

文章编号:1001-9081(2010)08-2125-05

## 新的传感器网络假冒攻击源检测方案

王登第,柴乔林,孙翔飞,李涛

(山东大学 计算机科学与技术学院,济南 250101)

(wdd586@yahoo.com.cn)

**摘要:**针对传感器网络假冒攻击,提出了一种新的假冒攻击源检测方案。新方案利用基于身份的签名技术,结合节点报警规则,构造了基于邻居节点相互认证的单个试图假冒攻击源测定算法,以此为基础,扩充为针对局部区域内的多个试图假冒攻击源测定算法。新方案也提出了成功假冒攻击源测定算法,其中采用了汇聚节点监控排查恶意区域、普通节点认证转发报警消息机制。新方案适用于假冒攻击状况复杂、网络安全性要求较高的环境。仿真实验证了新方案在成功检测方面的有效性。

**关键词:**传感器网络;假冒攻击;恶意节点;测定算法;基于身份的数字签名

**中图分类号:** TP393.08    **文献标志码:**A

## Novel masquerader detection scheme in sensor networks

WANG Deng-di, CHAI Qiao-lin, SUN Xiang-fei, LI Tao

(College of Computer Science and Technology, Shandong University, Jinan Shandong 250101, China)

**Abstract:** Concerning the masquerader attacks in the sensor network, a new masquerader detection scheme was proposed. By means of the identity-based signature technique and node alarming rules, a single masquerader detection algorithm was constructed, which was based on the neighbor mutual authentication. Moreover, an algorithm to detect multiple masqueraders was acquired from this. In addition, the succeeded masquerader detection algorithm was proposed in this scheme in which the sink nodes monitor and examine the malicious region, and the normal nodes identify and transmit the alert messages. The proposal scheme is applicable to complicated masquerade attack and high network security demanding environment. The simulation experiments show the effectiveness in detection of the proposed scheme.

**Key words:** sensor network; masquerader attack; malicious node; detection algorithm; Identity-Based Signature (IBS)

## 0 引言

传感器网络是由部署在监测区域内大量微型传感器节点组成,通过无线通信方式形成的一个多跳的自组织的网络系统,其目的是协作的感知、采集和处理网络覆盖区域内感知对象的信息,并发送给观察者<sup>[1]</sup>。但是,由于传感器节点本身的脆弱性、无线信道的广播特性、多跳自组织的组网特性、节点间协作工作的特性使得传感器网络很容易受到一系列不同类型的恶意攻击<sup>[2]</sup>,其中之一就是假冒节点攻击(masquerade attacks)<sup>[3]</sup>,其表现为恶意节点假冒其他正常节点发送假冒消息扰乱网络协议的运行,这种攻击方式会影响节点间协同工作的效果、破坏网络路由机制、干扰数据分组的正常传输。

目前,关于传感器网络恶意节点假冒攻击检测的研究还较少。Bhuse 等人<sup>[3]</sup>首先对传感器网络中恶意节点假冒攻击的行为进行了研究,提出了基于邻居节点相互保护的检测机制和基于收发包计数校验的检测机制。但是这两种检测机制都不能定位假冒攻击源。Krontiris 等人<sup>[4]</sup>通过对黑洞攻击的研究发现恶意节点可以通过假冒攻击伪造路由更新包,提出了通过报警节点邻居集合求交定位单个恶意节点的检测方案。但此方案存在漏报和不能定位的问题,对此谢磊等人<sup>[5]</sup>对此方案进行了改进,提高了成功测定率。

但在对传感器网络安全性要求较高的环境下,如在军事领域中,要求必须对恶意节点的入侵具有较高的成功检测率,同时要求考虑在局部区域内存在多个恶意节点,以及出现恶意节点成功欺骗周围正常节点的情况。

针对上述问题,本文提出了一种新的假冒攻击源检测方案,利用该检测方案,本文构造了测定隔离局部区域多个假冒攻击源以及成功假冒攻击源的算法。随后通过仿真实验对该检测方案的成功率进行了验证。

