一种基于半马尔可夫过程的匿名节点状态转移模型

郝建国,刘卫东,戴一奇
(清华大学计算机科学与技术系,北京 100084)

摘 要: 为揭示MANET(Mobile Ad-hoc NETworks)匿名路由协议中节点不端行为及其抵御机制对节点协作性的影响,本文根据匿名节点状态转移的特点,提出了一种基于半马尔可夫过程的匿名节点状态转移模型.在该模型下,针对MANET匿名路由协议中节点能量消耗大和隐私保护要求高的特点,对节点状态极限概率进行了理论估计,给出了节点状态转移概率矩阵和转移期望时间矩阵的理论模型.最后,用实验分析了不同模型参数对节点状态极限概率的影响,验证了本文模型的有效性.

关键词: 移动自组织网; 匿名路由协议; 不端行为; 建模; 半马尔可夫过程
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2011) 05-1082-05

An Anonymous Node State Transition Model Based on Semi-Markov Process

HAO Jian-guo, LIU Wei-dong, DAI Yi-qi
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: To reveal the effect of node misbehaviors and defense mechanisms against them on the node cooperation in anonymous routing protocol for MANET (Mobile Ad-hoc NETworks), an anonymous node state transition model based on semi-Markov process is proposed on the features of anonymous node state transition. Under this model, according to the characteristics of large energy consumption and high demand for privacy protection of anonymous node, we give a theoretical estimation of the limiting probability of node states, and present a model of the node state transition probability matrix and transition time expectation matrix. An experimental analysis to the effect of different model parameters on the limiting probability of node states verifies the model's validity at last.

Key words: mobile ad-hoc networks (MANET); anonymous routing protocol; misbehavior; modeling; semi-Markov process

1 引言

MANET匿名路由协议[1]是能有效保护节点身份、位置、移动模式等隐私信息的移动自组织网安全路由协议,在战场无线通信网、车载自组织网等领域有广阔的应用前景.内部节点的不端行为对MANET匿名路由协议的性能和安全性有很大影响,这种影响在车载自组织网等应用中尤为明显[2].在内部节点可能为不端节点的自组织网络环境中,提高匿名路由协议性能和隐私保护性的根本途径,是通过一定的不端节点抵御机制,使节点处于正常执行路由协议的协作状态,同时降低节点处于不端状态的概率.因此,对MANET匿名路由协议中的节点状态变化进行合理建模,有助于分析节点不端行为及其抵御机制对节点协作性的影响,是评价不端节点环境下MANET匿名路由协议的重要理论手段.Xing等人为进行移动自组织网的连通性分析,首次将半马尔可夫过程引入自组织网络节点行为建模[3],为动态描述自组织网络节点行为提供了新思路,但该模型无法描述MANET匿名路由协议中的节点状态变化.

本文以匿名移动自组织网中的节点状态作研究对象,在Xing等人工作基础上,通过分析MANET匿名路由协议中节点状态转移的成因及对节点状态的影响,提出了一种基于半马尔可夫过程的匿名节点状态转移模型.论文对该模型的节点状态极限概率进行了理论估计和数值实验,分析了不同模型参数对节点状态极限概率的影响,验证了该模型的有效性.本文模型具有以下特点,是评价不端节点环境下MANET匿名路由协议的有效理论工具:一是基于匿名节点状态转移的特点,动态描述了存在不端节点的匿名移动自组织网中节点状态的转移过程;二是针对匿名路由协议中节点能量消耗大的特点,将能耗作为节点状态转移的主因,基于能量消耗模型的节点状态转移模型符合匿名路由协议的特点;三是针对匿名路由协议面临的隐私攻击威胁,将合谋隐私攻击作为节点状态转移的重要原因,使本文模型符

收稿日期:2010-01-26;修回日期:2010-06-11

合 MANET 匿名路由协议中节点行为的特点.

