# 泛洪攻击对 Epidemic 机制下机会网络生命期的影响

孙践知，张迎新，陈丹，韩忠明
（北京工商大学 计算机与信息工程学院，北京 100048）

**摘 要**：机会网络应用中存在能量无法补充的场景，泛洪是机会网络中容易发生的攻击行为。从理论上分析了在 Epidemic 路由机制下，泛洪攻击导致的节点能量消耗以及对网络生命期的影响。分析表明恶意节点数量的增加会对网络生命期产生显著影响，而恶意节点注入的数据分组的数量仅能在特定的场景下产生影响，且影响轻微。使用 ONE 仿真平台对泛洪攻击进行了仿真实验，仿真结果与理论分析的结论一致。

**关键词**：机会网络；节点能量；生命期；恶意节点；泛洪攻击；Epidemic
**中图分类号**：TP301.6 **文献标识码**：B **文章编号**：1000-436X(2012)09-0185-06

# Effects on lifetime of opportunistic network based on Epidemic routing under flooding attacks

SUN Jian-zhi, ZHANG Ying-xin, CHEN Dan, HAN Zhong-ming
(College of Computer and Information Engineering, Beijing Technology and Business University, Beijing 100048, China)

**Abstract:** In some scenarios of opportunistic network, energy could not be replenished. It was prone to flooding attacks in opportunistic network. The energy consumption of nodes and the effect on the network lifetime caused by flooding attacks under the mechanism of the Epidemic routing was analyzed. The analysis showed that the increase of malicious nodes had significant effects on network lifetime, and the number of packets from malicious nodes can only had effects in particular scenarios, and had minimal effects. ONE to simulate flooding attacks was used, the simulation results are same as the theoretical analysis.

**Key words:** opportunistic network; node energy; lifetime; malicious node; flooding attacks; Epidemic

## 1 引言

机会网络是一种不需要在源节点和目的节点之间存在完整路径，利用节点移动带来相遇机会实现网络通信的、时延和分裂可容忍的自组织网络[1]。和传统多跳无线网络不同，机会网络的节点可能不是被统一部署的，节点间不存在确定的路径，节点通过移动而得相遇机会进行通信，网络中存在更多的不确定因素，对路由安全以及数据的完整性、机密性带来更大的挑战[2]。

在机会网络安全领域，主要关注如何保证网络的可用性以及数据的完整性、机密性。目前关于机会网络安全问题直接的文献还较少，但对 DTN(delay-tolerant networking)及 MANET（mobile ad hoc network）安全的研究已取得一些进展，其相关研究如下。

加密和身份认证是解决安全问题最常用的手

**收稿日期**：2012-03-20；**修回日期**：2012-08-07
**基金项目**：国家自然科学基金资助项目（61170112）；北京市属高等学校科学技术与研究生教育创新工程建设基金资助项目（PXM2012-014213-000079）
**Foundation Items:** The National Natural Science Foundation of China (61170112); Funding Project for Innovation on Science , Technology and Graduate Education in Institutions of Higher Learning Unde the Jurisdication of Beijing Municipality (PXM2012-014213-000079)

段。文献[3]定义了束层安全机制，通过定义 BAB（bundle authentication block）、PIB（payload integrity block）和 PCB（payload confidentiality block）来保证所传输束的真实性、完整性和机密性，核心思想与 IPSec 类似。

理论上讲，束层安全机制可以从根本上解决机会网络多数安全问题。但由于机会网络独有的特性，使密钥管理问题难于解决，以致于在机会网络中无法有效部署束层安全机制，许多学者在该领域做了大量研究。文献[4]分析了 DTN 网络安全领域的问题，指出目前还未得到很好解决的、最主要的问题是密钥管理问题。文献[5]指出在传统 MANET 网络中使用的密钥管理技术，如 PKI(public key infrastructure)[6]、off-line certificates[7]、a priori key distribution[8]、a reputation system[9]等，均难于部署。IBC(identity-based cryptography)[10]被认为是解决密钥管理问题最有希望的方案，也是 DTN 安全研究的一个热点。文献[11]提出用 IBC 解决端到端安全问题，文献[12]讨论了 IBC 在 DTN 网络中的应用，文献[4]指出了 IBC 方案的局限性，文献[13]指出 IBC 不能解决 DTN 网络中的密钥管理问题。

