·安全技术· 文章编号：1000—3428(2013)12—0152—05 文献标识码：A 中图分类号：TP393

WSN 中基于阈值机制的虚假数据过滤方案

朱凌志[1]，赵巾帼[1]，梁俊斌[2]，刘志雄[3]

(1. 湖南工学院计算机与信息科学学院，湖南 衡阳 421002；2. 广西大学计算机与电子信息学院，南宁 530004；
3. 中南大学信息科学与工程学院，长沙 410083)

摘 要：传统虚假数据过滤方案无法过滤从非转发区域注入的虚假数据。为解决该问题，提出一种基于阈值机制的虚假数据过滤方案。节点在部署后建立到 Sink 的转发路径，每个数据包包含 t 个检测节点的消息验证码(MAC)以及 2 个安全阈值，转发节点分别对 MAC 和安全阈值进行正确性验证。理论分析及仿真实验结果表明，该方案能有效识别与过滤任意区域注入的虚假数据，并且具有较低的能量开销。

关键词：无线传感器网络；虚假数据过滤；消息验证码；阈值机制；密钥分发；妥协节点

False Data Filtering Scheme Based on Threshold Mechanism in Wireless Sensor Network

ZHU Ling-zhi[1], ZHAO Jin-guo[1], LIANG Jun-bin[2], LIU Zhi-xiong[3]

(1. School of Computer and Information Science, Hunan Institute of Technology, Hengyang 421002, China;
2. School of Computer and Electronics Information, Guangxi University, Nanning 530004, China;
3. School of Information Science and Engineering, Central South University, Changsha 410083, China)

【Abstract】Aiming at the problems that the traditional false data filtering schemes can not filter false data injection attacks from non-forwarding areas, this paper proposes a false data filtering scheme based on threshold mechanism. Each node establishes a path to Sink. Each data package includes t Message Authentication Code(MAC) of detecting nodes and two security threshold parameters. Each forwarding node not only checks the correctness of the MAC but also validates the security threshold parameters. Theoretical analysis and simulation experimental results demonstrate that this scheme can resist false data injection attacks from arbitrary areas, and consumes less energy than existing schemes.

【Key words】Wireless Sensor Network(WSN); false data filtering; Message Authentication Code(MAC); threshold mechanism; key distribution; compromised node

DOI: 10.3969/j.issn.1000-3428.2013.12.033

1 概述

无线传感器网络(Wireless Sensor Network, WSN)在环境监测、医疗卫生和人体监控等领域[1]具有广泛的应用前景，因此，WSN 是一个非常活跃的研究领域。传感器节点通常是部署在恶劣环境中甚至敌方区域，簇头一般需要经过多跳才能将数据传送给基站，且节点容易被俘获，攻击者可以利用存储在节点内的密钥伪造事实上并不存在的虚假事件，恶意篡改正在传送的数据包，发送重复数据包等[2]。若不加防范，虚假数据会引发错误警报，干扰用户决策，消耗有限的网络资源。此外，一旦节点被俘，攻击者很容易获取并利用存储在节点内的密钥信息伪造虚假数据，并通过妥协节点发送给邻居节点，其邻居节点将难以判断数据包的真假。因此，如何识别并过滤 WSN 中的虚假数据是一个具有挑战性的难题[3-4]。

目前，学术界在 WSN 中虚假数据的识别和过滤研究已经取得了一些进展。文献[4]提出一种传感器网络中虚假数据转发过滤的基本框架 SEF(Statistical En-route Filtering)。

基金项目：国家自然科学基金资助项目(61103245)；广西自然科学基金资助项目(2012GXNSFBA053163, 2012GXNSFAA053222)；湖南省科技计划科学研究基金资助项目(2010SK3057)；湖南省教育厅科学研究基金资助项目(13C205, 09C290)；湖南省大学生研究性学习与创新性实验计划基金资助项目(湘教通[2013]191 号)；衡阳市科技计划科学研究基金资助项目(2009KJ21)