2　网络模型和隐私攻击模型

2.1　网络模型

假设移动自组织网的全部 N 个节点分布在某区域 F_N 内,任何离开 F_N 的节点都无法与其他节点通信.由于节点移动速度越快,其离开 F_N 的时间就越短,因此节点的移动水平能用其在 F_N 内的平均驻留时间 $\bar{T}_{in}$ 表示.假设节点能量受限,每个节点具有相同的初始能量 E.节点能与其信号传输范围内的任意邻居节点通信,且节点向邻居节点发送(或从邻居节点接收)单位数量数据包的能耗是一定的.

2.2　隐私攻击模型

路由匿名性是 MANET 匿名路由协议最重要的隐私保护属性之一,它是指数据流的不可追踪性,即攻击者无法发现数据流路由上的任何转发节点[1,4].合谋攻击是路由匿名性面临的主要隐私攻击威胁:在 MANET 匿名路由协议中,若多个节点被攻击者捕获,攻击者就能通过被俘节点间的合谋来比对数据内容,得出在一定时间内转发相同数据的被俘节点及其邻居节点在同一路径的判断,从而使路由匿名性无法达成[5].由上述合谋隐私攻击,易知以下引理:

引理 1　在数据内容对转发节点公开的 MANET 匿名路由协议中,为达成破坏路由匿名性的合谋隐私攻击,攻击者至少需要捕获某路径上的两个节点;攻击者捕获该路径上的节点越多,则路由匿名性越差.

根据引理 1,提出如下 MANET 匿名路由协议隐私攻击模型.假设全局攻击者通过分布式合谋隐私攻击破坏协议的路由匿名性.攻击者首先利用分布在 F_N 中的多个攻击设备 AP 对节点实施捕获,并将被俘节点转发的消息发送给中心攻击者 AC,由 AC 对这些消息进行对比,并实现对可能路径的判断.假设 AP 与 AC 间采用专用的秘密链接,建立链接和发送数据均能在很短的时间内完成;AC 具有较强计算能力,能在很短时间内实现消息内容对比和路径判断.攻击者采取逐次攻击,每次攻击都在上次攻击完成后的某个随机时刻,随机选取 F_N 中的部分节点进行攻击,捕获这些节点并实现消息内容对比和路径判断平均所需时间为 $\bar{T}_a$,其中存在某路径上不小于 2 个节点的概率为 q_r.

3　匿名节点状态转移模型

本节在节点状态定义和状态转移成因分析基础上,提出了基于半马尔可夫过程的节点状态转移模型,并对该模型的节点状态极限概率进行了理论估计.

3.1　节点状态定义

按照 MANET 匿名路由协议中节点的行为特征,将节点分为协作节点和不端节点两类,其中协作节点指按路由协议规则正常参加路由发现和数据转发、同时不对协议实施任何攻击的节点,其节点状态记为 C;不端节点指不能正常执行部分或全部路由协议,或利用协议漏洞实施隐私攻击的节点,分为三类:自私节点,指为转发自身数据而参与路由、但出于节约能量目的而不为其他节点转发数据的节点,其节点状态记为 S;失效节点,指由于能量水平低或不在 F_N 内,而不执行任何路由协议的节点,其节点状态记为 F;恶意节点,指被攻击者捕获、且能与其他恶意节点合谋实施隐私攻击模型所示攻击的节点,其节点状态记为 M.

3.2　节点状态转移成因

MANET 匿名路由协议中,节点状态可能在节点能量的消耗与补充、攻击者的攻击行为、节点激励机制及节点移动性等多种因素作用下,在 C、S、F、M 间发生转移.

为实现节点匿名性和数据机密性,MANET 匿名路由协议在路由发现和数据转发中采用了能量消耗较大的密码运算,同时节点能量是受限的,从而使节约自身能量成为节点状态转移的主因.设每个节点都在本地维护两个能量阈值 ξ_S、$\xi_F(0<\xi_F<\xi_S<1)$,在没有其他状态转移因素作用的情况下,节点根据 ξ_S、ξ_F 决定其状态转移,其状态随能量的变化用表 1 所示的节点能量消耗模型描述.