## 1 模型假设与参数定义

### 1.1 基于身份的数字签名技术

1984年,Shamir<sup>[6]</sup>首次提出了基于身份的公钥密码体制,它简化了在公共密钥基础结构中密钥的生成过程。在公钥密码体制中,公钥来自于实体的一部分(用户的身份证号、网站的IP地址或者使用者的E-mail等)。换句话说,用户的公钥可以直接用其身份代替。私钥则是由可信第三方产生。2000年,Sakai 等人<sup>[7]</sup>首次突出了由双线性对构造基于身份签名(Identity-Based Signature, IBS)方案;2003年,Cha 等人<sup>[8]</sup>给出了一种针对IBS的安全性定义;2005年,Barreto 等人<sup>[9]</sup>提出了一种基于q-SDH群的IBS方案并在Random Oracle模型下证明了其安全性;随后Waters<sup>[10]</sup>提出了标准模型安全的IBE

收稿日期:2010-01-14;修回日期:2010-03-08。

基金项目:国家自然科学基金资助项目(60873232);山东省自然科学基金资助项目(Y2007G37)。

作者简介:王登第(1980-),男,山西临汾人,硕士研究生,主要研究方向:网络、分布式系统;柴乔林(1956-),男,山东青岛人,教授,主要研究方向:网络、分布式系统;孙翔飞(1984-),男,山东威海人,硕士研究生,主要研究方向:信息安全;李涛(1980-),男,山东济南人,硕士研究生,主要研究方向:网络、分布式系统。

方案，并扩展成 IBS 方案。

自 2000 年, Joux<sup>[11]</sup>首次把双线性对引入了密码系统的构造中后,大多 IBS 方案都采用双线性对来实现。但由于双线性运算的时间复杂度远远高于模指数运算,不利于无线传感器这一特殊的环境,因此本文仍采用由运算次数少、能耗低的模指数运算构造的 IBS 方案,如 Shamir<sup>[6]</sup>。

签名过程如下:

Alice, Bob 为交互的双方,其对应的身份及私钥分别为  $(ID_A, Sk_A)$ ,  $(ID_B, Sk_B)$ 。

1) Alice 随机选取消息  $M$  发送给 Bob。

2) Bob 计算  $H(M)$ ,并使用其私钥  $Sk_B$  对  $H(M)$  进行签名,得到签名消息  $Sign_{sk_B}(H(M))$ ,发送给 Alice。其中  $H(M)$  表示 Hash 函数。

3) Alice 收到  $Sign_{sk_B}(H(M))$  后,用 Bob 的身份公钥  $ID_B$  解签名得到  $H(M)'$ ,并验证  $H(M)'$  与  $H(M)$  是否相等,相等即为合法签名。

## 1.2 网络模型假设

为不失一般性,对网络模型作如下假设:

1) 传感器网络由相同传感器节点组成,它们具有相同的通信半径,设为  $R$ 。节点一经部署就不再移动,具有全网唯一的  $ID$  标识。

2) 节点在二维平面上随机均匀撒布,单个节点通信覆盖面积内的节点数期望为  $k$ ,节点的邻居集合记为  $N(ID)$ 。

3) 汇聚节点具有持续电源,较其他节点具有较强的运算能力和较大的存储空间。

4) 恶意攻击发生在整个网络拓扑建立完毕,在汇聚节点还没有重新更新路由的  $\Delta t$  时间段内。

## 1.3 网络拓扑结构建立

1) 初始阶段,汇聚节点存储了其辖域内所有普通节点的  $ID$ ,每个普通节点提前设置好自己的  $ID$  对应的私钥  $Sk_{ID}$ ,汇聚节点的私钥为  $Sk$ 。

2) 节点传输的数据分组拥有优先级  $l$ ,  $l \in \{l_1, \dots, l_n\}$ ,优先级从  $l_1$  到  $l_n$  递减排列,优先级水平的数量  $n$  取决于具体应用和用户希望划分的级别。

3) 汇聚节点经过  $\Delta t$  时间周期性广播路由更新消息建立全局拓扑结构,广播包结构如下:

$Broadcast(ID, HopCount)$

其中  $HopCount$  表示到达该节点的最小跳数。当节点转发该广播包时会加上自己的  $ID$  及  $HopCount$  值,使所有的邻居知道自己的  $ID$  及到达汇聚节点的最小跳数。