作者简介：朱凌志(1979－)，男，讲师、硕士，主研方向：无线传感器网络，网络安全；赵巾帼，副教授、硕士；梁俊斌，副教授、博士；刘志雄，博士研究生

收稿日期：2012-05-03 **修回日期：**2012-08-22 **E-mail：**lingzhi0825@163.com

该方案的主要思想是借鉴数字签名的思想，在待发送的数据包后额外附加 t 个消息验证码(Message Authentication Code, MAC)，并在数据转发的过程中对数据包进行认证，从而实现对虚假数据的识别和过滤[4]，这里 t 是系统阈值，但是该方案没有将密钥与检测区域进行绑定，一旦攻击者俘获了 t 个不同的密钥分区，即可任意伪造假数据包而不被中转节点识别。文献[5]提出了一种基于哈希函数的过滤方案，该方案采用单向哈希链技术，保证中间节点只能认证而无法篡改数据，但该方案没有将节点密钥和哈希值进行绑定，因此，攻击者很容易从合法包中获取合法哈希值而攻破安全机制。文献[6]提出了一种基于簇组织和投票机制的过滤方案(Probabilistic Voting-based Filtering Scheme, PVFS)，该方案在一定程度上可以抵抗虚假报告攻击，过滤率不低，但簇头之间需要以比普通节点大得多的通信半径进行数据转发，簇头很容易耗尽能量。文献[7]提出了在路由时进行交叉的逐步认证机制 IHA。该机制能保证虚假数据在 T 跳之内被发现并且被过滤。但其密钥分发方式不适应于动态的 WSN 路由，从而需要较大的维护开销。文献[8]提出了一种基于多坐标轴的虚假数据过滤方案。该方案虽然能较好地适应多 Sink 和动态 Sink 的情形，但需要每个节点配备 GPS 等昂贵的定位设备，因此，开销太大。针对这种情况，文献[9]在文献[8]的基础上进一步提出了一种多维(multi-dimensional)的虚假数据过滤方案，该方案提高了覆盖性能和过滤概率。文献[10]提出了一种动态过滤方案，同时对付虚假数据注入攻击和 DOS 攻击。

SEF、IHA 和 PVFS 等方案都无法过滤从妥协节点的非转发区域注入的虚假数据，本文主要研究不受区域限制的虚假数据过滤策略，提出一种基于阈值机制的虚假数据过滤方案 TFDF(Threshold based False Data Filtering mechanism)。

2 基于阈值机制的过滤方案 TFDF

2.1 系统模型及相关假设

假设每个传感器节点具有唯一的 ID 标识，且节点在布撒后的一段较短的时间内是安全的。部署后，利用成簇机制组织成簇。假设传感器节点分布密度较大，事件发生后，至少有同一簇内的 t 个节点检测到。各个检测节点利用密钥对事件进行加密后生成 MAC，然后将 MAC 和位置信息发送给簇头，以生成数据报告。

普通传感器节点能力较弱，容易被俘获，而 Sink 节点无法被妥协，配备充足的能量、强大的计算、通信能力，并拥有全局秘密信息，能够对最终到达的假包进行检测和过滤。攻击者俘获节点后，可以利用存储在节点中的秘密信息伪造虚假数据分组并发送到网络中，或者利用妥协节点篡改传输中的合法数据包[3]等，但本文仅针对虚假数据注入攻击提出解决方案。

2.2 数据报告生成

在检测到突发事件后，簇头 C_i 收集簇内节点的感知数据并选取一个较完整的值 e 作为本次突发事件的描述，然后将 e 在簇内进行广播。簇内节点 S_i 将 e 与自身感知到的数据进行比较，若误差在一个规定的阈值之内，则利用与 Sink 共享的主密钥 K_i 对感知数据进行加密，生成 M_i:$K_i(e)$。然后，S_i 利用对偶密钥机制[11]将签名加密并发送给簇头 C_i。簇头收集簇内 t 个不同节点的签名并形成数据包 R，同样采用对偶密钥机制将数据包加密后发送给下一跳簇头。

$$R:\{e,S_1,S_2,\cdots,S_t,M_1,M_2,\cdots,M_i,Bin_v,T_v,T_c,flag\} \quad (1)$$

其中，标识符 Bin_v 是 t 位的二进制字符串，分别标示对应各个 MAC 的状态；T_v、T_c 和 $flag$ 分别标示被验证成功的 MAC 的数量、连续未被认证的传输跳数以及数据包的状态。Bin_v 的初始值为 t 个连续的 0，T_v、T_c 以及 $flag$ 的初始值均为 0。

