响。基于分析结果，本文提出了两种同步发送策略并进行了分析和模型检验，结果表明，这两种策略能更好地防御被动攻击，提供低延迟、受节点移动影响小的匿名服务。

参考文献

[1] Kong J. ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad Hoc Networks[C]//Proc. of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Annapolis, USA: ACM Press, 2003: 291-302.

[2] Zhu Bo. Anonymous Seure Routing in Mobile Ad Hoc Networks[C]//Proc. of the 29th Annual IEEE International Conference on Local Computer Networks. Tampa, USA: [s. n.], 2004: 102-108.

[3] Serjantov A. From a Trickle to a Flood: Active Attacks on Several Mix Ttypes[C]//Proc. of the 5th Information Hiding Workshop. Noordwijkerhout, Netherlands: [s. n.], 2002: 36-52.

[4] Danezis G. Statistical Disclosure Attacks: Traffic Confirmation in Open Environments[C]//Proc. of the 18th International Conference on Information Security. Athens, Greece: [s. n.], 2003: 421-426.

[5] 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.

(上接第 153 页)

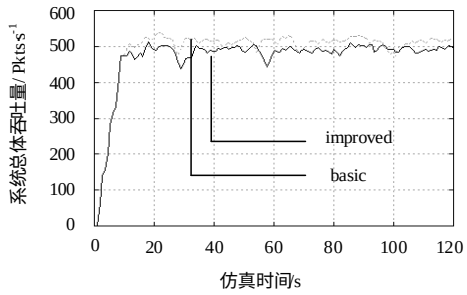

图 4　basic 与 improved 802.11 系统吞吐量的比较

5　结束语

本文基于公平性考虑，并在已有的带宽管理机制上引入了一种加权最大最小带宽分配方案，目的是保证用户的最低需求。通过仿真实验表明，此算法不仅可以实现带宽分配的公平性，而且可以更有效地利用网络资源，从而提高网络的吞吐量和服务质量。

参考文献

[1] Tassiulas L. Adaptive Back——Pressure Congestion Control Based on Local Information[J]. IEEE Trans. on Automatic Control, 1995, 40(2): 236-250.

[2] Tassiulas L, Sarkar S. Maxmin Fair Scheduling in Wireless Networks[C]//Proc. of IEEE INFOCOM'02. [S. l.]: IEEE Press, 2002: 763-772.

[3] Shah S H, Chen Kai, Nahrstedt K. Dynamic Bandwidth Management for Single-hop Ad Hoc Wireless Networks[J]. Mobile Networks and Applications, 2005, 10(1): 199-217.

[4] Chen Kai, Nahrstedt K. Exact: An Explicit Rate Based Flow Control Framework in MANET[R]. Dept. of Computer Science, University of Illinois at Urbana Champaign, USA, Tech. Report: UIUCDCS-R-2002-2286/UILU-ENG-2002-1730, 2002.

[5] Ahn G, Campbell A, Veres A, et al. Swan: Service Differentiation in Stateless Wireless Ad Hoc Networks[C]//Proc. of IEEE INFOCOM' 02. [S. l.]: IEEE Press, 2002: 457-466.

(上接第 156 页)

图 5 为事务请求的平均等待时间，由图可见，事务请求的平均等待时间受队列长度的影响较大，因为队列的长度越大，等待处理的事务请求就越多，每个事务请求的平均等待时间也会增大。

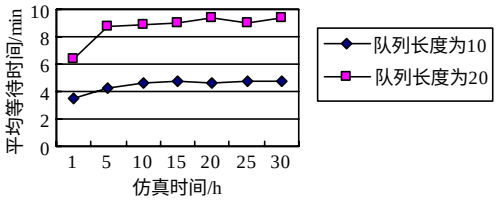

图 5　事务请求的平均等待时间

4　结束语

本文提出一种基于混合式结构的 P2P 网络的事务管理模型，根据超级节点和普通节点处理能力的差异，合理地让超级节点担负事务调度的任务，管理所在自治域内的事务。从整个网络拓扑上看，让每个超级节点管理一部分事务，从而实现整个网络的事务管理。而且通过超级节点来管理事务的调度和回滚，相当于在一个小的范围内实现了事务的统一管理，可以提高事务管理的效率。最后对事务模型的性能做了数学论证和仿真。事务模型的仿真和性能评价仍然是进一步研究的目标。

参考文献

[1] Haller K, Schuldt H, Turker C. A Fully Decentralized Approach to Coordinating Transaction Processes in Peer-to-peer Environments[R]. Department of Computer Science, ETH Zuich, Tech. Rep.: 463, 2004.

[2] Oszu M T, Valduriez P. Principles of Distributed Database System[M]. 2 ed. [S. l.]: Prentice Hall, 1999.

[3] 肖卫军. 多数据库系统的事务管理研究[D]. 武汉: 华中科技大学, 2002.

[4] Gray J, Reuter A. Transaction Processing: Concepts and Techniques[M]. Beijing: China Machine Press, 2004.

[5] 夏启志, 谢高岗, 闵应骅, 等. IS-P2P: 一种基于索引的结构化 P2P 网络模型[J]. 计算机学报, 2006, 29(4): 603-610.