文献[4]认为由于 DTN 网络资源匮乏，DTN 网络安全防护的重点是保证 DTN 网络不被非授权使用。

文献[4, 14, 15]分别描述了 DTN 网络面对的威胁，主要有资源消耗、完整性和机密性问题、DoS 攻击、广播风暴等。文献[5]描述了具体的攻击形态，主要有泛洪、Drop 攻击、破坏路由表、伪造 ACK、发送畸形数据分组、重放、流量分析、授权用户侦听其他用户等。文献[5]使用了 UMass Dieselnet 项目[16]和 Cambridge Haggle 项目[17]数据集，研究了在缺乏安全机制下，DTN 网络中的攻击效果，得出了即便在强有力的攻击下，DTN 网络依然是健壮的结论。

在 Epidemic 机制下，恶意节点会向网络中注入伪造的数据分组，但由于机会网络不存在始终连接的链路，恶意泛洪行为难以持续进行，显然会影响泛洪效果。文献[18]和文献[19]分别研究了泛洪攻击对 Epidemic 机制下网络性能的影响，得出了截然不同的结论，文献[18]认为难以产生影响，而文献[19]认为会产生显著影响，但两者都没有涉及泛洪攻击对机会网络生命期的影响。

本文通过理论分析和仿真实验方法，从节点能量消耗的角度，研究 Epidemic 机制下泛洪攻击对机会网络生命期的影响。

## 2 泛洪攻击和网络生命期

### 2.1 攻击模型

由于密钥管理的问题未得到很好的解决，在机会网络中难于部署有效的身份认证和加密机制[4,7]。因此本文假定在束层未部署身份认证和加密机制，但应用层是否进行身份认证和加密不作限制。

本文假定机会网络中存在正常节点和恶意节点。正常节点是构成机会网络的基础，恶意节点具有正常节点的部分特征，如遵循共同的移动模型、路由协议等，但其具有某种攻击行为，以破坏网络、阻碍正常数据分组传输为目的。

当恶意节点和正常节点相遇时会尽力向正常节点转发伪造的数据分组，即采用无限制泛洪策略。正常节点接收到恶意节点伪造的数据分组时，由于无法判定数据分组性质，在随后的转发中亦会按照既有转发策略尽力向其他节点转发，会进一步放大攻击的效果。

### 2.2 机会网络的生命期

在机会网络应用的某些场景中，存在节点无法补充能量的情况，如灾难场景、野生动物监控场景。节点出于维持通信的需要不断地消耗固有能量，当能量耗尽时，会发生节点死亡事件。节点死亡事件的不断发生最终导致整个网络死亡，即机会网络具有生命期。

机会网络的生命期始于网络部署，止于网络失去功能。何为网络失去功能可以从不同角度定义，如剩余存活节点数量、剩余的传输能力、剩余的网络覆盖情况等，也可以是几种角度的组合。目前尚无法检索到和机会网络生命期直接相关的文献，但无线自组织网络生命期的研究工作已有一些进展，如文献[20]对 WSN（wireless sensor networks）生命期定义做了很好的分类。

在机会网络中节点分布是不均匀的，一些节点处于“枢纽”位置，这些节点和其他节点有较高的相遇概率，会承担较多的转发工作，消耗的节点能量也较多，这些节点会首先死亡；而一些节点处于“末梢”位置，这些节点消耗的能量较少，会有较长的生命期。当网络中一定比例的节点死亡后，尽管网络中还有一些节点存活，但网络的整体传输能力严重下降，难以完成原有网络的工作，此时即认为网络死亡。

本文从存活节点占总节点数百分比的角度定义机会网络生命期，当比值超过阈值时，即认为机会网络死亡。

## 3　泛洪攻击的影响

假设在机会网络中有 $n$ 个正常节点，$k$ 个恶意节点。将机会网络整个生命期分为 $M$ 个时间片，$m$ 为第 $m$ 个时间片；$e_0^m$ 是第 $m$ 个时间片内正常节点的总能量。$E_D$ 为单位时间传输的能量消耗，$E_s$ 为单位扫描的能量消耗，$E_w$ 为无法使用的能量。

在无攻击时，$t_i^m$ 表示第 $i$ 个节点在第 $m$ 个时间片内与其他节点接触的时间长度。节点相遇特征属移动模型研究范畴，是通过期望相遇时间来刻画的。关于期望相遇时间目前有 2 种观点，一种观点认为服从指数分布或其尾部服从指数分布[21]，而另一种观点认为近似地服从幂律分布[22]，是指数分布还是幂率分布还在争论之中。

