一种传感器网络假冒攻击源的测定方法

谢 磊[1,2] 王惠斌[1,3] 祝跃飞[1] 徐勇军[2]
(信息工程大学信息工程学院 郑州 450002)[1] (中国科学院计算技术研究所 北京 100190)[2]
(河南司法警官职业学院 郑州 450002)[3]

摘 要 传感器网络中的假冒攻击是一种主动攻击形式,它极大地威胁传感器节点间的协同工作。提出了基于邻居协同测定假冒攻击源算法(CNAMDI)。在CNAMDI算法中,节点根据主动报警规则和从动报警规则发现假冒行为,基于义务测定集传递规则的邻居协同实现对假冒攻击源的测定。CNAMDI算法无需全网拓扑信息及路由协议支撑,测定过程不借助密码算法。通过分析得出,当局部网络密度较高时,CNAMDI算法具有漏报率低、成功测定率高的特点。仿真分析表明,对比朴素算法,CNAMDI算法使漏报率平均降低了25.8%,成功测定率平均提高了45.5%,平均发包数仅增加了1.19个。

关键词 传感器网络,邻居协同,假冒攻击
中图法分类号 TP393.08 **文献标识码** A

Masquerader Detection and Identification Approach in Sensor Networks

XIE Lei[1,2] WANG Hui-bin[1,3] ZHU Yue-fei[1] XU Yong-jun[2]
(Information Engineering Institute, Information Engineering University, Zhengzhou 450002, China)[1]
(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China)[2]
(Henan Judicial Police Vocational College, Zhengzhou 450002, China)[3]

Abstract Masquerade attack is one of active attack forms in sensor networks, which will be a serious threat to the synergies among sensor nodes. A collaborative neighbor based algorithm for masquerader detection and identification (CNAMDI) was proposed. In CNAMDI algorithm, nodes can use initiative or slave alarm rules to detect a masquerade attack and can identify the masquerader based on collaborative neighbor with volunteer rule of suspect set forwarding. CNAMDI algorithm can work without the need of any underlying routing protocols and global topology information, and the identification process does not rely on any cryptographic algorithms. Theoretical analysis shows that, when higher density in local area networks, this algorithm has a property of low leak rate and high success identification rate. Simulation analysis shows that, compared with simplicity algorithm, CNAMDI algorithm reduces averagely 25.8% leak rate and improves averagely 45.5% success identification rate with only introducing additional 1.19 sending packets per neighbor.

Keywords Sensor networks, Collaborative neighbor, Masquerade attack

1 引言

传感器网络[1]多部署于非受控区域,无线信道的广播特性、多跳自组织的组网特征、节点间协同信任的工作特性以及节点资源极度受限这一固有的网络脆弱性都使其极易受到各种安全威胁[2]。和传统网络一样,安全威胁主要来自恶意攻击[3,4]。传感器网络中的假冒攻击[5]是一种主动攻击形式,表现为攻击者发送假冒消息扰乱网络协议的运行。因此,这种攻击会极大地影响节点间协同工作的效果。

到目前为止,就我们所知,传感器网络中针对假冒攻击检测的研究还较少。Bhuse等人[5]首先对传感器网络中假冒攻击的检测进行研究,提出了MG和SRP两种检测方案。MG方案基于邻居间相互保护机制来发现假冒异常;SRP方案依赖节点收发包计数校验来检测假冒攻击。然而这两种方案均不能定位发起假冒攻击的源节点。Krontiris等人[6]在研究Sinkhole攻击[3]的检测中注意到攻击者可以通过假冒攻击伪造路由更新包,并基于局部包检测明确提出了触发局部假冒攻击警报的两条规则:即(1)确保没有攻击者假冒自己发送路由更新包,(2)确保没有攻击者假冒邻居发送路由更新包。由于节点本身不能算是自己的邻居,上面规则(2)实际上包括了规则(1),本文后面也称规则(2)为基本报警规则。文献[6]进一步指出,由于报警节点可以确定攻击者必定是自己的邻居。这样,如果一个Sinkhole攻击的发生可以触发多个节点报警,攻击者应该在这些节点的邻居表交集中。如果该交集只含一

