



POST CARD  
CANTON  
PHOTOGRAPHIC  
ANTONIO TORONI  
N. 36  
ORINO

17.3.1926  
Cartolina postale

FOTOGRAFIA  
Umberto Bonivento  
PIOLA  
Via Promontore 4

Stimata signora  
Contessa Abenti  
voglio augurarvi

Alle mie amiche  
Maurina, Paola  
se ricordo qualche  
volta di me, che  
sola affetto  
lavoro. Plita

X'CON 2003

移动无线自组网中路由算法的安全性研究

作者：金鑫

日期：2003/10/20



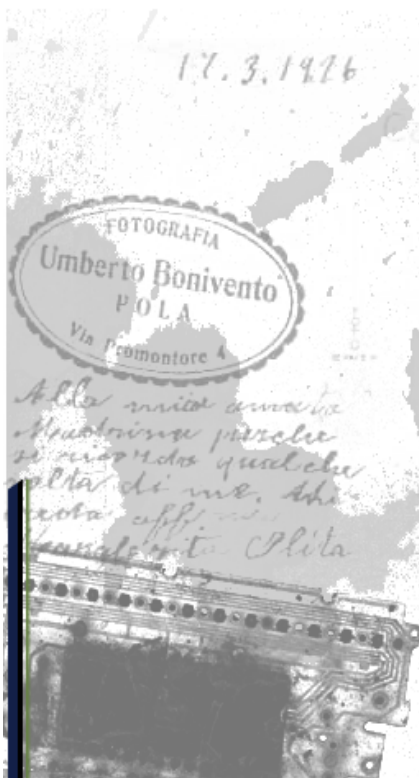
X'CON 2003

# 本文提纲

## 一、MANET面临的安全威胁

## 二、目前的研究成果

## 三、未来的研究方向



# 一、MANET面临的安全威胁

攻击的模型



主动攻击

针对路由协议的常见攻击

被动攻击

Active-n-m [1]

17.3.1926

cartolina postale



Stimabilissima  
Contessa Bentivoglio  
voglio abbracciarti.

Alle mie amiche  
che vogliono passare  
se ricordate qualche  
volta di me. Ah  
che affetto  
Umberto Piola





# 主动攻击



X'CON 2003

- 主动攻击主要指更改、删除传输的数据、干扰通信信道以及拒绝服务攻击等来自外部的攻击。这类攻击的主要目标是造成网络拥塞、扩散错误的路由信息、阻止服务的正常工作或者彻底关闭它们等等。



Atta mia amica  
Maurina pare che  
si ricordi qualche  
volta di me. Ah  
nota aff  
Maurina Piola

Stimabilissima  
Contessa Monto  
voglio abbracciarti.



# 被动攻击



X'CON 2003

- 攻击者并不去干扰正常的路由协议,而仅仅窃听路由数据,通过分析窃听到的路由数据就可能得到有用的信息。由于Ad hoc网络使用的是无线信道,所以这种攻击比较隐蔽,一般无法检测到。



## Active-n-m



X'CON 2003

- 作者在文献[1]中提出了一个攻击模型：  
把一个攻击者表示成Active-n-m，其中n是它所侵害的正常节点，而m是它本身所拥有的节点的个数。另外，如果一个攻击者将整个网络拓扑结构中所有关键路径上的节点都控制了，也就是说正常节点被分成了若干个子集，这些子集间如果要进行通信就必须通过这个攻击者所控制的节点，作者称之为Active-VC。





# 一、MANET面临的安全威胁

攻击的模型

针对路由协议的常见攻击

资源耗费攻击

路由破坏攻击

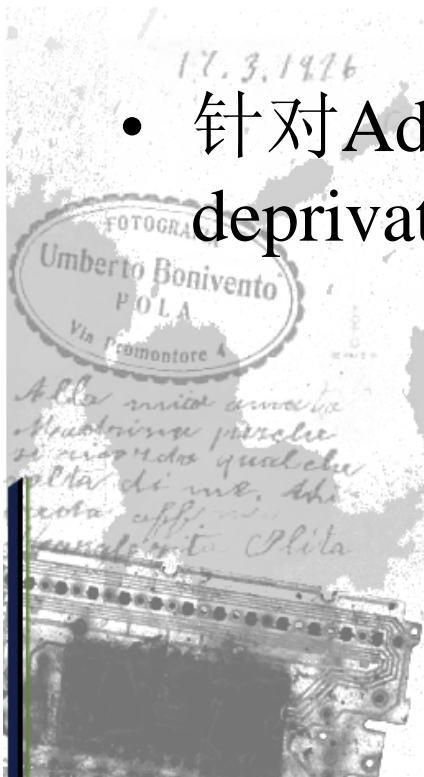
两种攻击都可以看作拒绝服务  
(Denial-of-Service, DoS) 攻击的实例。