表 1　节点能量消耗模型

```
energy_initial = E
state_initial = C
if (energy≤ξ_S E)
   state = S
else if (energy≤ξ_F E){
      state = F
      if (recharge == true) {
         recharge_time = T̄_R
         energy = E
         state = C}
}
return
```

攻击者的攻击行为是使节点转移到 M 状态的原因.根据隐私攻击模型,只有转发数据的节点才可能成为恶意节点,因此只有当节点处于 C 状态时,才可能转移到 M 状态.出于攻击者最大化其攻击效果的考虑,节点转移到 M 状态后,只会在能量消耗到不大于 $\xi_F E$ 后转移到 F 状态.

为描述节点激励机制[6]对状态转移的影响,假设存在如下基于信用的激励机制:每个节点在初始状态都拥有 C_{init} 数量的虚拟货币,节点每为其他节点转发 n 个消息就获得 n 个虚拟货币,每发送 n 个自身消息就花费 n 个虚拟货币;当节点拥有的虚拟货币数量为 0

时,节点转移到 C 状态.假设节点单位时间内平均消耗的虚拟货币数量为 ΔC.

根据网络模型,移动性对节点状态转移的影响主要体现在节点因离开 F_N 而转移到 F 状态.

3.3 节点状态转移模型

可见,匿名节点的状态转移有以下特点:一是节点的未来状态仅与其当前状态有关;二是节点状态转移的成因复杂,使状态变化的时间间隔可看成是随机变量.这些特点符合半马尔可夫过程的基本性质,因此,能用半马尔可夫过程对 MANET 匿名路由协议中的节点状态转移进行建模.

定义 1 若匿名节点在时刻 t 的状态为 $Z(t)$,则定义

$$Z(t)=X_n,\quad \forall\ t_n\leqslant t<t_{n+1}$$

为一个状态空间是 $\boldsymbol{S}\equiv\{C,S,F,M\}$ 的半马尔可夫过程,其中 $\{X_n,n=0,1,2,\cdots\}$ 表示节点在转移时间 t_n 的状态,称为半马尔可夫过程 $\{Z(t)\}$ 的嵌入式马尔能夫链.

在不同输入下,定义 1 的半马尔可夫过程可描述匿名路由协议中节点状态的各种随机特征.若定义节点从状态 i 到 j 的转移概率为 $p_{ij}=Pr(X_{n+1}=j\mid X_n=i)$、转移时间分布为 $F_{ij}(t)=Pr(T_n\leqslant t\mid X_{n+1}=j,X_n=i)$,其中 $T_n=t_{n+1}-t_n$ 为第 n 次和第 $n+1$ 次状态转移之间的停留时间,则根据半马尔可夫过程定义[7],当数据输入为 $\{X_n\}$ 的状态转移概率矩阵 $\boldsymbol{P}=(p_{ij})$ 和状态转移时间分布矩阵 $\boldsymbol{F}=(F_{ij}(t))$ 时,$\{Z(t)\}$ 能描述从任意状态 i 到状态 j 的转移.进一步,若令 T_{ij} 表示节点从状态 i 到 j 的转移时间、T_i 表示节点在状态 i 的停留时间,$\mu_{ij}=E[T_{ij}]$、$\mu_i=E[T_i]$ 分别为 T_{ij}、T_i 的数学期望,则根据[7]的定理 4.8.3,节点在某状态 $j\in S$ 的极限概率 P_j 为

$$P_j\equiv\lim_{t\to\infty}P\{Z(t)=j\mid Z(0)=i\}=\frac{\pi_j\mu_j}{\sum_{i\in S}\pi_i\mu_i}\quad(1)$$

式(1)中,$\vec{\pi}\equiv<\pi_i>(i\in\boldsymbol{S})$ 是 $\{X_n\}$ 的平稳分布,$\vec{\pi}=\vec{\pi}\boldsymbol{P}$,$\sum_{i\in S}\pi_i=1,\pi_i\geqslant 0;\mu_i=\sum_{j\in\boldsymbol{S}}p_{ij}\mu_{ij}$.