4) 当该节点广播完该路由更新消息后,从通过它认证的上一层邻居节点中选取能量最多的节点,向汇聚节点转发 Ack 数据包,其结构如下:

$Ack(Sign_{sk_ID}(H(ID, HopCount, Energy, N(ID))), ID, HopCount, Energy, N(ID))$

其中  $Energy$  表示该节点拥有的能量。

5) 汇聚节点收到各节点的 Ack 返回包后,将各节点的  $ID, HopCount, Energy, N(ID)$  存储到内存当中,并记录首次收集全体节点 Ack 返回包所需时间  $t$ 。

6) 各节点以一定时间间隔  $t'$  ( $t' < \Delta t$ ) 周期性向汇聚节点发送优先级为  $l_n$  的 Ack 确认数据分组,表明自己的有效性。

## 1.4 恶意节点行为

根据恶意节点的行为特点可以分为试图假冒攻击源和成功假冒攻击源两类。

**试图假冒攻击源** 具有该类攻击行为的恶意节点,试图假冒其他节点,向其邻居节点广播路由变更消息,欺骗其他节点向其传输数据分组,从而改变路由结构。在局部区域内,可能存在多个试图假冒攻击的节点。

**成功假冒攻击源** 具有该类攻击行为的恶意节点,已经成功欺骗其所有邻居节点,并与所有邻居节点组成恶意区域欺骗正常节点。在该区域中的恶意节点不向外界发送任何消息,只接受周围被欺骗成功的邻居节点转发给它的消息。由于受害邻居节点是被恶意节点欺骗后造成被动攻击,本身并不假冒任何节点,所以它们仍以正常节点的身份分布在恶意节点周围,正常节点仍向其转发数据分组,受害邻居节点将所有接收到的数据分组全部转发给恶意节点,从而造成路由黑洞。由于恶意节点和被它成功欺骗的邻居节点往往组成闭合的连通子图,致使其下游节点无法通过该恶意区域。因此该恶意区域越靠近汇聚节点,造成的危害也越大。

本文对这两类假冒攻击行为进行分析,提出如何有效检测假冒行为和如何有效地剔除恶意节点。

## 2 假冒攻击入侵检测机制描述

### 2.1 节点报警规则

对于试图假冒攻击,本文采用基于局部包检测触发假冒攻击的报警的规则:

1)如果有节点假冒自己发送路由更新包,则主动报警并将要求签名消息广播给邻居节点。

2)如果有节点假冒自己不存在的邻居发送路由更新包,则主动报警并将要求签名消息广播给邻居节点。

3)主动报警节点向邻居广播自己的测定集,以传递攻击源报警信息。

4)如果有节点假冒自己存在的邻居发送路由更新包,则不能触发报警机制,只能通过接收其他主动报警节点的测定集信息产生被动报警,被动报警节点也向邻居广播测定集信息。

对于假冒攻击成功形成恶意区域,本文采用汇聚节点监控报警机制:

若汇聚节点在  $t' + t$  时间后统计的未应答节点队列中出现  $k$  个相邻节点,则说明回路上可能出现了恶意区域。汇聚节点报警并对存储的节点信息进行分析。

### 2.2 总体检测步骤

新的假冒攻击检测方案分为 3 个阶段:触发报警阶段、攻击源定位阶段、决策与防御阶段。

**触发报警阶段** 即网络完成各项初始化工作,包括相邻节点路由建立完毕、汇聚节点掌握其辖域内节点数量、各节点到达汇聚节点的最小跳数、各节点当前能量、当前邻居等状况信息。网络此时出现恶意节点并触发入侵检测模型报警规则阶段。

**攻击源定位阶段** 若恶意节点为试图假冒攻击节点,则采用邻居监控报警机制,通过恶意节点广播的非法  $ID$  签名直接定位出恶意节点。若恶意节点成功欺骗了其邻居,则采用汇聚节点监控报警机制,通过汇聚节点监控到其辖域内大量相邻节点不再向其发送数据的情况,采用从到达汇聚节点最小跳数最少的未回应节点开始排查的策略,并最终定位出恶意节点。