2.3 转发过滤阶段

首先给出 2 个参数 T_{v-max} 以及 T_{c-max} 的取值计算过程，然后介绍转发过滤的过程。每个数据包后附带 t 个 MAC，令 $T_{v-max}=t$，当 T_v 超过阈值 T_{v-max} 时，说明数据包中所有 t 个 MAC 均已被验证成功，因此，后续节点无需再对该数据包进行验证。假设网络中有 N_c 个妥协节点，则攻击者为了捏造一个假数据包必须伪造(t–N_c)个假 MAC。若假包在妥协节点的转发路径中传输 1 跳被过滤的概率为 p_a，则其在该路径中传输的跳数约为：

$$\sum_{i=1}^{\infty} i\times(1-p_a)^{i-1}\times p_a=\frac{1}{p_a} \quad (2)$$

令 $T_{c-max}=1/p_a$，当 T_c 超过阈值 T_{c-max} 时，说明数据包在转发路径中已经连续传输 $1/p_a$ 跳而未被验证，因此，该数据包为攻击者从妥协节点的非转发区域注入的假数据包。

当中转节点接收到数据包时，按照以下步骤对 R 进行验证：

(1)首先检查数据包的状态标识 $flag$ 是否等于 1，若 $flag$=1，说明数据包中所有 MAC 均被验证成功，无需再对该数据包进行验证，因此中转节点直接转发数据包。

(2)若 $flag$ 不等于 1，检查数据包中包含的 MAC 的数量是否为 t。若数据包中包含多于或者少于 t 个 MAC，则直接将数据包 R 丢弃。

(3)如果 MAC 数量满足要求，那么检索密钥索引表，若没有存储与数据包 R 中相同的密钥，则 T_c 标志加 1。然后判断(T_c=T_{c-max})，若结果为 true，说明 R 已经连续传输了 T_{c-max} 跳而未被验证，断定该数据包为攻击者从妥协节点的非转发区域注入的假数据包，因此，直接将 R 丢弃，结束验证流程；若结果为 false，则转发数据包。

(4)若中转节点拥有与数据包 R 中相同的密钥，则利用该密钥和 e 重新计算一个 MAC，并将计算结果与待验证的 MAC 进行比较。如果 2 个 MAC 相等，则说明验证成功，置 T_c 标志为 0，T_v 标志加 1，并将 Bin_v 中对应于该 MAC 的标志位设为 1。然后判断 T_c=T_{c-max}，若结果为 true，则置 $flag$=1，结束验证流程，并转发数据包；若结果为 false，转发数据包。如果计算的 MAC 与待验证 MAC 不相等，则说

明验证失败，丢弃数据包。

TFDF 转发验证算法的伪代码如下：

//*当中转节点接收到数据包时，按照以下步骤对 R 进行验证*//

(1)如果数据包 R 的状态标识 flag 为真(即等于 1)，则直接转发数据包。

(2)检查数据包 R 中包含的 MAC 的数量是否等于 t，若不为 t 则直接将数据包 R 丢弃。

(3)检索密钥索引表，如果中转节点没有存储与数据包 R 中相同的密钥，T_c 标志加 1，然后判断 T_c=T_{c-max}，若结果为 true，则直接将 R 丢弃；若结果为 false，则转发数据包。

(4)如果中转节点拥有与数据包 R 中相同的密钥 K∈{Kiv, 1≤v≤t}，则利用 M=K(e)重新计算一个 MAC，如果 Miv 等于 M，则置 T_c 标志为 0，T_v 标志加 1，并将 Bin_v 中对应于该 MAC 的标志位设为 1，否则直接将数据包丢弃。

(5)中转节点转发数据包 R。

2.4 Sink 过滤

Sink 节点拥有全局密钥信息以及所有节点的位置信息，且具备强大的计算、存储能力以及充足的能量，能够过滤所有漏过中转验证而最终到达的虚假数据。当 Sink 接收到数据包时，对所有的 MAC 以及检测节点位置信息进行重新校验，如果所有 MAC 以及位置信息都正确，则接收数据包并执行相应的决策，否则将数据包丢弃。