$R_i^m$ 表示第 $i$ 个节点在第 $m$ 个时间片内向其他节点转发数据分组的概率；$L_m$ 表示第 $m$ 个时间片内机会网络的生命期；在有攻击时，$t_i^m$、$R_i^m$ 和 $L_m$ 分别以 $t_i^{m'}$、$R_i^{m'}$ 和 $L_m^{'}$ 表示。

在无攻击时，第 $m$ 个时间片有

$$e_0^m - E_w = L_m E_s + \sum_{i=1}^{n} E_D t_i^m R_i^m \tag{1}$$

有攻击时，第 $m$ 个时间片内，正常节点有

$$e_0^m - E_w = L_m^{'} E_s + \sum_{i=1}^{n} E_D t_i^{m'} R_i^{m'} \tag{2}$$

假设恶意节点和正常节点有相同的移动模型，则节点 $i$ 遇到正常节点的概率约为 $\frac{n}{n+k}$，遇到恶意节点的概率为 $\frac{k}{n+k}$，由此可得

$$e_0^m - E_w = L_m^{'} E_s + \frac{n}{n+k}\sum_{i=1}^{n} E_D t_i^{m'} R_i^{m'}\left(1+\frac{k}{n}\right) \tag{3}$$

式(3)中，$\frac{n}{n+k}\sum_{i=1}^{n} E_D t_i^{m'} R_i^{m'}$ 是有攻击时正常节点间传输数据分组导致的能量消耗，由于恶意节点加入到网络中并不会改变正常节点的移动轨迹，即不会改变正常节点间相遇的概率，亦即在有攻击时，正常节点间转发数据分组消耗的能量不会发生改变，即有

$$\sum_{i=1}^{n} E_D t_i^m R_i^m = \frac{n}{n+k}\sum_{i=1}^{n} E_D t_i^{m'} R_i^{m'} \tag{4}$$

由式(3)和式(4)可得

$$e_0^m - E_w = L_m^{'} E_s + \left(1+\frac{k}{n}\right)\sum_{i=1}^{n} E_D t_i^m R_i^m \tag{5}$$

由式(1)和式(5)可得

$$L_m E_s = L_m^{'} E_s + \frac{k}{n}\sum_{i=1}^{n} E_D t_i^m R_i^m \tag{6}$$

若以 $DL_m$ 表示在 $m$ 时间片内对网络生命期的影响，则有

$$DL_m = \frac{k}{n}\cdot\frac{E_D}{E_s}\sum_{i=1}^{n} t_i^m R_i^m \tag{7}$$

若以 $DL$ 表示对网络生命期的影响，则有

$$DL = \sum_{m=1}^{M}\left(\frac{k}{n}\cdot\frac{E_D}{E_s}\sum_{i=1}^{n} t_i^m R_i^m\right) = \frac{k}{n}\cdot\frac{E_D}{E_s}\sum_{m=1}^{M}\sum_{i=1}^{n} t_i^m R_i^m \tag{8}$$

由式(8)可知，恶意节点的泛洪攻击对网络生命期影响有 4 个因素，分别是：

1) 正常节点和恶意节点数量之比；

2) 单位扫描能量消耗和单位传输能量消耗之比；

3) 节点间的接触时间 $t_i^m$，$t_i^m$ 取决于节点移动模型；

4) 转发概率 $R_i^m$，影响 $R_i^m$ 的因素较多将在第 4 节中专门讨论。

## 4　恶意数据分组数量的影响

恶意节点注入网络数据分组的数量是否会对网络生命期产生影响也是需要研究的问题，下面分析正常节点和恶意节点的数量确定时，恶意节点产生的数据分组数量对网络生命期的影响。

若 $w_i$ 是第 $i$ 个节点生成数据分组的个数；$W_n$ 和 $W_k$ 分别是正常节点和恶意节点产生数据分组的总数，则 $W_n = \sum_{i=1}^{n} w_i$，$W_k = \sum_{i=1}^{k} w_i$；$g_i$ 是第 $i$ 个节点缓存大小；$d_i$ 是第 $i$ 个数据分组大小，$d = \frac{1}{n}\sum_{i=1}^{n} d_i$；$C_i^{\max}$ 和 $C_j^{\max}$ 分别是 $i$ 和 $j$ 节点最大可存储的数据分组个数，$C_i^{\max} = g_i / d$、$C_j^{\max} = g_j / d$；$t_{ij}$ 是节点 $i$ 和节点 $j$ 相遇持续的时间长度；$v_{ij}$ 是节点 $i$ 和节点 $j$ 间数据传输的速度；$Q_{ij}^{\max}$ 是当 $i$ 节点和 $j$ 节点相遇时可传输数据分组的最大个数，$Q_{ij}^{\max} = t_{ij} \times v_{ij} / d$。