**决策与防御阶段** 在成功定位恶意节点的基础上,邻居节点主动将该恶意节点从邻居列表中删除,或者汇聚节点广

播通知所有与恶意节点相邻的节点删除该恶意节点。

### 2.3 试图假冒攻击源测定算法

依据恶意节点与被假冒节点之间的跳数可将假冒方式分为3类,即假冒两跳以外节点、假冒一跳节点(假冒邻居)、假冒两跳节点。

#### 2.3.1 假冒两跳以外节点

假设节点A被俘获成为恶意节点,妄图假冒节点B( $\forall C \in N(A), B \notin N(A), B \notin N(C)$ ),为了欺骗周围正常节点向其传输数据分组,A节点必须首先向其所有邻居节点以广播形式发出重建路由的消息M,以达到欺骗正常节点进行路由调整的目的。邻居节点C收到M并触发报警规则2)后执行如下检测过程:

- 1) 节点C产生随机数 $r_c$ 并发送给邻居。
- 2) 节点C的邻居节点D( $D \in N(C), D \neq A$ ),收到 $r_c$ 后,产生签名 $\sigma_D = Sign_{sk_D}(r_c)$ ,并将 $\sigma_D$ 发送给节点C。
- 3) 由于节点A要冒充节点B,需要伪造签名 $\sigma_B = Sign_{sk_B}(r_c)$ ,由于节点A无法知道节点B的私钥 $Sk_B$ ,因此无法伪造签名。
- 4) 通过验证签名节点C发现收不到来自节点A的合法签名,确定A为恶意节点,并将节点A从 $N(C)$ 中删除。
- 5) 节点C向其邻居节点广播报警消息( $A \parallel unvalid, Sign_{sk_C}(H(A \parallel unvalid))$ )。
- 6) C的邻居节点收到C传递的报警消息后,首先检查其邻居列表,若存在A节点并且报警消息签名验证通过,则将A节点删除并再次广播报警消息,否则丢弃此报警消息。

#### 2.3.2 假冒一跳节点

假设节点A被俘获成为恶意节点,妄图假冒节点B( $B \in N(A)$ )。A节点向其所有邻居节点以广播形式发出重建路由的消息M。节点B收到M后触发报警规则1),A的邻居节点C( $C \in N(A), C \notin N(B)$ )收到M并触发报警规则2),后执行检测过程如2.3.1中所示步骤。若A的邻居节点D( $D \in N(A), D \in N(B)$ ),收到报警消息( $A \parallel unvalid, Sign_{sk_C}(H(A \parallel unvalid))$ )后,触发报警规则4),并将节点A从 $N(D)$ 中删除。

#### 2.3.3 假冒两跳节点

假设节点A被俘获成为恶意节点,妄图假冒节点B( $\exists C \in N(A), B \notin N(A), B \in N(C)$ )。A节点向其所有邻居节点以广播形式发出重建路由的消息M。A的邻居节点C( $C \in N(A), C \notin N(B)$ )收到M并触发报警规则2),后执行检测过程(如2.3.1节中所示步骤)。若A的邻居节点D( $D \in N(A), D \in N(B)$ )。收到报警消息( $A \parallel unvalid, Sign_{sk_C}(H(A \parallel unvalid))$ )后,触发报警规则4),并将节点A从 $N(D)$ 中删除。

对局部区域内存在多个假冒攻击源的情况,由于存在某个节点与其中一个或者两个恶意节点互为邻居,但不与某些报警节点互为邻居的现象。若恶意节点未触发该节点报警规则,且报警消息无法传递到该节点,会使该节点产生漏报。

### 2.4 成功假冒攻击源测定算法

成功假冒攻击源考虑恶意节点在没有得到汇聚节点私钥的情况下成功欺骗它周围所有邻居节点,使它周围邻居认为它是上层节点,将接收到的数据包只向恶意节点转发的情况。由于恶意节点不向外界发包,受害邻居点也不假冒任何节点,只是将接收到的数据包全部转发给恶意节点,如果这些节点组成连通子图,则危害是巨大的。一旦这些受害节点被告知

恶意节点是假的上层节点,受害节点会立即切断与恶意节点的连接。

成功假冒攻击源测定算法步骤如下:

1) 汇聚节点知道其辖域内所有节点,以及各节点的邻居信息。然后以每个节点为表头,通过添加该节点的上一层邻居节点组成链表。

2) 由于各节点以一定时间间隔 $t'$ 周期性向汇聚节点发送一个具有最低优先级的确认包,以表明自己的有效性。当汇聚节点长期收不到一个或者少数几个节点的确认包,则说明这几个节点失效了(此时如果确实存在恶意节点,由于其危害程度不大所以先不予考虑),到了 $\Delta t$ 时间后重新广播再次建立路由拓扑。

3) 如果汇聚节点在 $t' + t$ 时间后收不到 $k$ 个连续相邻(处在同一区域内的)节点的确认包,则说明路由回路上可能出现了恶意区域,触发汇聚节点的报警机制。

4) 汇聚节点查找所存储的节点记录中有哪些节点没有向它发送确认包,并把这些未回应节点按照到汇聚节点的跳数由小到大排成节点序列。然后将该序列中的节点与所存储的节点上层邻居链表进行比对,如果链表中某个节点的所有上层邻居节点全部出现在未回应节点序列中,那么该节点就被确定为潜在的恶意节点。

5) 将这些潜在恶意节点按照到达汇聚节点的跳数分为不同的潜在恶意节点集合,将离汇聚节点最近集合中的潜在恶意节点,按其上层邻居数多少由大到小进行排序。把上层邻居数最多的潜在恶意节点判定为恶意节点。

6) 如果离汇聚节点最近集合中的最大上层邻居数的潜在恶意节点只有一个,则可以判定此节点为恶意节点。如果最大上层邻居数相同的潜在恶意节点有多个,汇聚节点首次判定集合中第一个节点为恶意节点。

7) 假设 $ID_1^*$ 为恶意节点,汇聚节点发出报警消息,报警消息为:( $N(ID_1^*), ID_1^* \parallel unvalid, Sign_{sk}(H(ID_1^* \parallel unvalid))$ ),将此报警消息广播出去。

8) 其他节点收到此报警消息包后,首先检查 $N(ID_1^*)$ 中有无自己的ID标识,如果没有则只转发此报警消息。如果多次收到相同的报警消息,则只转发第一个报警消息,其余丢弃。

9) 恶意节点的邻居节点收到此报警消息后,首先验证汇聚节点的签名。若签名通过,则将 $ID_1^*$ 从自己的邻居列表中删除,并转发此报警消息。

10) 经过时间 $t' + t$ 后,汇聚节点仍未接收到恶意节点上层邻居节点发送的确认包,说明此次的判定失误,将集合中第2个节点 $ID_2^*$ 判定为恶意节点,并发送报警消息( $N(ID_1^*), N(ID_2^*), ID_1^* \parallel valid, ID_2^* \parallel unvalid, Sign_{sk}(H(ID_1^* \parallel valid, ID_2^* \parallel unvalid))$ ),将此报警消息广播出去。 $N(ID_1^*)$ 中的节点重新添加 $ID_1^*$ 为邻居节点, $N(ID_2^*)$ 中的节点断开与 $ID_2^*$ 节点的连接。直至最终测定出恶意节点。

## 3 仿真实验和结果分析

### 3.1 仿真环境设置

仿真工具采用Omnet++3.2p1,网络覆盖面积为 $600\text{ m} \times 600\text{ m}$ 。在该区域内分五次均匀随机分布100、150、200、250、300个节点,分别对单个假冒源试图攻击检测、局部区域多个假冒源试图攻击检测,成功假冒攻击源检测进行仿真。每一轮进行500次仿真。

### 3.2 仿真结果参数定义

- 1) Nnum: 节点数。每一轮仿真实验所采用的节点个数。
- 2) Mc: 漏报数。在一次仿真实验中,发生节点未能检测出恶意节点的情况,记为产生漏报 1 次。
- 3) Ps: 成功检测率。每种检测算法 500 次实验完成后,成功检测次数所占比例。
- 4) Oc: 签名与验证签名操作次数。节点进行签名记为 1 次操作,收到数据包后,对签名进行验证,也记为 1 次操作。OcMax 表示节点最大签名与验证签名次数、OcMin 表示节点最小签名与验证签名次数、OcAve 表示节点平均签名与验证签名次数。
- 5) Nb: 恶意节点周围邻居数。NbMax 表示恶意节点最大邻居数、NbMin 表示恶意节点最小邻居数、NbAve 表示恶意节点的平均邻居数。
- 6) Mn: 恶意节点数。MnMax 表示最大恶意节点数, MnMin 表示最小恶意节点数、MnAve 表示平均恶意节点数。