# 资源耗费攻击



X'CON 2003

- 在Ad hoc网络中，由于节点的能量和带宽都非常有限，所以资源耗费攻击更容易被实施，造成的危害也更大。
- 针对Ad hoc网络还有一种叫做“剥夺睡眠(sleep deprivation torture)”的特殊攻击。



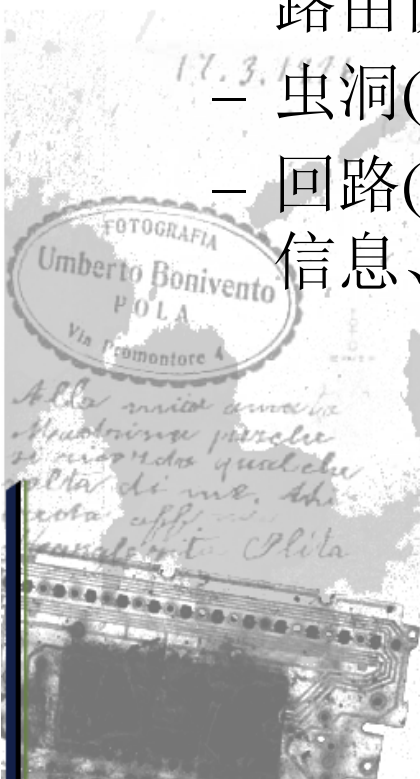


# 路由破坏攻击



X'CON 2003

- 攻击者可以创建：
  - 黑洞(black hole): 偷偷地将数据包全部丢弃。
  - 灰洞(gray hole): 有选择的丢弃其中的一部分, 如转发路由协议包而丢弃数据包。
  - 虫洞(wormhole)[2]: 通过有向天线等手段。
  - 回路(route loop)或是分割网络(partition): 通过修改路由信息、发送虚假路由信息造成路由。



## 二、目前的研究成果

1 密钥的管理

2 安全路由

3 入侵检测

## 二、目前的研究成果

密钥的管理



分布式密钥管理[3][4][5]

健壮路由

自组织密钥管理[6]

入侵检测

基于口令的密钥管理[7]

复活的鸭子 [8][9]

分布式轻负荷认证模型[10]



# 分布式密钥管理



X'CON 2003

- 文献[3][4]中提出了一种基于Shamir门限[5]方法的分布式密钥认证体系。它将CA的私钥SK分解成N个部分( $S_1, S_2, \dots, S_n$ ), 每个部分由一个节点存储。其中任意K个节点可以恢复出这个私钥, 从而充当CA, 完成证书的签发工作。

Key: How to share a secret



Atta mia amata  
Madrina pare  
si ricorda qualche  
volta di me. Ah  
nota aff  
Umberto Piola

Stimabilissima  
Contessa Obento  
voglio abbracciare.



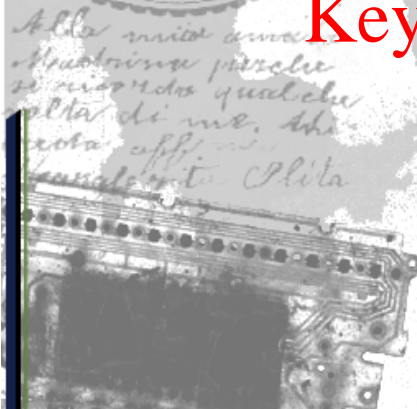
# 自组织密钥管理



X'CON 2003

- 文献[6]中提出了一种类似于PGP的自组织密钥系统。系统通过证书链来实现CA的功能。一个节点存储它所信任的节点的证书。如果一个节点想获得另一个节点的证书，那么它就顺着证书链去查找，直到找到为止。

Key: Small world phenomenon



# 基于口令的密钥管理



X'CON 2003

- 文献[7]中提出的基于口令的密钥管理策略是针对小范围内的成员间通信。首先，一个弱口令被分发给组内成员，每个成员用这个弱口令将自己的密钥信息提交，然后系统将这些提交的密钥信息综合起来生成系统密钥，最后所有用户就可以用这个系统密钥进行通信。



Atta mia amata  
Madrina pare  
si ricorda qualche  
volta di me. Ah  
nota aff.  
Umberto Piola

Stimatissima  
Contessa Benti  
voglio abbracci.