当节点 $i$ 和任意节点 $j$ 相遇时，在 $i$ 节点中存在，而在 $j$ 节点中不存在的数据分组个数小于 $Q_{ij}^{\max}$ 时，会出现节点间有传输能力但无数据分组需要传输的情况，出现这种情况的概率在式(1)中由 $R_i^m$ 表述。若 $X$ 是表述 $i$、$j$ 2 节点缓存中相同数据分组个数的随机变量，则

$$R_i^m = 1 - p(X > \min(C_i^{\max}, C_j^{\max}) - Q_{ij}^{\max}) \tag{9}$$

容易证明在 Epidemic 机制下，$X$ 服从参数为 $(C_i^{\max}, C_j^{\max}, W)$ 的超几何分布，记为

$$X \sim H(C_i^{\max},\ C_j^{\max},\ W) \tag{10}$$

由式(9)和式(10)可知，$R_i^m$ 和机会网络中数据分组总数、数据分组大小、传输速度、移动模型和节点缓存大小 5 个因素有关。由超几何分布的特性可知，在某些特定的情况，当上述 5 个因素间关系恰当时，上述 5 个因素还是会对 $R_i^m$ 的值产生影响的。

若 $Q_{ij}^{\max} = \frac{1}{h}\min(C_i^{\max}, C_j^{\max})$，$\min(C_i^{\max}, C_j^{\max}) = \frac{1}{l}W$，当 $h$ 和 $l$ 大于 5 时，由超几何分布的特性可知，$R_i^m$ 高度接近 1。在此情况下，$W$ 值增加虽然 $R_i^m$ 值会更加接近 1，但值变化的范围会非常小，由此可知除某些特定情况外，恶意节点注入数据分组的数量难以影响 $R_i^m$ 的值，即难以对机会网络生命期产生影响。

## 5 仿真实验设计

本文设计的实验场景中确定了度量值，通过软件仿真的方法来定量分析泛洪攻击对机会网络生命期的影响，并以此验证理论分析结果。

### 5.1 度量值

本文从存活节点数量和单位时间段内传输成功率 2 个方面来评价路泛洪攻击对机会网络生命期的影响。

1) 存活节点数量

由于节点需不断地进行扫描、传输工作，随着节点能量的不断消耗，网络中节点会相继死亡，剩余的存活节点构成了网络的新形态，而存活节点的数量会对新形态下的网络性能产生决定性的影响。本文将一段时间后存活节点数量作为评价泛洪攻击的一个度量值。

2) 单位时间传输成功率

传输成功率是指在一定的时间内到达目标节点数据分组总数和所有数据分组总数之比，该指标刻画了网络的传输能力，是机会网络最重要的指标。为评估节点死亡对网络性能的影响，本文采用每个时间单位上的传输成功率作为度量值。在后面的分析中，仅计算正常节点在各时间单位上传输成功率。

### 5.2 场景设计

文本使用了 ONE（opportunistic networking environment）[23]仿真平台，模拟了携带无线智能设备的行人步行于赫尔辛基的场景，并以此来分析泛洪攻击对机会网络生命期的影响。具体设置如表 1 所示。

表 1 仿真场景设置

| 类别 | 参数 | 值 |
|---|---|---|
| 场景特征 | 仿真时间 | 24h |
| | 仿真区域范围 | 3 400m×4 500m |
| 节点特征 | 移动模型 | SPMBM |
| | 移动速度 | 0.5~1.5m/s |
| | 传输速率 | 250kbyte/s |
| | 最大传输范围 | 10m |
| | 缓存大小 | 50MB |
| 数据分组特征 | 大小 | 500KB~1MB，随机生成 |
| | 生存期 | 5h |