3 性能分析与仿真结果

3.1 安全性分析

TFDF 和大多数已有方案一样[4-8]，在节点部署后的一段较短的时间内进行密钥分发。若在这段时间内有节点被妥协，则攻击者可以利用妥协节点干扰密钥分发，甚至造成密钥泄露，进而影响过滤方案的整体性能。此外，若攻击者从妥协节点的转发区域注入假数据，和已有方案一样，上游节点可以利用共享的密钥很快将假数据进行过滤。另一方面，若攻击者从妥协节点的非转发区域注入假数据，当假数据传输的跳数超过阈值 T_{c-max} 时，也会被过滤掉。因此，TFDF 结合密钥认证机制和阈值超越机制，能过滤从网络中任意区域注入的虚假数据。

3.2 过滤效率

若网络中有 N_c 个节点被妥协，攻击者为了捏造一个假数据包必须伪造(t–N_c)个假 MAC。以基于簇组织和投票机制的过滤方案[6]做比对分析，记假包在 PVFS 中传输 1 跳被过滤的概率为 p_v。

在 TFDF 中，攻击者从妥协节点的非转发区域注入的假包最多在网络中传输 t 跳，因此，其传输 1 跳被过滤的概率为 1/t，此外，攻击者从妥协节点的转发区域注入的假包在网络中传输 1 跳被过滤的概率为 p_v。当攻击者从妥协节点的转发区域以及非转发区域注入的假包比例为 1:α 时，假包在网络中传输 1 跳被过滤的概率为：

$$P_{a\_1}=\frac{1}{a+1}\times P_v+(\frac{a}{a+1})\times\frac{1}{t} \tag{3}$$

其传输 h 跳被过滤的概率为：

$$P_{a\_h}=1-(1-P_{a\_1})^h \tag{4}$$

图 1 为 TFDF 与 PVFS[6]的过滤概率对比情况。其中，攻击者从妥协节点的转发区域以及非转发区域注入的假包比例为 1:1、t=5、N_c=2、m=17、N=340。当攻击者从网络的任意区域注入虚假数据时，TFDF 能以比 PVFS 较高的概率过滤虚假数据，而 PVFS 仅能以较低概率对虚假数据进行过滤。如当 h=10 时，TFDF 和 PVFS 过滤假数据的概率分别为 97.3%和 21.4%，这是因为 PVFS 依赖中间节点对数据报告中 MAC 正确性进行验证，所以仅能过滤从妥协节点转发区域注入的虚假数据；而 TFDF 由中间节点对产生数据的源节点的合法性进行验证，从而能同时对从妥协节点转发区域和非转发区域注入的虚假数据进行过滤。

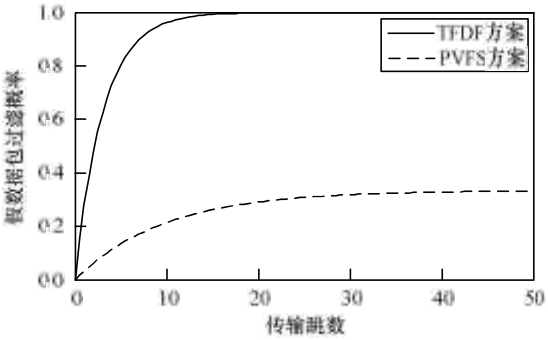

图 1 N_c=2 时虚假数据包过滤概率随传输跳数的变化

3.3 能量开销

文献[12]指出计算开销与传输数据包的能量相比可以忽略不计。在本文方案中，虽涉及到大量计算，但与传输数据包的能量相比来说还是较小，在此主要考虑数据转发的能耗。与已有过滤方案相比，TFDF 在数据包中额外增加了 3 个标志位以及一个字符串。