# 复活的鸭子



X'CON 2003

- Stajano 和 Anderson 在文献[8]和[9]中提出了铭记策略和它的扩展。在这个模型中,两个设备之间通过一个安全的瞬时关联形成一种主从关系.鸭子指从设备,而它的母亲指主控设备.从设备把第一个给它发送密钥的设备当作它的主控设备,并听从主控设备的指挥。

Key: imprinting policy



Atta mia amata  
Maurina parole  
si ricorda qualche  
volta di me. Ah  
nota aff.  
Luisa Piola



# 分布式轻负荷认证模型



X'CON 2003

- 文献[10]综合了上述几种模型的思想，提出了一种分布式轻负荷的认证模型。该模型的主要目的并不是要保障交易的绝对安全，而是要使攻击者付出的代价要高于交易本身。这样攻击者就不愿意付出大量的努力去破坏大量的交易，但是他可能付出较高的代价去破坏一个单独的交易。



Atta mia amata  
Maurina pare  
si ricorda qualche  
volta di me. Ah  
nota aff.  
Umberto Piola

Stimabilissima  
Contessa Obento  
voglio abbracciarti.



## 二、目前的研究成果

密钥的管理

SRP[11]

健壮路由

ARIADNE[12]

入侵检测

SEAD[13]

SAR [14]

激励机制[15][16]





X'CON 2003

# SRP

- SRP[11]假设在通信的两个节点间存在一个安全关联（Security Association, SA），通过SA进行双向验证来保证两个通信节点间路由信息的准确性，这样在路由请求过程中就可以不考虑中间节点的安全性。



Atta mia amata  
Maurina pare  
si ricorda qualche  
volta di me. Ah  
nota aff  
Maurina Piola

Stimabilissima  
Contessa Monto  
voglio abbracciarti.



# ARIADNE



X'CON 2003

- 文献[12]中提出了一种基于DSR的安全按需路由协议——Ariadne。

Ariadne分为三个阶段：

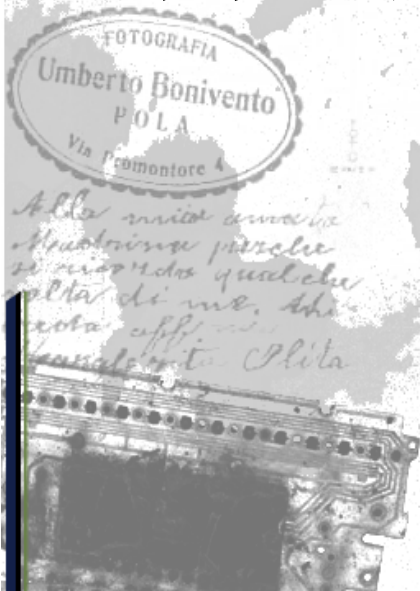
- 1) 提出一种允许目的节点验证路由请求的机制。
- 2) 提出了三种可以互换的机制来验证路由请求和路由回复中的数据。
- 3) 提出了一种有效的哈希算法来验证路径上的每个节点都不能缺少。

# SEAD



X'CON 2003

- SEAD [13]是Hu, Johnson和Perrig提出了一种基于距离矢量路由协议DSDV安全路由协议。通过让哈希值和路由信息中的权值以及序列号相关联,使用单向哈希函数来防止恶意节点减小路由信息中对应目的节点的权值或者增加它的序列号。





# SAR



X'CON 2003

- 文献[14]中提出的SAR算法是一种面向分层结构的ad hoc网络的安全路由算法。它假设已经存在一种密钥分发算法，使得在每一个层次上的节点共享一个对称加密密钥。并且它假设每个节点和它所处的信任等级是绑定得，节点不能随意修改它的信任等级，这样一个节点就不能解密其它层次上节点间传输的信息。



Atta mia amata  
Maurina pare  
si ricorda qualche  
volta di me. Ah  
nota aff  
Maurina Piola