到稿日期:2008-07-22 返修日期:2008-11-10 本文受国家863计划(2006AA01Z223, 2006AA01Z225)和国家自然科学基金(60772070)资助。
谢 磊(1973-),男,博士生,研究方向为信息安全等,E-mail:x_lei@126.com;王惠斌(1964-),男,副教授,研究方向为信息安全等;祝跃飞(1962-),男,教授,博士生导师,研究方向为密码学和信息安全等;徐勇军(1979-),男,博士,助研,研究方向为传感器网络等。

个节点，则该节点就是攻击者。

基于 Krontiris 等人的假冒攻击源测定思想，本文提出了基于邻居协同测定假冒攻击源算法(Collaborative Neighbors based Algorithm for Masquerader Detection and Identification，CNAMDI)。相比朴素的 Krontiris 算法，CNAMDI 算法具有漏报率低、成功测定率高的特点，是一种轻量级分布式的高效检测算法。

2 模型假设与术语

本文假定的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。同时假设，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。

定义 1 当两个节点之间的距离 $r \leqslant R$ 时，它们可直接通信，互为邻居；距离较远的节点间需借助邻居转发进行多跳通信，节点间最短链路的长度称为节点间的距离矢量(即跳数)。并且任一节点 i 的邻居集是指那些在二维平面上与该节点的距离不大于 R 的所有节点的集合，记为 $Nr(i)$。

定义 2 有限集 S 中元素的个数称为集合 S 的基数，用 card(S)表示。若 card(S)=1，称集合 S 为一元集。

根据前述传感器节点的撒布假设可知，节点 i 的邻居数期望为：$E(\text{card}(Nr(i)))=k-1$。

由于传感器网络常常是为一个组织或集团服务的，故假设在网络部署阶段，每个节点是可信的，均可获得自己的邻居集，并在网络更新过程中能及时更新自己的邻居集。在网络工作阶段，部分节点可能被攻击者捕获，成为恶意节点。恶意节点可针对特定的网络任务发起假冒攻击，其发出的假冒消息可以被该恶意节点的邻居监听到。相应地，当任一节点监听到一条假冒消息，即可断定一次假冒攻击发生，且攻击源是其邻居。考虑到恶意节点增大功率发送假冒消息只会使更大范围的节点监听到该消息而容易被察觉，故假设恶意节点不改变原节点发射功率。

若设一次假冒攻击中，攻击源所发出的消息为 M，可以定义如下术语：

定义 3 若已检测到 M 是假冒消息，节点 i 怀疑的攻击源节点集称为 i 对 M 的攻击源测定集或测定集，记为 $S_{\text{suspect}}(i,M)$。当 $S_{\text{suspect}}(i,M)$为一元集时，称 i 成功测定 M 的攻击源。

定义 4 一次假冒攻击的漏报率是指，监听到 M 但未报警的节点数同收到 M 的节点数之比，记为 $P_{\text{miss}}(M)$。

定义 5 一次假冒攻击的成功测定率是指，成功测定 M 的攻击源的节点数同收到 M 节点数之比，记为 $P_{\text{success}}(M)$。

为简化问题，本文假设局部范围内同一时刻仅发生一次假冒攻击，故除特殊说明，上述标记中 M 可缺省。

3 朴素的假冒攻击源测定算法

基于 Krontiris 等人的测定思想，我们设计了朴素的假冒攻击源测定算法，简称为 Krontiris 算法。其测定假冒攻击源的过程包括两个阶段，即报警和求交测定集。

在报警阶段，依据基本报警规则，每当监听到邻居发出的消息 M，节点 i 将检查 M 的源 id，若源 $id \notin Nr(i)$，表明发送者和所申明的源 id 不一致，可以肯定假冒攻击发生，节点 i 即可认定 M 为假冒消息，且假冒攻击源就是自己的邻居之一，因此令 $S_{\text{suspect}}(i)=Nr(i)$，报警并广播 $S_{\text{suspect}}(i)$。