本文采用与 SEF[4]、PVFS[6]一样的方式对能耗进行量化分析。令 I_r、I_n、I_m、I_f 以及 I_b 分别表示不采用安全机制时的纯数据包长度、节点号长度、MAC 的长度、标志位长度以及字符串长度，则 TFDF 中数据包长度为：

$$I_{r0}'=I_r+(I_n+I_m)\times t+3I_f+I_b \tag{5}$$

TFDF 的能耗 E_0 可以表示为：

$$E_0=[1+\frac{I_m+I_n}{I_r}\times t+3I_f+I_b]\times [H+\beta\times(H-\sum_{i=1}^{H-1}P_{a\_i})] \tag{6}$$

图 2 为 100 个假包分别在 TFDF 和 PVFS 中传输 20 跳所消耗的能量对比情况。其中，假设攻击者俘获的妥协节点数量为 N_c=4，其他参数值设置分别为 I_r=24 Byte、I_n=10 bit、I_m=64 bit、N=1 000。从图 2 中可以看出，在 PVFS 中，数据包传输所消耗的能量随虚假数据量 β 和每个数据包所携带的 MAC 数量 t 增大而迅速增大。例如，当 β=0、

t=5 时，PVFS 所消耗的能量仅为 120 J，而当 β=10、t=9 时，其所消耗的能量达到了 850。在 TFDF 中，数据包传输所消耗的能量随 β、t 的增大而缓慢增大。例如，当 β=10、t=9 时，TFDF 所消耗的能量分别为 160 J。因此，与 PVFS 相比，TFDF 在能耗节省方面优势明显。

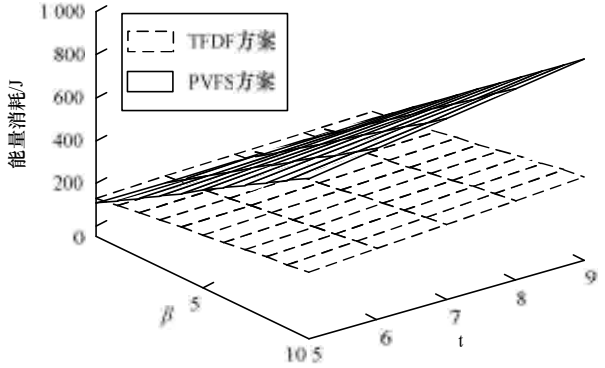

图 2　h=20、N_c=4 时 TFDF 与 PVFS 传输能耗对比

3.4　仿真实验

为了进一步验证 TFDF 的性能，本文利用 C++语言建立了模拟仿真平台。实验中采用的 TFDF 与 PVFS 数据包大小分别为 72 Byte、70 Byte，节点发送和接收一个 72 Byte 数据包的功耗分别为 6.2×10^{-3} J、1.25×10^{-3} J，发送和接收一个 70 Byte 数据包的功耗分别为 6×10^{-3} J、1.2×10^{-3} J[3]。仿真环境如下：在一个 $\pi\times45\times45$ m^2 圆形网络区域中，静态源节点和一个静态 Sink 分别位于圆心和圆周上，其他 340 个节点随机分布。源节点每隔 2 s 产生一个假数据包，总计产生 100 个数据包。节点采用的感知半径和通信半径分别为 5 m 和 2.5 m。限于篇幅，仅给出 TFDF 与 PVFS 在过滤概率以及能耗方面的实验数据。取 10 次仿真实验的平均值作为实验结果，表 1 给出了实验仿真参数。

表 1　实验仿真参数

参数	参数值
网络区域大小/(m^2)	$\pi\times45\times45$
节点数量	340
源节点发包间隔/s	2
源节点发包总数	100
节点通信半径/m	2.5
节点感知半径/m	5
全局密钥池大小 N	150
密钥分区数量	15
节点存储密钥数量	5

图 3 给出了当转发区与非转发区虚假包 1:1 时过滤概率随传输跳数的变化情况，其中，从妥协节点转发区域和非转发区域注入的假包各为 50 个。从图 3 可以看出：(1)假包在网络中传输的跳数越大，被过滤的概率也越高，例如在 TFDF 中，当 h=5 和 10 时，过滤概率 P 分别为 60%和 85%；(2)TFDF 过滤假包的性能远强于 PVFS，例如当传输跳数为 h=15 时，TFDF 和 PVFS 过滤假包的概率分别为 95%和 69%。