3.4 节点状态极限概率的理论估计

根据式(1),为对节点状态极限概率 P_j 进行理论估计,需分别建立 $\boldsymbol{P}=(p_{ij})$ 和 $\mu_{ij}(i,j\in\boldsymbol{S})$ 的理论模型.为此,提出如下定理,其中符号的含义如表 2 所示.

表 2 符号及其含义

符号	含义
P_S	节点的平均发送功率
P_R	节点的平均接受功率
P_{CRYPT}	节点单位时间内解密/加密数据的能耗
α	节点发送数据与处理数据的数量比
δ	自私节点的能量节约系数$(0<\delta<1)$
E_{cosume}	协作或恶意节点单位时间内的能耗

定理 1 在 3.2 节的节点状态转移成因下,节点状态转移模型的状态转移概率矩阵为

$$\boldsymbol{P}=\begin{pmatrix}0&p_{CS}&p_{CF}&p_{CM}\\p_{SC}&0&p_{SF}&0\\1&0&0&0\\0&0&1&0\end{pmatrix}$$

证明:根据定义 1,$\{X_n\}$ 中的节点状态转移是不同状态间的转移,故模型的状态转移概率矩阵中,$p_{ii}=0$,$\forall\ i\in\boldsymbol{S}$.由 3.2 节的节点状态转移成因,不同节点状态间的可能转移为:状态 C 能转移到状态 S、M;由于能量不大于 $\xi_S E$ 的节点能在激励机制作用下转移到状态 C,节点也能因能耗从状态 C 直接转移到状态 F;状态 S 能在激励机制作用下转移到状态 C,也能因能耗转移到状态 F;状态 F 只能在重新充电到 E 后转移到状态 C;状态 M 只能因能耗而转移到状态 F.因此,

$$\boldsymbol{P}=\begin{pmatrix}0&p_{CS}&p_{CF}&p_{CM}\\p_{SC}&0&p_{SF}&0\\p_{FC}&0&0&0\\0&0&p_{MF}&0\end{pmatrix}$$

根据 3.3 节状态转移概率矩阵的定义,$\boldsymbol{P}$ 是一个右随机矩阵,其元素满足 $\sum_j p_{ij}=1$,故

$$\boldsymbol{P}=\begin{pmatrix}0&p_{CS}&p_{CF}&p_{CM}\\p_{SC}&0&p_{SF}&0\\1&0&0&0\\0&0&1&0\end{pmatrix}$$

证毕.

定理 2 令 $E_{cosume}=\alpha P_S+(1-\alpha)P_R+P_{CRYPT}$,则 $\mu_{ij}(i,j\in\boldsymbol{S})$ 用如下状态转移期望时间矩阵 $\boldsymbol{M}$ 表示:

$$\boldsymbol{M}=\begin{pmatrix}0&\dfrac{(1-\xi_S)E}{E_{cosume}}&\min\left(\dfrac{(1-\xi_F)E}{E_{cosume}},\bar{T}_{in}\right)&\begin{cases}\dfrac{\bar{T}_a}{q_r},\text{if }\dfrac{\bar{T}_a}{q_r}<\dfrac{(1-\xi_S)E}{E_{cosume}}\\0,\text{else}\end{cases}\\\dfrac{C_{init}}{\Delta C}&0&\min\left(\dfrac{(\xi_S-\xi_F)E}{(1-\delta)E_{cosume}},\bar{T}_{in}\right)&0\\\bar{T}_R&0&0&0\\0&0&\begin{cases}\min\left(\dfrac{(1-\xi_F)E}{E_{cosume}}-\dfrac{\bar{T}_a}{q_r},\bar{T}_{in}\right),\text{if }\dfrac{\bar{T}_a}{q_r}<\dfrac{(1-\xi_F)E}{E_{cosume}}\\0,\quad\text{else}\end{cases}&0\end{pmatrix}$$