在求交测定集阶段，每当收到邻居 j 广播的报警消息 $S_{\text{suspect}}(j)$，节点 i 若认定 M 为假冒消息，可求交以缩小测定集，即 $S_{\text{suspect}}(i)=S_{\text{suspect}}(i)\cap S_{\text{suspect}}(j)$；当 $\text{card}(S_{\text{suspect}}(i))=1$ 时，i 成功测定 M 的攻击源。

图 1 所示拓扑中，依据基本报警规则，节点 4,5,7 可以检测出消息 M 是假冒的，并且有：$S_{\text{suspect}}(4)=\{1,3,5,6\}$，$S_{\text{suspect}}(5)=\{4,6,7,8\}$，$S_{\text{suspect}}(7)=\{5,6,8\}$。经求交测定集可得：$S_{\text{suspect}}(4)=\{6\}$，$S_{\text{suspect}}(5)=\{6\}$，$S_{\text{suspect}}(7)=\{6,8\}$。不难发现，接收消息 M 的节点 1 不会报警，节点 7 不能测定攻击者。因此，图 1 实例中，Krontiris 算法的 $P_{\text{miss}}=25\%$，$P_{\text{success}}=50\%$。

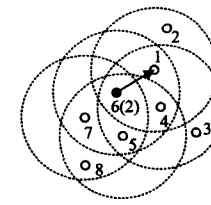

图 1 节点 6 假冒 2 给 1 发消息 M

4 CNAMDI 算法

下面首先分析图 1 实例中 Krontiris 算法出现漏报和不能测定问题的原因。

由于节点 1,2 恰好是邻居，因此收到节点 2 发出的消息 M 并不违背基本报警规则，所以节点 1 漏报了。这是一个致命的漏报，因为假冒消息的直接受害者就是接收者。实际上，节点 4 的报警已经包含有可能是节点{1,3,5,6}假冒了消息 M 的信息。节点 1 收到该报警后，基于邻居间的协同信任关系，可知 M 是假冒的，由此确定 $S_{\text{suspect}}(1)=S_{\text{suspect}}(4)\cap Nr(1)=\{6\}$。因此，节点 1 可成功测定节点 6 为攻击源。

一般地，若在收到邻居 j 广播的报警消息 $S_{\text{suspect}}(j)$前，节点 i 已经收到了 M。由于邻居间的协同信任关系，节点 i 信任 j，即认定 M 为假冒消息，并可确定 $S_{\text{suspect}}(i)=Nr(i)\cap S_{\text{suspect}}(j)$。然后节点 i 也向邻居报警并广播 $S_{\text{suspect}}(i)$。

为区别，我们称依基本报警规则产生的报警为主动报警，相应的节点为主动报警节点。这样因信任邻居报警信息而产生报警的节点称为从动报警节点，其报警为从动报警。因此，上面这条规则也称为从动报警规则。

类似地，针对节点 7 不能测定攻击者而其邻居 5 可以测定的情况，可增加一条测定集传递规则：报警节点有义务向邻居广播自己的测定集，以传递攻击源测定信息。这样，节点 7 从 5 处收到 $S_{\text{suspect}}(5)=\{6\}$后可排除节点 8，从而测定节点 6 为攻击源。