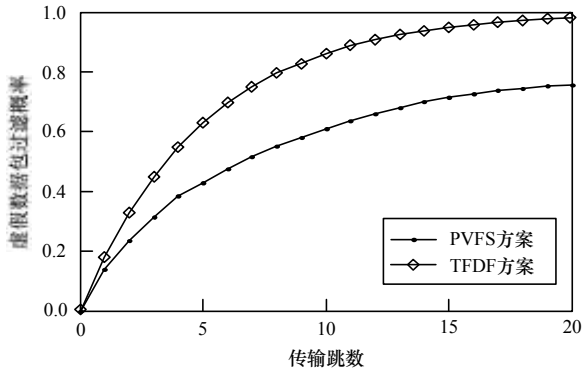

图 3　虚假数据包过滤概率随传输跳数的变化

图 4 为源节点产生的 100 个虚假数据包在 TFDF 与 PVFS 中的传输能耗对比情况。从图 4 可以看出，TFDF 所消耗的能量远低于 PVFS，例如当传输跳数为 h=10 时，TFDF 和 PVFS 传输假包所消耗的能量为 3.6 J 和 6.5 J。这是因为 TFDF 能通过尽早将从妥协节点的非转发区域注入的假包过滤掉而比 PVFS 节省能量。

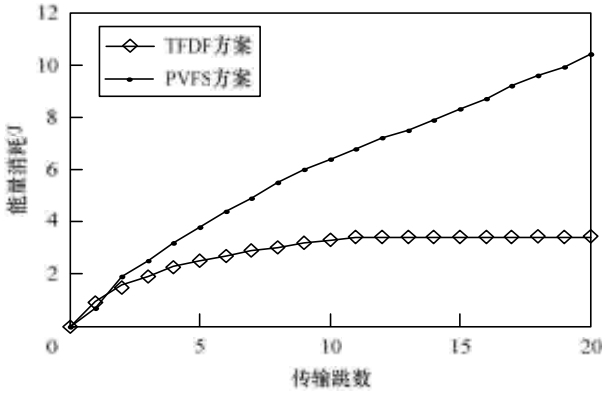

图 4　h=10 时 TFDF 与 PVFS 传输能耗对比

4　结束语

如何有效识别和过滤虚假数据包是无线传感器网络中一个具有挑战性的难题[3]，已有的方法无法对传感器网络中由妥协节点非转发区域注入的虚假数据进行有效检测、识别和过滤。本文在分析无法有效检测、识别和过滤的原因后，提出了一种解决方案 TFDF，节点在部署后建立到 Sink 节点的转发路径，每个数据包必须包含 t 个检测节点的 MAC 以及 2 个安全阈值，转发节点既对 MAC 正确性进行校验，还对阈值进行验证。理论分析和仿真结果表明，TFDF 能够有效防范非转发区域的虚假数据注入攻击，节约有限的网络资源，且安全性较好，但不能找到并隔离发送虚假数据的妥协节点，使得虚假数据还是不断地注入 WSN，直到耗尽节点能量和网络带宽为止。因此，研究更为主动的溯源追踪方案，找出并排除发送虚假数据的妥协节点将成为下一步的工作重点。

参考文献

[1] 任丰原, 黄海宁, 林 闯. 无线传感器网络[J]. 软件学报, 2003, 14(7): 1282-1291.

[2] 苏 忠, 林 闯, 封富君, 等. 无线传感器网络密钥管理的方案和协议[J]. 软件学报, 2007, 18(5): 1218-1231.

[3] 朱凌志, 赵巾帼, 刘志雄, 等. 无线传感器网络中虚假数据过滤方案[J]. 计算机应用研究, 2012, 18(5): 1218-1231.

[4] Ye Fan, Luo Haiyun, Zhang Lixia. Statistical En-route Filtering of Injected False Data in Sensor Networks[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(4): 839-850.

[5] Zhou Li, Ravishankar C V. A Fault Localized Scheme for False Report Filtering in Sensor Networks[C]//Proc. of International Conference on Pervasive Services. Santorini, Greece: IEEE Press, 2005: 59-68.