在仿真中正常节点和恶意节点分属不同的群组，群组间节点不互为目标节点，但可以相互转发数据分组。

## 6 结果分析

本文从恶意节点数量和恶意节点注入网络数据分组数量 2 个角度，分析泛洪攻击对机会网络生命期的影响。

### 6.1 恶意节点数量的影响

以表 1 场景为基础，正常节点数为 200 个，恶意节点数为 0~200 个。恶意节点生成 5 倍于正常节点的数据分组数量注入网络中。图 1 为恶意节点数量对网络生命期的影响。

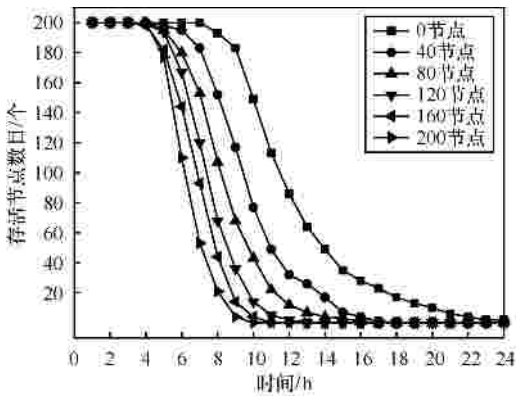


图 1 恶意节点数量对网络生命期的影响

图 1 表明，在不同数量恶意节点攻击下，正常节点死亡发生的趋势是一致的。只是由于恶意节点的加入导致正常节点能耗大大增加，使节点死亡的时间提前。图 1 表明，有力的泛洪攻击会大大增加正常节点能量的消耗，加速正常节点的死亡，从而加快整个网络的死亡。

图 2 描述了不同数量恶意节点的攻击下，各时

间单位段上传输成功的数据分组个数。图 2 表明，恶意节点的攻击不会改变机会网络各单位时间传输成功个数的总体形态，但会令单位时间传输成功个数大幅度地下降，随着节点大批死亡，单位时间传输成功率急剧下降。

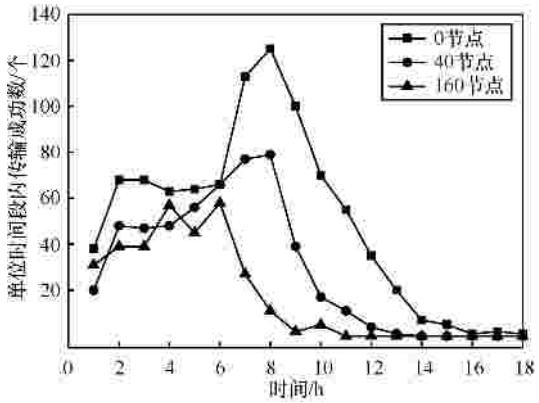


图 2　恶意节点数量对网络传输性能的影响

表 2 描述了恶意节点数量对网络生命期的影响，以剩余的存活节点减少到节点总数的 20%为阈值。表 2 表明，恶意节点的数量增加网络生命期会大幅度下降，两者间有显著的关系，这与式(8)的结果一致。

表 2　恶意节点数量对网络生命期的影响

| 恶意节点数/个 | 网络生命期/h |
|---|---|
| 0 | 17.6 |
| 40 | 13.5 |
| 80 | 11.1 |
| 120 | 9.6 |
| 160 | 8.6 |
| 200 | 8 |

### 6.2　恶意数据分组数量的影响

为分析恶意节点注入网络数据分组的数量对网络生命期的影响，以表 1 场景为基础，设置 200 个正常节点，200 个恶意节点，令恶意节点分别以正常节点数据分组数量 10%、100%和 500%向网络中注入数据分组。由表 1 给出的节点和数据分组的参数可计算超几何分布的 4 个参数，进而计算出 $R_i^m$。

$$C_i^{\max} = C_j^{\max} = 50\text{MB}/750\text{KB} \approx 66(\text{个})$$

$i$ 节点和 $j$ 节点的接触时间和节点移动模型有关，目前还是一个尚无定论的问题，一般认为节点间接触时间符合幂律分布。为简化起见，以表 1 中定义的 2 个在一条直线上相向运动节点的接触时间作为平均接触时间来估计 $Q_{ij}^{\max}$，并以此来计算 $R_i^m$。本文中对 $Q_{ij}^{\max}$ 估计可能会有较大误差，但由于超几何分布的特点，这种误差并不会对计算 $R_i^m$ 产生显著影响。

$$Q_{ij}^{\max} = 10\text{m}/1\text{m/s} \times 250\text{kB}/750\text{kB} \approx 3(\text{个})$$