Contessa Monto  
voglio strizza

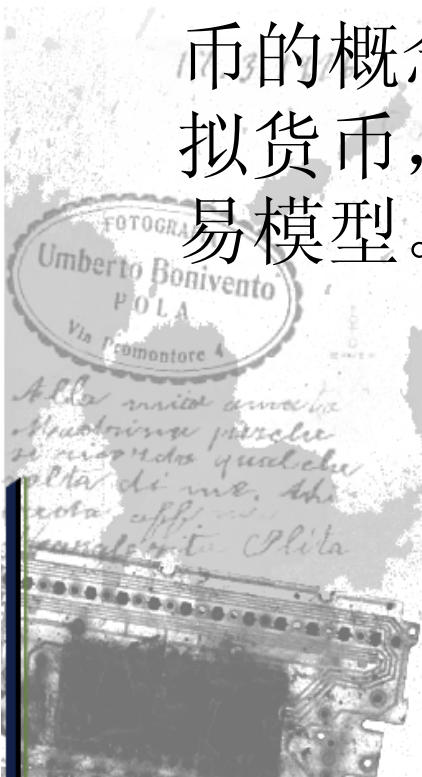


# 激励机制



X'CON 2003

- Buttyan和Hubanx将经济学中的思想引入到了Ad hoc网络中，他们在文献[15]和[16]中提出了虚拟货币的概念，并把它作为转发数据包的报酬。使用虚拟货币，作者提出了两种支付模型：钱包模型和交易模型。



## 二、目前的研究成果

密钥的管理

安全路由

入侵检测

分布式协作入侵检测[17]

Watchdog&Pathrater[18]

CONFIDANT[19][20][21]

CORE[22]

游戏理论[23]

性能比较[24]



# 分布式协作入侵检测



X'CON 2003

- Zhang和Lee在文献[17][24]中提出并在NS2上实现了一种分布式协作入侵检测体系模型。在这个模型中，IDS代理在每个单独的移动节点上运行，进行本地的数据采集和入侵检测，当一个节点发出异常警报时，周围的节点就配合进行检测并在整个网络范围内进行反馈。



Atta mia amata  
Maurina pare  
si ricorda qualche  
volta di me. Ah  
nota aff  
Maurina Piola

Contessa Abenti  
voglio abbracci



# Watchdog & Pathrater



X'CON 2003

- 斯坦福大学的Marti等人提出了一种看门狗和选路人算法[18]。
  - 看门狗是指数据包的发送者在将包发出去之后还要监视他的下一跳的节点，如果下一跳的节点没有对包进行了转发怎说明那个节点可能存在问题。
  - 选路人作为一种响应办法，它评定每一条路的信任等级，使数据包尽量避免经过那些可能存在恶意节点的路径。

# CONFIDANT



X'CON 2003

- CONFIDANT[19][20][21]是EPFL提出的一种入侵检测协议。它通过节点自身观察和相互通告的手段来检测几种已知类型的攻击，使得网络中节点在进行路由时绕过可能的恶意节点，进而将恶意节点孤立。模拟结果显示，对于拒绝转发这类攻击，CONFIDANT可以有效地对付占节点总数一半的恶意节点的攻击。



# CORE



X'CON 2003

- 文献[22]中提出了一种基于游戏理论[23]的CORE机制，它的主要目的是对付Ad hoc网络中的自私节点。节点的协作是通过一种相互配合的监督技术和一套信誉体系来实现的。每个节点的信誉分为主观信誉，直接信誉和功能信誉。这些信誉值被加权平均成一个总的信誉值，然后用它来决定是配合还是逐步孤立一个节点。