### 3.3 单个假冒源试图攻击检测结果

每次仿真随机选择一个恶意节点实施假冒攻击,算法仿真结果如表 1 所示。

表 1 单个假冒源试图攻击检测结果

Nnum	NbMin	NbMax	NbAve	OcMin	OcMax	OcAve	Mc	Ps
100	5	19	10.86	22	499	197.80	0	1
150	4	24	15.94	25	969	443.44	0	1
200	5	29	19.88	55	1329	768.07	0	1
250	5	41	25.91	145	2834	1275.53	0	1
300	7	50	28.97	110	4179	1661.50	0	1

#### 3.3.1 算法有效性分析

由于本文提出的测定算法是通过签名机制直接测定恶意节点而非邻居节点测定集求交定位,所以单个假冒源测定成功率与网络拓扑状况无关,也与恶意节点邻居数无关,检测成功率 100%。因此,该算法在单个假冒源检测成功率方面具有较好的效果。但是随着网络密度的增大,网络中节点的邻居数增多,签名与验证签名操作次数也随之升高。

表 2 多个假冒源试图攻击检测结果

Nnum	MnMin	MnMax	MnAve	NbMin	NbMax	NbAve	OcMin	OcMax	OcAve	Mc	Ps
100	2	5	2.88	6	17	12.33	117	1948	778.63	13	0.97
150	2	7	3.55	7	24	15.61	324	4049	1608.93	4	0.99
200	2	8	4.24	8	32	20.15	238	6803	3362.32	0	1.00
250	2	13	5.32	11	39	24.91	408	18349	6328.22	0	1.00
300	2	14	5.78	13	45	28.53	1341	26759	9188.76	0	1.00

#### 3.4.1 算法有效性分析

在某节点与某些恶意节点相邻,但不与某些报警节点相邻的情况下,若恶意节点不触发此节点的报警规则,该节点会产生漏报。如表 2 所示,当节点数为 100 时产生的漏报次数较多,因为此时网络节点密度较小,出现漏报现象的可能性较大。随着网络密度的增加,被动报警节点与主动报警节点互为邻居的情况增多,使得漏报次数明显下降。所以,该算法在多个假冒源测定方面也具有较高的检测成功率。但是,随着网络密度的增大,签名与验证签名操作次数也随之增多。

#### 3.4.2 算法复杂度分析

假设网络中各节点平均邻居数为  $n$ ,局部区域内平均恶

#### 3.3.2 算法复杂度分析

假设网络中各节点平均邻居数为  $n$ ,为检测出其邻居节点集合中的恶意节点,该节点需要向其所有邻居节点发出签名请求,所有邻居节点共进行了  $n$  次签名操作,签名数据包返回后,该节点需要进行  $n$  次验证签名操作,并检测出恶意节点,然后将检测结果签名后广播给邻居节点,被动报警节点需要对此报警消息进行解签名操作。因此,一个节点想要检测出恶意节点,所需要的签名与验证签名操作次数约为  $n \times 2$ ,恶意节点有  $n$  个邻居节点,所以检测出单个恶意节点的操作次数约为  $n \times 2 \times n$ ,因此可推出该算法平均时间复杂度为  $O(n^2)$ ,算法可在多项式时间内完成。

#### 3.3.3 单个假冒源试图攻击测定算法与 Krontiris 算法比较

本文提出的单个假冒源试图攻击测定算法(SMDA)与文献[4]提出的报警节点邻居集合求交定位算法(Krontiris)在检测成功率方面的比较如图 1 所示。

从图 1 可以看出,本文提出的单个假冒源试图攻击测定算法检测成功率要高于 Krontiris 算法,但由于 Krontiris 算法邻居节点间不涉及签名与验证签名操作,所以 Krontiris 算法的复杂度要小于单个假冒源试图攻击测定算法,因此要针对应用环境的侧重点选择适当的检测方案。