表 3 给出了 3 种不同攻击场景下各参数值。仿真结果如图 3 所示。

表 3　恶意数据分组数量的影响

| 攻击场景 | $Q_{ij}^{\max}$ | $C_i^{\max}$ | $C_j^{\max}$ | $W_n$ | $W_k$ | $R_i^m$ |
|---|---|---|---|---|---|---|
| 1 | 3 | 66 | 66 | 2 932 | 293 | 1 |
| 2 | 3 | 66 | 66 | 2 932 | 2 932 | 1 |
| 3 | 3 | 66 | 66 | 2 932 | 14 660 | 1 |

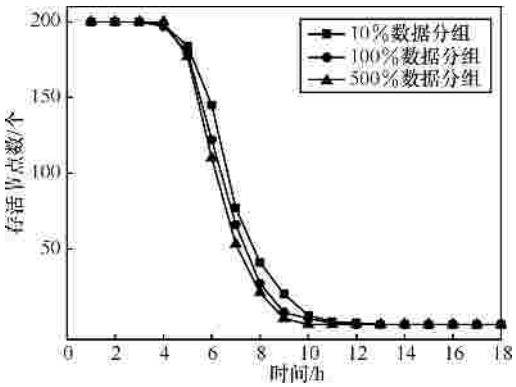


图 3　恶意数据分组数量的影响

第 1 和第 3 种攻击场景注入网络数据分组的数量相差 50 倍，由表 2 可知，其 $R_i^m$ 的值均为 1，由式(8)可知不会对网络生命期产生影响。图 3 显示，3 种场景网络中节点死亡的情况非常接近，影响轻微，此结果与本文第 4 节中的理论分析高度吻合。由式(9)可知，恶意节点注入数据分组数量仅在某些特定的情况下对网络生命期产生影响，在多数情况下影响轻微。

## 7　结束语

本文给出了泛洪攻击时，恶意节点个数等因素对机会网络生命期的影响，理论分析及仿真结果表明，泛洪攻击会对机会网络生命期产生显著影响。

文献[5]从网络性能的角度出发，认为泛洪攻击在 DTN 网络中是难以实现的，而从节点能量消耗的角度分析本文结果不支持该结论。本文结果表明，恶意节点数量和机会网络生命期基本呈线性关

系，即恶意节点数越多，机会网络的生命期会越短，传输成功率同时也会显著下降。

文献[18]从网络性能角度出发，认为在 Epidemic 机制下对网络的恶意攻击难以奏效，但从节点能量消耗角度，本文结果不支持该观点。本文结果表明，Epidemic 机制下的恶意攻击会导致大量的节点能量消耗，导致节点死亡，使网络生命期显著下降，部分节点的死亡也会导致网络性能的显著下降。

本文给出了节点缓存大小、传输速度、数据分组个数等 5 个因素和机会网络生命期的关系，理论分析和仿真实验表明，一般情况下，网络生命期与恶意节点注入机会网络恶意数据分组的数量相关度较小。

## 参考文献：


[1] 任智，黄勇，陈前斌. 机会网络路由协议[J]. 计算机应用. 2010, (3): 723-728.
REN Z, HUANG Y, CHEN Q B. Routing protocols for opportunistic networks[J].Journal of Computer Applications, 2010, (3): 723-728.

[2] 熊永平，孙利民，牛建伟. 机会网络[J]. 软件学报, 2009, 20(1): 124-137.
XIONG Y P, SUN L M, NIU J W. Opportunistic networks[J]. Journal of Software, 2009, 20(1): 124-137.

[3] SYMINGTON S, FARRELL S, WEISS H, *et al*. Bundle Security Protocol Specification[R]. IETF Internet Draft, Work Progress, 2007.

[4] FARRELL S, SYMINGTON S, WEISS H, *et al*. Delay-Tolerant Networking Security Overview[R]. IRTF, DTN Research Group, 2008.

[5] BURGESS J, BISSIAS G D, CORNER M D, *et al*. Surviving attacks on disruption-tolerant networks without authentication[A]. Proceeding of the 8th ACM Internation Symposium on Mobile Ad Hoc Networking and Computing[C]. Montreal, Quebec, Canada, 2007. 61-70.