证明:根据定理 1,易知

$$\boldsymbol{M}=\begin{pmatrix}0 & \mu_{CS} & \mu_{CF} & \mu_{CM}\\ \mu_{SC} & 0 & \mu_{SF} & 0\\ \mu_{FC} & 0 & 0 & 0\\ 0 & 0 & \mu_{MF} & 0\end{pmatrix}$$

由表 1 的节点能量消耗模型,易知 $\mu_{CS}=\frac{(1-\xi_S)E}{E_{cosume}}$,$\mu_{FC}=\overline{T}_R$. $\mu_{SC}=\frac{C_{init}}{\Delta C}$即虚拟货币消耗为 0 所需时间.根据攻击模型,$\mu_{CM}=\frac{\overline{T}_a}{q_r}$,但当$\frac{\overline{T}_a}{q_r}\geqslant\frac{(1-\xi_S)E}{E_{cosume}}$时,即$\frac{\overline{T}_a}{q_r}$大于节点因能耗而转移到 S 状态的时间时,节点不能转移到 M 状态,故此时 $\mu_{CM}=0$. μ_{iF}, $i\in\{C,S,M\}$是各状态的节点能量消耗到不大于 $\xi_F E$ 所需时间与驻留时间 $\overline{T}_{in}$二者的较小值,故有 $\mu_{CF}=\min(\frac{(1-\xi_F)E}{E_{cosume}},\overline{T}_{in})$,$\mu_{SF}=\min(\frac{(\xi_S-\xi_F)E}{(1-\delta)E_{cosume}},\overline{T}_{in})$. μ_{MF}是节点能量从 E 消耗到 $\xi_F E$ 所需时间与$\frac{\overline{T}_a}{q_r}$的差,故 $\mu_{MF}=\min(\frac{(1-\xi_F)E}{E_{cosume}}-\frac{\overline{T}_a}{q_r},\overline{T}_{in})$;但当$\frac{\overline{T}_a}{q_r}\geqslant\frac{(1-\xi_F)E}{E_{cosume}}$时,即$\frac{\overline{T}_a}{q_r}$大于节点因能耗而转移到 F 状态的时间时,节点不能转移到 M 状态,故此时 $\mu_{MF}=0$.证毕.

4　实验及分析

本节通过实验分析了不同参数对节点状态极限概率的影响,实验参数如表 3 所示.根据攻击模型,$\overline{T}_a$ 包括 AP 的节点捕获时间以及 AP 与 AC 通信时间、AC 的消息内容对比和路径判断时间.由于后两者相对于节点捕获时间可忽略,故 $\overline{T}_a$ 约为节点捕获时间,该时间的缺省值设为 45s[8].典型 MANET 匿名路由协议 AN-ODR[1]的数据转发采用 128 位的 AES 块加密算法,加/解密能量消耗分别为 1.62/2.49 μJ/byte[9],设链路带宽为 2Mpbs,则 $P_{CRYPT}\approx 0.515W$. P_S 及 P_R是在 $2Mpbs$ 的带宽下从文献[10]的能耗模型求得的.

表 3　实验参数

参数	E	$\overline{T}_{in}$	ξ_S	ξ_F	$\frac{C_{init}}{\Delta C}$	q_r	$\overline{T}_a$
缺省值	100W.s	150s	0.2	0.06	30s	0.7	45s
参 数	$\overline{T}_R$	P_S	P_R	P_{CRYPT}	α	δ	
缺省值	60s	0.705 W	0.385 W	0.515W	0.5	0.5	

在定理 1 基础上,结合上述参数,实验中

$$\boldsymbol{P}=\begin{pmatrix}0 & 0.650.61 & 0.30 & 0.050.09\\ 0.80 & 0 & 0.20 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\end{pmatrix}$$