# 游戏理论

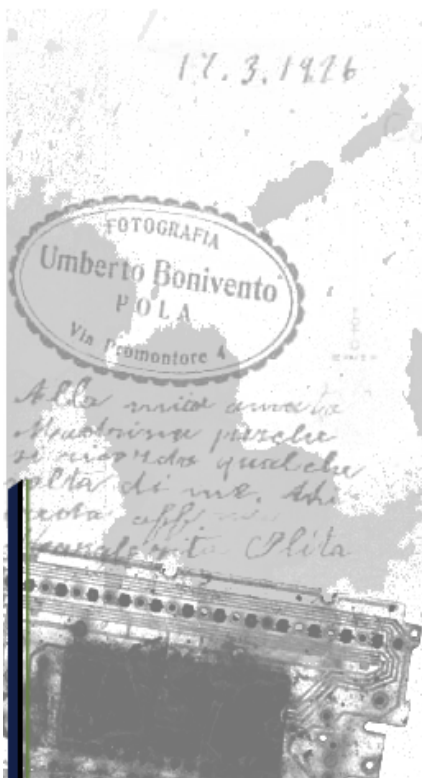


X'CON 2003

»The preference structure

»The prisoner's dilemma

»The Nash equilibria

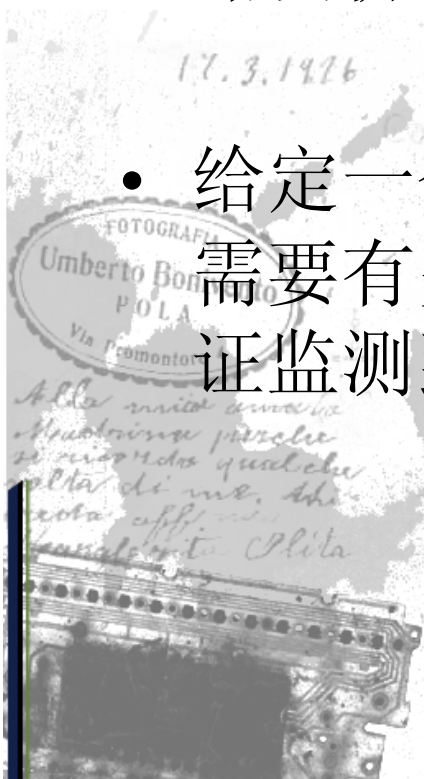


# 性能比较



X'CON 2003

- 入侵检测系统在不同的路由协议下的性能是不一样的。实验结果显示无论节点是否移动，先应式路由协议的性能要好于反应式路由协议。
- 给定一个路由协议和一个具有N个节点的系统，需要有多少个节点加入到入侵检测系统中才能保证监测到的攻击不小于一定的比例。