[6] PAPADIMITRATOS P, HAAS Z J. Secure routing for mobile ad hoc networks[A]. Proceeding of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference[C]. San Antonio, TX, 2002. 193-204.

[7] SANZGIRI K, LAFLAMME D, DAHILL B, *et al*. Authenticated routing for ad hoc networks[J]. Selected Areas in Communications, IEEE Journal, 2005, 23(3): 598-610.

[8] HU Y C, PERRIG A, JOHNSON D B. Ariadne: A secure on-demand routing protocol for ad hoc networks[J]. Wireless Networks, 2005, 11(1-2): 21-38.

[9] BUCHEGGER S, LE B J. The effect of rumor spreading in reputation systems for mobile ad-hoc networks[J]. Proceedings of WiOpt '03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks[C]. Sophia-Antipolis, France, 2003.

[10] BONEH D, FRANKLIN M. Identity-Based Encryption From the Weil Pairing[A]. Cryptology CRYPTO[C]. Springer, 2001. 213-229.

[11] SETH A, KESHAV S. Practical security for disconnected nodes[A]. First IEEE ICNP Workshop on Secure Network Protocols (NPSec)[C]. 2005. 31-36.

[12] ASOKAN N, KOSTIAINEN K, GINZBOORG P, *et al*. Applicability of identity-based cryptography for disruption-tolerant networking[A]. Proceedings of the 1st International MobiSysWorkshop o Mobile Opportunistic Networking[C]. 2007. 52-56.

[13] MCMAHON A, FARRELL S. Delay-and disruption-tolerant networking[J]. Internet Computing, IEEE, 2009, 13(6): 82-87.

[14] KATE A, ZAVERUCHA G M, HENGARTNER U. Anonymity and security in delay tolerant networks[A]. Proceedings of the 3rd International Conference on Security and Privacy in Co munication Networks[C]. 2007. 504-513.

[15] ASOKAN N, KOSTIANINEN K, GINZBOORG P, *et al*. Towards Securing Disruption-Tolerant Networking[R]. Nokia Research Center, Tech Rep NRC-TR-2007-007, 2007.

[16] BURGESS J, GALLAGHER B, JENSEN D, *et al*. Maxprop: Routing for vehicle-based disruption-tolerant networks[A]. The 25th IEEE International Conference on Computer Communications[C]. Barcelona, Spain, 2006. 1-11.

[17] HUI P, CHAINTREAU A, SCOTT J, *et al*. Pocket switched networks and human mobility in conference environments[A]. Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-Tolerant Networking[C]. 2005. 244-251.

[18] FAWAL A, BOUDEC J Y, SALAMATIAN K. Vulnerabilities in epidemic forwarding[A]. World of Wireless, Mobile and Multimedia Networks[C]. 2007. 1-6.

[19] 孙践知，贠冰，韩忠明. 泛洪攻击下机会网络典型路由算法健壮性分析[J]. 计算机工程与应用, 2012, 48(5):54-58.
SUN J Z, YUN B, HAN Z M. Robustness analysis of opportunistic network routing algorithms under flooding attacks[J]. Computer Engineering and Applications, 2012, 48(5): 54-58.

[20] CHEN Y, ZHAO Q. On the lifetime of wireless sensor networks[J]. IEEE Communications Letters, 2005, 9(11): 976-978.

[21] CHAINTREAU A, HUI P, CROWCROFT J, *et al*. Impact of human mobility on opportunistic forwarding algorithms[J]. IEEE Transactions on Mobile Computing, 2007, 6(6): 606-620.

[22] KARAGIANNIS T, LEBOUDEC J Y, VOJNOVIC M. Power law and exponential decay of intercontact times between mobile devices[J]. IEEE Transactions on Mobile Computing, 2010, 9(10): 1377-1390.

[23] KERÄNEN A, OTT J, KÄRKKÄINEN T. The one simulator for DTN protocol evaluation[A]. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)[C]. 2009. 55.


## 作者简介：


孙践知（1967-），男，内蒙古呼和浩特人，硕士，北京工商大学副教授，主要研究方向为网络及信息安全。

张迎新（1967-），女，山西太原人，硕士，北京工商大学副教授，主要研究方向为信息安全。

陈丹（1968-），女，黑龙江哈尔滨人，硕士，北京工商大学副教授，主要研究方向为网络及信息安全。

韩忠明（1972-），男，山西太原人，博士，北京工商大学副教授，主要研究方向为数据分析与挖掘、复杂网络等。