节点初始能量及移动性对 P_C、P_M 的影响如图 1 所示.从图 1 可见,P_C、P_M 都随 E 值的增大而增大.当 $E\geqslant$50W·s 时,E 值增加对 P_C 的影响越来越小,P_C 趋于一个固定概率.这是因为,E 越高,节点因能耗从 C 状态转移到 S 或 F 状态所需时间就越长,同时节点被攻击者捕获而转移到 M 状态的概率也越高.当 $E\leqslant$70W·s 时,由于 $\overline{T}_a/q_r$ 大于节点因能耗而转移到 S 或 F 状态的时间,$P_M=0$.此外,由于低速节点能量消耗速度慢,同时易被攻击,因此 $\overline{T}_{in}$越大,则节点处于 C 或 M 状态的概率就越高.

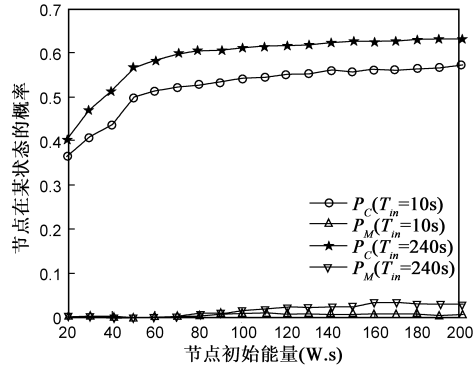

图1　节点初始能量及移动性的影响

ξ_S 和 $C_{init}/\Delta C$ 是决定自私节点状态的参数.如图 2 所示,ξ_S 的增大使节点因能耗从 C 转移到 S 状态的时间缩短,因此随着 ξ_S 的增大,P_C 减小、P_S 增大.在 $\xi_S=0.2$ 时,当 $C_{init}/\Delta C$ 从 10s 增加到 50s 后,由于节点从 S 状态转移到 C 状态的时间增加,P_C 减小 14.54%、P_S 增大 191.34%,说明节点激励机制的强度对 P_C 特别是 P_S 有显著影响.

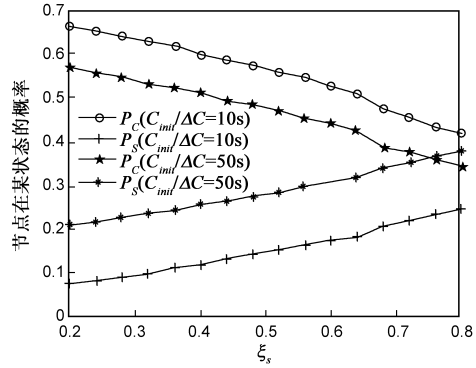

图2　自私节点参数的影响

隐私攻击参数 $\overline{T}_a$、q_r 对 P_M 的影响如图 3 所示.实验表明,若 $q_r=0.7$,则当 $\overline{T}_a<$65s 时,P_M 与 $\overline{T}_a$ 成反比;当 $\overline{T}_a\geqslant$65s 时,由于 $\overline{T}_a/q_r$ 大于节点因能耗转移到 S 或 F 状态的时间,$P_M=0$.此外,提高 q_r 会显著增大 P_M:若 $\overline{T}_a$ = 45s,当 q_r 从 0.7 增大到 0.9 后,P_M 会增大 102.86%.因此,若攻击者受节点捕捉技术限制而无法缩短 $\overline{T}_a$,可通过增加 AP 数量获得的较高 q_r 来提高 P_M,

以达成对路由匿名性的破坏.