### 三、未来的研究方向



- **Network Performance Centric Security Design**

- **Game Theory in Security Design**

17.3.1 Rational exchange VS Fair exchange

- **Exploiting the Synergy between Peer-to-Peer and Mobile Ad Hoc Networks**



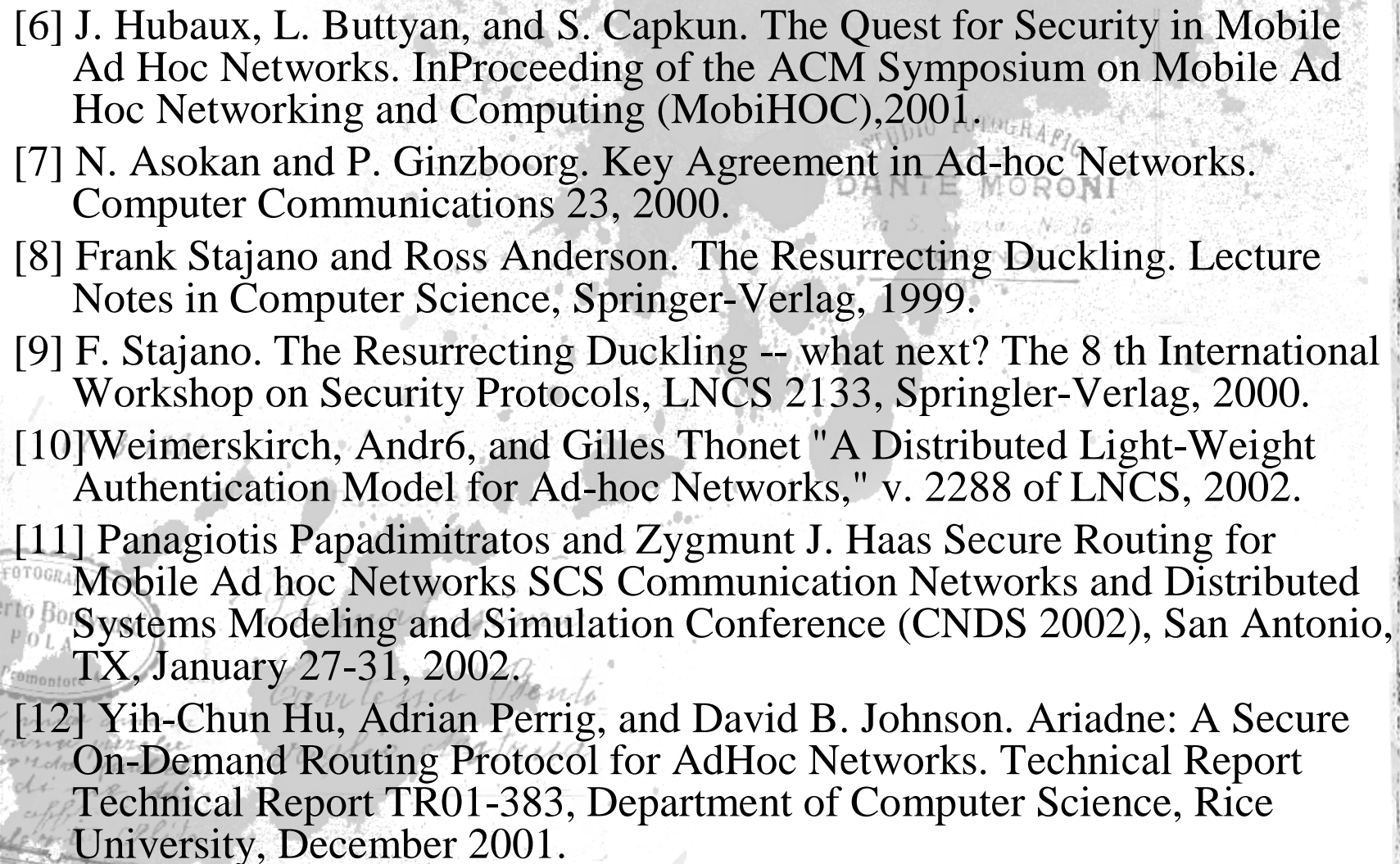
# 参考文献



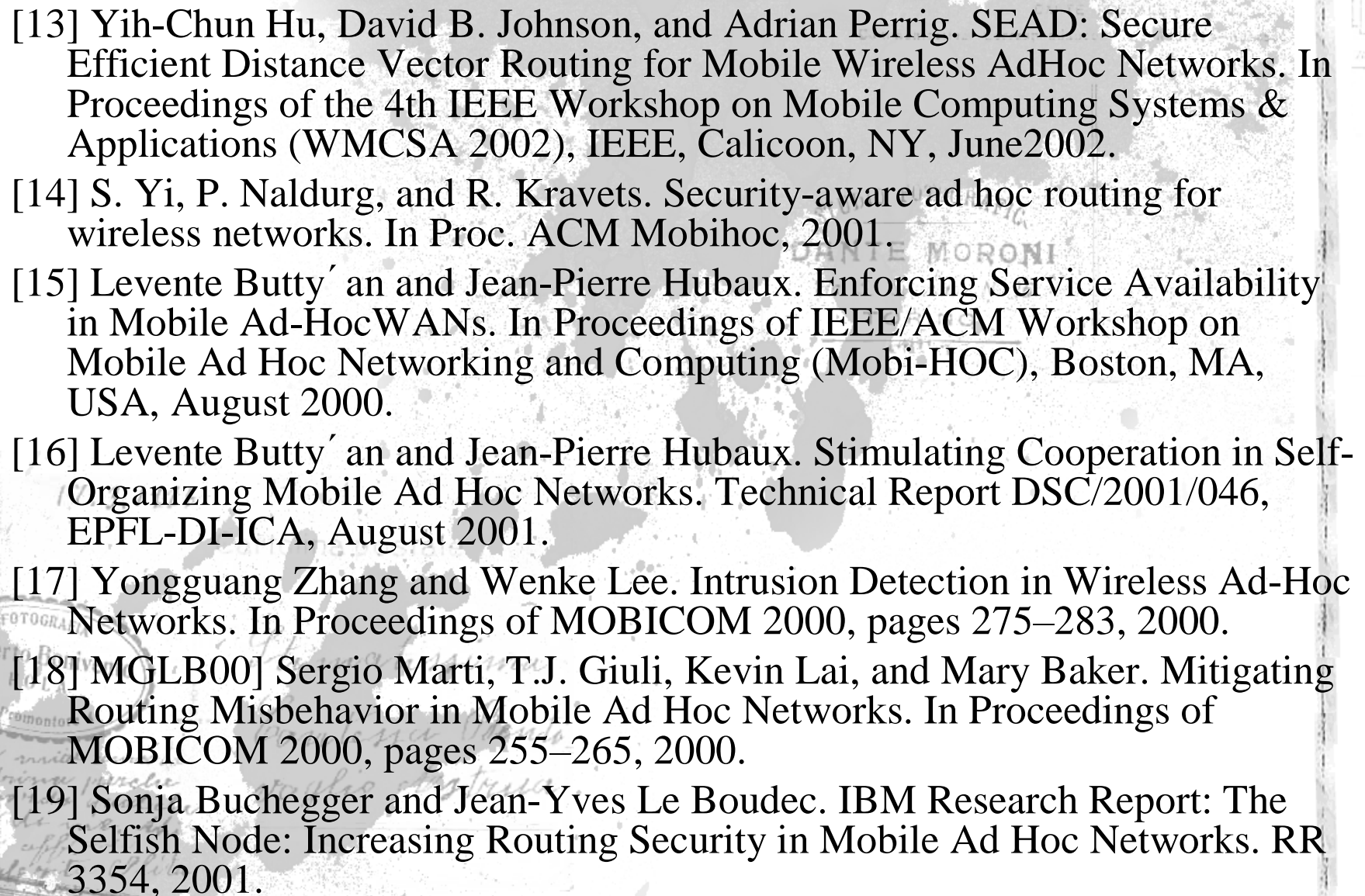
X'CON 2003

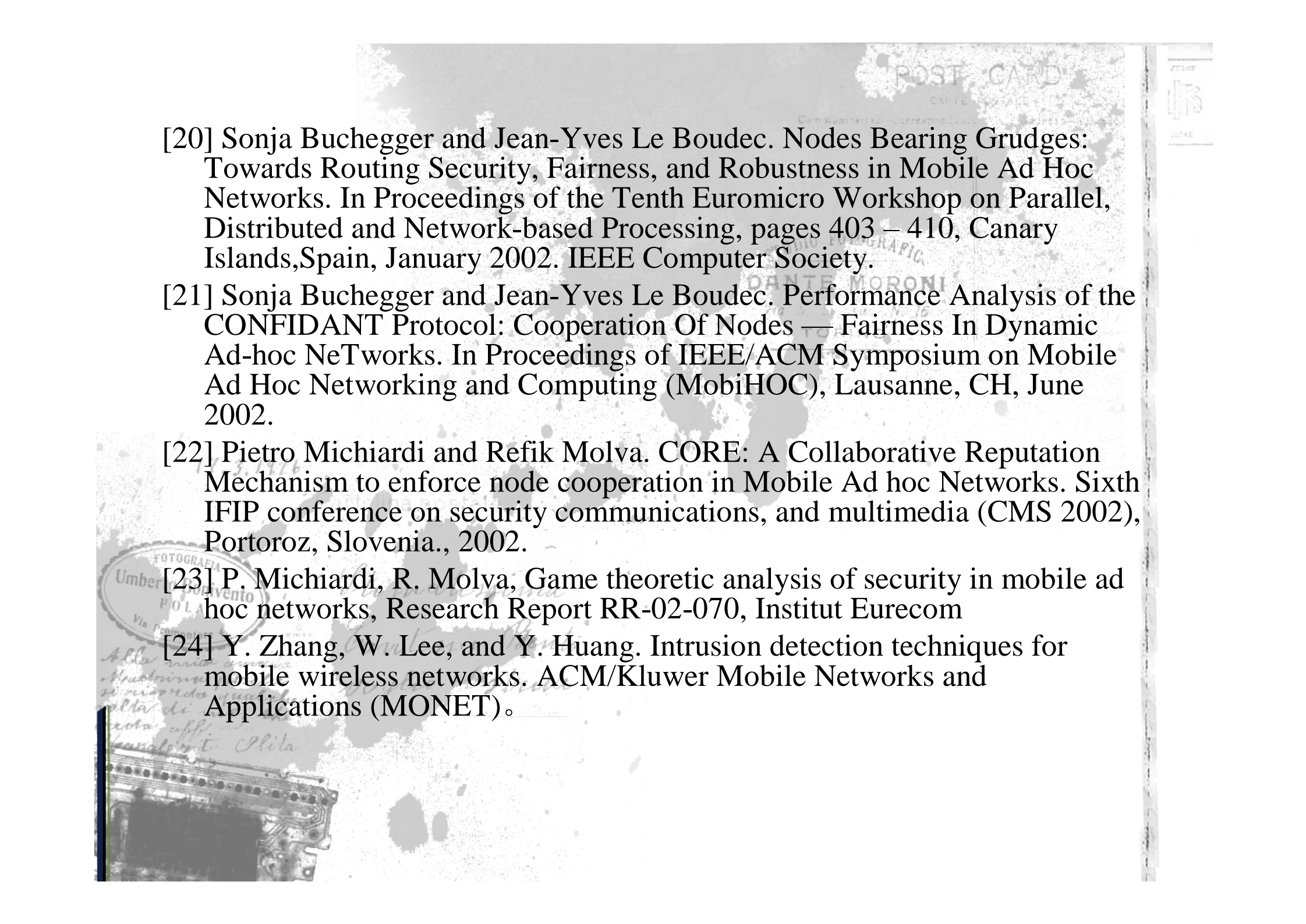
- [1] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks. Technical Report Technical Report TR01-383, Department of Computer Science, Rice University, December 2001.
- [2] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proceedings of the TwentySecond Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), IEEE, San Francisco, CA, April 2003.
- [3] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu and Lixia Zhang. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. IEEE 9th International Conference on Network Protocols (ICNP'01), 2001.
- [4] Haiyun Luo, Jiejun Kong, Petros Zerfos, Songwu Lu and Lixia Zhang, Self-securing Ad Hoc Wireless Networks accepted by the Seventh IEEE Symposium on Computers and Communications (ISCC'02).
- [5] A. Shamir, "How to share a secret," Communications of ACM, 1979