[6] Zhang Yutao, Yang Jun, Vu H T. The Interleaved Authentication for Filtering False Reports in Multipath Routing Based Sensor Network[C]//Proc. of the 20th International Conference on Parallel and Distributed Processing. Washington D. C., USA: IEEE Computer Society, 2006: 112-121.

[7] Zhu Senchun, Setia S, Jajodia S. An Interleaved Hop-by-hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks[C]//Proc. of IEEE Symposium on Security and Privacy. [S. l.]: IEEE Press, 2004: 259-271.

[8] Yu Lei, Li Jianzhong. Grouping-based Resilient Statistical En-route Filtering for Sensor Networks[C]//Proc. of the 28th Annual Joint Conference on Computer and Communications Societies. Rio de Janeiro, Brazil: IEEE Press, 2009: 1782-1790.

[9] Yang Feng, Zhou Xuehai, Zhang Qiyuan. Multi-dimensional Resilient Statistical En-route Filtering in Wireless Sensor Networks[J]. Journal of Internet Technology, 2011, 12(1): 130-139.

[10] Naresh K, Pradeep K P, Sathish K S. An Active En-route Filtering Scheme for Information Reporting in Wireless Sensor Networks[J]. International Journal of Computer Science and Information Technology, 2011, 2(4): 1812-1819.

[11] Feng J, Potkonjak M. Real-time Watermarking Techniques for Sensor Networks[C]//Proc. of IEEE International Conference on Security and Watermarking of Multimedia Contents. [S. l.]: IEEE Press, 2003: 391-402.

[12] Ren Kui, Lou Wenjing, Zhang Yanchao. Providing Location-aware End-to-end Data Security in Wireless Sensor Networks[J]. IEEE Transactions on Mobile Computing, 2008, 7(5): 585-598.

编辑 陆燕菲

(上接第 151 页)

[6] Upham D. JPEG-JSteg-V4[EB/OL]. (2007-06-01). http://www.funet.fi/pub/crypt/steganography/jpeg-JSteg-v4.diff.gz.

[7] Westfeld A. F5-A Steganographic Algorithm High Capacity Despite Better Steganalysis[C]//Proc. of the 4th International Workshop on Information Hiding. New York, USA: [s. n.], 2001: 289-302.

[8] Sallee P. Model-based Steganography[C]//Proc. of the 2nd International Workshop on Digital Watermarking. New York, USA: Springer-Verlag, 2003: 154-167.

[9] Sallee P. Model-based Methods for Steganography and Steganalysis[J]. International Journal of Image and Graphics, 2005, 5(1): 167-189.

[10] Kovovský J, Fridrich J, Pevný T. Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities[C]//Proc. of the 9th ACM Multimedia & Security Workshop. Dallas, USA: [s. n.], 2007: 3-14.

[11] Li Bin, Huang Jiwu, Shi Yunqing. Textural Features Based Universal Steganalysis[C]//Proc. of SPIE Security, Forensics, Steganography and Watermarking of Multimedia Contents X. [S. l.]: IEEE Press, 2008.

[12] Pevný T, Bas P, Fridrich J. Steganalysis by Subtractive Pixel Adjacency Matrix[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 215-224.

[13] Kharrazi M, Sencar H, Memon N. Improving Steganalysis by Fusion Techniques: A Case Study with Image Steganograohy[M]//Shi Y Q. Transactions on Data Hiding and Multimedia Security. Berlin, Germany: Springer-Verlag, 2006: 123-137.

[14] 邓诗智, 刘九芬, 张卫明, 等. 基于多种检测算法的隐写分析方法[J]. 计算机工程, 2008, 34(8): 150-152.

[15] Bishop C M. Pattern Recognition and Machine Learning[M]. New York, USA: Springer, 1995.

[16] Chang Chih-Chung, Lin Chih-Jen. LIBSVM: A Library for Support Vector Machines[EB/OL]. (2010-05-14). http://www.csie.ntu.edu.tw/~cjlin/libsvm.

[17] Doërr G. Image Database for Steganalysis Studies[EB/OL]. (2011-05-17). http://www.cs.ucl.ac.uk/staff/I.Cox/Content/Downloads.html.

编辑 陆燕菲