基于上述两条规则的改进，我们设计的 CNAMDI 算法如表 1 所列。

表 1 CNAMDI 算法(运行在节点 i 上)

```
①确定测定集
If (接收到 j 发送的 M) then
    If ! (j∈Nr(i)) then //发送者不是邻居
        Allocate(Ssuspect(i)); //分配测定集空间
        Ssuspect(i)= Nr(i);
    End if
End if
```

```
If (接收到 j 广播的报警消息(M,Ssuspect(j))) then
    If (Ssuspect(i)为空且已收到消息 M ) then
        Allocate(Ssuspect(i));
        Ssuspect(i)= Nr(i);
    End if
    If (Ssuspect(i)不为空) then
        Ssuspect(i) = Ssuspect(i) ∩Ssuspect(j);
        If(card(Ssuspect(i))==1) then
            假冒者被测定,即集合中的元素;
        End if
    End if
End if
```

```
②测定集传递
启动定时器 Timer1 和 Timer2;
While(Timer1 超时且 Ssuspect(i)有变化)do
    随机选择发送窗口广播(M,Ssuspect(i));
    If(Timer2 超时)then break; End if
    Restartup Timer1;
End while
```

可见,对于单个传感器节点而言,算法不涉及复杂的密码算法运算,每遭受一次假冒攻击,CNAMDI 算法中测定集的确定非常简单,最坏情况下需要遍历邻居表以确认发送者 j 不是邻居。由于 $E(\mathrm{card}(Nr(i)))=k-1$,因此其时间复杂度为 $O(k)$。在空间复杂度方面,每个节点存储自己的邻居集,每个报警节点的测定集不大于其邻居集。因此其空间复杂度也为 $O(k)$,并且在测定结束后可回收测定集空间。CNAMDI 算法中测定集传递决定通信开销。通过设置适当的 Timer1 和 Timer2,每个报警节点非频繁地发送报警包,并且由于不需转发报警包,故没有泛洪危险。后面的仿真实验表明,攻击源的邻居平均发包数低于 2 个。由此可见,CNAMDI 算法是一种轻量级测定算法,适于在资源受限的传感器节点上实现。

5 CNAMDI 算法安全性分析

本节我们用漏报率刻画 CNAMDI 算法对假冒攻击行为的检测效率,用成功测定率刻画 CNAMDI 算法对攻击源的确定效率。概率分析表明,CNAMDI 算法能降低漏报率,提升成功测定率。

为便于描述,不妨设 A 假冒 b 发送消息 M。根据 $Nr(A)$ 中节点报警与否可将其分为三类,即主动报警节点集 S_{active}、从动报警节点集 S_{slave} 和漏报警节点集 S_{miss}。依 A 和 b 间的距离矢量可以定量表示 S_{active},S_{slave} 和 S_{miss},如表 2 所列。由此可见,仅当 b 为 A 的 2 跳节点时,CNAMDI 算法才会产生漏报现象。

表 2 依 A 和 b 间的距离矢量,定量表示 S_{active},S_{slave} 和 S_{miss}

Nr(A)分类	A 和 b 间的距离矢量		
	1 跳(即邻居)	2 跳	>2 跳
S_{active}	Nr(A)−Nr(b)	Nr(A)−Nr(b)	Nr(A)
S_{slave}	Nr(A)∩Nr(b)	$S_{\mathrm{slave}}+=\left\{ i \left\| \begin{array}{c} i\in Nr(A)\cap Nr(b) \\ \text{and} \\ Set\neq\phi \end{array} \right. \right\}$	∅
S_{miss}	∅	$S_{\mathrm{miss}}=\left\{ i \left\| \begin{array}{c} i\in Nr(A)\cap Nr(b) \\ \text{and} \\ Set=\phi \end{array} \right. \right\}$	∅

注:$Set=(S_{\mathrm{active}}\cup S_{\mathrm{slave}})\cap Nr(i)$

由前述定义,P_{miss} 和 P_{success} 可如下计算:

$$P_{\mathrm{miss}}=\mathrm{card}(S_{\mathrm{miss}})/\mathrm{card}(Nr(A)) \tag{1}$$

$$P_{\mathrm{success}}=\mathrm{card}(S_{\mathrm{success}})/\mathrm{card}(Nr(A)) \tag{2}$$

这里 S_{success} 表示成功测定攻击源的节点集,即:

$$S_{\mathrm{success}}=\left\{ i \left\| \begin{array}{c} i\in S_{\mathrm{active}}\cup S_{\mathrm{slave}} \\ \text{and} \\ \mathrm{card}(S_{\mathrm{suspect}}(i))=1 \end{array} \right. \right\} \tag{3}$$