- 
- [6] J. Hubaux, L. Buttyan, and S. Capkun. The Quest for Security in Mobile Ad Hoc Networks. In Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), 2001.
- [7] N. Asokan and P. Ginzboorg. Key Agreement in Ad-hoc Networks. Computer Communications 23, 2000.
- [8] Frank Stajano and Ross Anderson. The Resurrecting Duckling. Lecture Notes in Computer Science, Springer-Verlag, 1999.
- [9] F. Stajano. The Resurrecting Duckling -- what next? The 8 th International Workshop on Security Protocols, LNCS 2133, Springer-Verlag, 2000.
- [10] Weimerskirch, Andr , and Gilles Thonet "A Distributed Light-Weight Authentication Model for Ad-hoc Networks," v. 2288 of LNCS, 2002.
- [11] Panagiotis Papadimitratos and Zygmont J. Haas Secure Routing for Mobile Ad hoc Networks SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.
- [12] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks. Technical Report Technical Report TR01-383, Department of Computer Science, Rice University, December 2001.



- 
- [13] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless AdHoc Networks. In Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), IEEE, Calicoon, NY, June 2002.
- [14] S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. In Proc. ACM Mobihoc, 2001.
- [15] Levente Buttyán and Jean-Pierre Hubaux. Enforcing Service Availability in Mobile Ad-Hoc WANS. In Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (Mobi-HOC), Boston, MA, USA, August 2000.
- [16] Levente Buttyán and Jean-Pierre Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. Technical Report DSC/2001/046, EPFL-DI-ICA, August 2001.
- [17] Yongguang Zhang and Wenke Lee. Intrusion Detection in Wireless Ad-Hoc Networks. In Proceedings of MOBICOM 2000, pages 275–283, 2000.
- [18] MGLB00] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In Proceedings of MOBICOM 2000, pages 255–265, 2000.
- [19] Sonja Buchegger and Jean-Yves Le Boudec. IBM Research Report: The Selfish Node: Increasing Routing Security in Mobile Ad Hoc Networks. RR 3354, 2001.

- 
- [20] Sonja Buchegger and Jean-Yves Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing, pages 403 – 410, Canary Islands, Spain, January 2002. IEEE Computer Society.
- [21] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes — Fairness In Dynamic Ad-hoc NeTworks. In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, June 2002.
- [22] Pietro Michiardi and Refik Molva. CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks. Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia., 2002.
- [23] P. Michiardi, R. Molva, Game theoretic analysis of security in mobile ad hoc networks, Research Report RR-02-070, Institut Eurecom
- [24] Y. Zhang, W. Lee, and Y. Huang. Intrusion detection techniques for mobile wireless networks. ACM/Kluwer Mobile Networks and Applications (MONET).



Thanks !

POST CARD

DATE

Cartolina postale



STUDIO FOTOGRAFICO  
DANTE MORONI  
Via S. ... N. 36  
TORINO

17.3.1926

Cartolina postale

FOTOGRAFIA  
Umberto Bonivento  
PIOLA  
Via Promontore 4

Alle mie amiche  
Maurina e Paola  
si ricorda qualche  
volta di me. Ah  
nota affettuosa  
Umberto Piola

Stimabilissima  
Contessa Benti  
voglio augurarvi



X'CON 2003