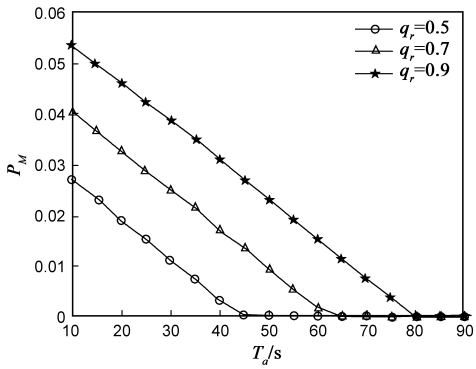

图3 隐私攻击参数的影响

5 结论

本文基于 MANET 匿名路由协议节点状态转移的特点,提出了一种基于半马尔可夫过程的匿名节点状态转移模型,对该模型的节点状态极限概率进行了理论估计和实验分析.本文模型充分体现了节点能量变化和隐私攻击对节点状态的影响,符合不端节点环境下 MANET 匿名路由协议的一般特点,是评价抵御不端节点的 MANET 匿名路由协议机制的有效理论工具.论文研究表明,在存在不端节点的移动自组织网络环境下设计匿名路由协议时,不仅要综合考虑节点能量变化、攻击行为、激励机制等多种因素的影响,以保证节点有效协作;而且应针对不同网络环境,把握影响节点协作的主要状态转移因素,有重点地设计协议机制,以免因协议过于复杂而影响整体性能.作为本文的后续工作,未来应结合具体网络环境,对节点状态的其他随机特征进行深入的理论分析和实验.

参考文献

[1] J Kong, X Hong, et al. An Identity-free and On-demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks [J]. IEEE Transactions on Mobile Computing, 2007, 6(8): 888 – 902.

[2] E Schoch, F Kargl, et al. Impact of Pseudonym Changes on Geographic Routing in VANETs [A]. In Proceedings of the European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2006) [C]. Hamburg: Springer-Verlag, 2006. 43 – 57.

[3] F Xing, W Wang. Modeling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes [A]. In Proceedings of IEEE ICC 2006 [C]. New York: IEEE Press 2006, 1879 – 1884.

[4] 章洋,范植华,等.移动自组网络中多径路由的匿名安全[J].电子学报,2005,33(11):2022 – 2030.
Y Zhang, Z H Fan, et al. Anonymous Secure Multipath Routing in Mobile Ad-Hoc Networks [J]. Acta Electronica Sinica, 2005, 33(11): 2022 – 2030. (in Chinese)

[5] Y Qin, D Huang, et al. OLAR: On-demand Lightweight Anonymous Routing in MANETs [A]. In Proceedings of the 4th International Conference on Mobile Computing and Ubiquitous Networking [C]. Tokyo: IPSJ, 2008. 72 – 79.

[6] 易平,蒋嶷川,等.移动 ad hoc 网络安全综述[J].电子学报,2005,33(5):893 – 899.
P Yi, Y C Jiang, et al. A Survey of Security for Mobile Ad Hoc Networks[J]. Acta Electronica Sinica, 2005, 33(5): 893 – 899. (in Chinese)

[7] S M Ross. Stochastic Processes [M]. New York: John Wiley and Sons, 1983.

[8] C Hartung, J Balasalle, et al. Node Compromise in Sensor Networks: the Need for Secure Systems, TR CU-CS-990-05 [R]. Boulder: University of Colorado at Boulder, 2005.

[9] A Wander, N Gura, et al. Energy Analysis of Public-key Cryptography for Wireless Sensor Networks [A]. In Proceedings of third IEEE International Conference on Pervasive Computing and Communications [C]. New York: IEEE Press, 2005. 324 – 328.

[10] L Feeney, M Nilsson. Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment [A]. In Proceedings of the 20th IEEE Conference on Computer Communications (INFOCOM 2001) [C]. New York: IEEE Press, 2001. 1548 – 1557.

作者简介

郝建国 男,1976 年生于河北宣化.清华大学计算机科学与技术系博士生,主要研究方向为无线网络安全和隐私保护、移动电子支付.
E-mail: hjg06 @ mails. tsinghua. edu. cn; tigerzhh @ gmail. com

刘卫东 男,1968 年生于江西,清华大学计算机科学与技术系副教授,主要研究方向为计算机网络.
E-mail: liuwd@mail.tsinghua.edu.cn

戴一奇 男,1946 年生于浙江,清华大学计算机科学与技术系教授,博士生导师,主要研究方向为网络信息安全.
E-mail: dyq@tsinghua.edu.cn