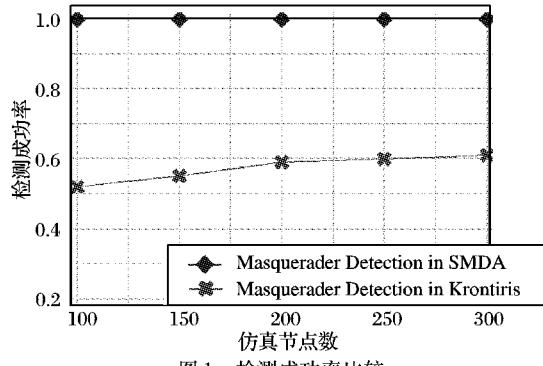


图 1 检测成功率比较

### 3.4 多个假冒源试图攻击检测结果

每次仿真首先随机选取一个节点作为“种子节点”,在“种子节点”的邻居节点中随机选取多个节点作为局部区域内的多个恶意节点,并将恶意节点的数量限定为不超过“种子节点”邻居数的  $1/3$ 。算法仿真结果如表 2 所示。

意节点数为  $m$ 。同理,为检测出邻居节点集合中的单个恶意节点,需要的签名与解签名操作次数约为  $n \times 2 \times n$ ,但要检测出  $m$  个恶意节点,所需要的操作数约为  $n \times 2 \times n \times m$ ,因此可推出该算法平均时间复杂度为  $O(n^2 \times m)$ ,算法可在多项式时间内完成。

### 3.5 成功假冒源攻击检测结果

每次仿真随机选择一个节点作为成功假冒源,并与其所有邻居节点组成恶意区域。通过收集不同样本集合的首次检测成功率、第 2 次检测成功率、第 3 次检测成功率对检测方案的效果进行评估。算法仿真结果如图 2 所示。

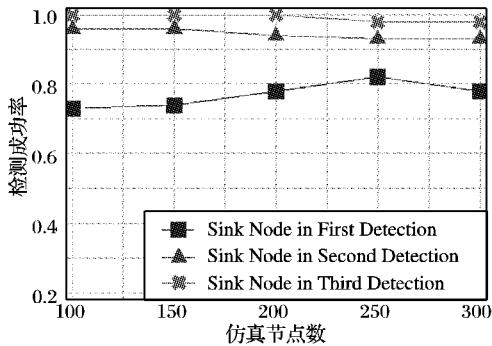


图2 汇聚节点检测成功率

### 3.5.1 算法有效性分析

曲线1表示首次测定假冒源的成功率,随着网络密度的增大,潜在恶意节点集合为一元集的概率也在增大,所以首次测定成功率随节点数的增加而上升。总体上首次能够检测出假冒源的概率为77%,第2次能够测定出假冒源的概率为95%,第3次能够测定出假冒源的概率为99%。所以汇聚节点最多通过3次检测就可以定位出恶意节点。在成功假冒源测定过程中,由于仅恶意节点的邻居节点进行签名与验证签名操作,所以签名与验证签名操作次数较少,总体平均首次测定假冒源的签名与验证签名操作次数仅为19.12,因此该算法能够有效检测出成功假冒源。

### 3.5.2 算法复杂度分析

假设单个恶意节点平均邻居数为n,由于报警消息由汇聚节点签名发出,只有恶意节点的邻居节点才会验证签名,所以首次测定需要的平均操作次数约为n+1。根据该算法有效性分析,最多3次就可检测出恶意节点,因此最大平均操作次数约为3(n+1),因此可推出该算法平均时间复杂度为O(n),算法可在多项式时间内完成。

## 4 结语

传感器网络中恶意节点假冒攻击严重影响节点间协同工作的效果,破坏网络路由机制。目前,还没有针对局部区域内存在多个假冒源和成功假冒源检测方案的研究工作。本文通过采用基于身份的签名技术,提出了一种新的假冒攻击源检测方案。构造了单个试图假冒攻击源测定算法,并扩充为针对局部区域内多个试图假冒攻击源测定算法。针对成功假冒

(上接第2090页)

## 5 结语

实验证明,本文提出的算法在特征匹配中感知编组,在感知编组中特征匹配,将特征匹配和感知编组有机地结合在一起,既提高了匹配成功的线特征的数量,又增加自由形状线特征的长度,方便了后续人工地物(如建筑物)的提取。

同时,从匹配结果也可以看出,线特征匹配的精度还不够高,如何将自由形状线特征匹配与最小二乘匹配等高精度的匹配方法相结合,进一步提高特征匹配的精度是今后需要进一步研究的问题。

### 参考文献:

- [1] 范永弘. 立体影像匹配和DTM自动生成技术的研究与实践 [D]. 郑州:信息工程大学, 2000.
- [2] MEDIONI G, NEVIATIA R. Matching images using linear features

攻击的情况,该方案也提出了成功假冒攻击源的测定算法。通过仿真验证了检测方案的有效性,该检测方案适用于假冒攻击状况复杂,网络安全性要求较高的环境。

但是,在试图假冒攻击源检测过程中,平均签名与验证签名操作次数会随着网络密度的增加而增大,如何选取合适网络密度,使得在签名与验证签名操作次数有效减少的情况下取得较高的成功检测率,仍然需要进一步的研究。

### 参考文献:

- [1] 孙利民, 李建中, 陈渝, 等. 无线传感器网络 [M]. 北京: 清华大学出版社, 2005.
- [2] 曹晓梅, 俞波, 陈贵海, 等. 传感器网络节点定位系统安全性分析 [J]. 软件学报, 2008, 19(4): 879–887.
- [3] BHUSE V, GUPTA A, AL-FUQAH A. Detection of masquerade attacks on wireless sensor networks [C]// Proceedings of the IEEE International Conference of Communications. Washington, DC: IEEE, 2007: 1142–1147.
- [4] KRONTIRIS I, DIMITRIOU T, GIANNETSOS T, et al. Intrusion detection of sinkhole attacks in wireless sensor networks [C]// Proceedings of the 3rd international conference on Algorithmic aspects of wireless sensor networks. Berlin: Springer-Verlag, 2007: 150–161.
- [5] 谢磊, 王惠斌, 祝跃飞, 等. 一种传感器网络假冒攻击源的测定方法 [J]. 计算机科学, 2009, 36(6): 68–71.
- [6] SHAMIR A. Identity-based cryptosystem and signature scheme [C]// Proceedings of CRYPTO 84 on Advances in cryptology. Berlin: Springer-Verlag, 1985: 47–53.
- [7] SAKAI R, OHGISHI K, KASAHARA M. Cryptesystems based on paring [C]// Proceedings of Symposium on Cryptography and Information Security. Japan: [s. n. ]. 2000: 26–28.
- [8] CHA J C, CHEON J H. An identity-based signature from gap diffie-hellman groups [C]// Proceedings of Public Key Cryptography — PKC 2003. Berlin: Springer, 2003: 18–30.
- [9] BARRETO P, HBERT B, MCCULLAGH N, et al. Efficient and provably secure identity-based signature and signcryption from bilinear maps [C]// Advance in Cryptology — ASIACRYPT 2005. Berlin: Springer, 2005: 515–532.
- [10] WATERS R. Efficient identity based encryption without random oracles [C]// Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2005: 114–127.
- [11] JOUX A. A one round protocol for tripartite diffie-hellman [J]. Journal of Cryptology, 2004, 17(4): 263–276.

- [J]. IEEE Transactions on Pattern Recognition and Machine Intelligence, 1984, 6(6): 675–685.
- [3] TOTH K C, SCHENK T. Feature-based matching for automatic image registration [J]. ITC Journal, 1992, (1): 40–46.
- [4] RIGNOT E, KOWK R, CURLANDER J, et al. Automated multi-sensor registration: Requirements and techniques [EB/OL]. [2009–12–10]. <http://rkwok.jpl.nasa.gov/publications/kwok.1991.Automated.pdf>.
- [5] 郭海涛. 一种基于自由形状线特征的影像匹配方法 [J]. 测绘通报, 2009, (1): 21–24.
- [6] 董鸿燕, 沈振康, 罗军, 等. 感知编组综述 [J]. 计算机工程与应用, 2007, 43(14): 9–13.
- [7] 徐胜华. 面向立体影像特征匹配的直线提取方法 [D]. 武汉: 武汉大学, 2007: 75–77.
- [8] PALMER S. Common region: A new principle of perceptual grouping [J]. Cognitive Psychology, 1992, 24(3): 436–447.