网络正常运行期间,只要网络设计功能没有大的变动,$\mathrm{card}(Nr(A))$ 基本不会改变(节点的新老更替量是平衡的)。从式(1)可知,若 $\mathrm{card}(S_{\mathrm{miss}})$ 小,则 P_{miss} 低。并且 $\mathrm{card}(S_{\mathrm{miss}})$ 小则 $\mathrm{card}(S_{\mathrm{active}}\cup S_{\mathrm{slave}})$ 大,同时若 $i\in(S_{\mathrm{active}}\cup S_{\mathrm{slave}})$ 时 $S_{\mathrm{suspect}}(i)$ 为一元集的概率较高,则 $\mathrm{card}(S_{\mathrm{success}})$ 大,由式(2)可得较高的 P_{success}。

下面,我们首先将分析存在节点 $v\in S_{\mathrm{miss}}$ 的概率小而推导出 $\mathrm{card}(S_{\mathrm{miss}})$ 小,然后分析报警节点 i 的 $S_{\mathrm{suspect}}(i)$ 为一元集的可能性较高。

若将邻居间建立的直接互连通信链路看成边,传感器网络的拓扑结构可看成一个无向 UDG 图[7]。这样,在 CNAMDI 算法中,当攻击者 A 假冒节点 b 发送消息 M 时,我们考察在传感器网络拓扑图中由 $Nr(A)$ 导出的导出子图 $G_{Nr(A)}=\langle Nr(A),E_{Nr(A)}\rangle$,可给出如下定理:

定理 1 在部署密度较高的传感器网络中,$G_{Nr(A)}$ 将以较大概率连通。

证明:在二维平面上随机均匀撒布,密度为 λ 的传感器网络中,由独立性条件可知,任一节点是否在某区域内,只取决于该区域面积 Δ 的大小,而与区域形状及位置无关。并且节点 v 落入区域 Δ 的概率满足[8]:

$$P\{\exists v,v\in\Delta\}=1-e^{-\lambda\Delta} \tag{4}$$

这里由前述假设节点通信半径 R 及节点通信覆盖面积内的节点数期望 k 可知 $\lambda=k/\pi R^2$。

若 $G_{Nr(A)}$ 不是一个连通图,则必存在一个连通分支 C,其所有节点均位于中心节点 A 的同一侧,且存在节点 u 是 C 中离中心点 A 最近一侧的凸边界节点,如图 2 所示,使得扇形域 S_{bud} 和 S_{cud} 中没有属于连通分支 C 的节点存在。这里设事件 B 表示存在节点 v 落入扇形域 S_{bud} 和 S_{cud} 中(由于在二维平面中落在某直线或曲线上的概率为 0,故可排除节点 $v=A$ 的情况),则 $\alpha\geqslant\pi/3$,由式(4),在 $u\in Nr(A)$ 条件下,扇形域 S_{bud} 和 S_{cud} 中存在节点 v 的概率满足:

$$P\{B\mid u\in Nr(A)\}=(1-e^{-2\lambda S_{\mathrm{bud}}})/(1-e^{-\lambda\pi R^2})\geqslant (1-e^{-\frac{k}{3}})/(1-e^{-k}) \tag{5}$$

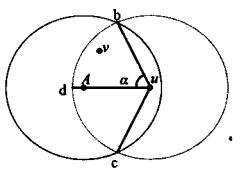

图 2 节点 v 落入 u 旁扇形域中

图 3 中用圆圈线标注了式(5)的下界概率曲线。可以看出,当 $k>5$ 时,节点 v 落入扇形域 S_{bud} 和 S_{cud} 中的概率大于 80%。换句话说,节点 v 能以较大概率成为节点 u 的邻居,从而使连通分支 C 增大直至 $G_{Nr(A)}$ 全连通。证毕。

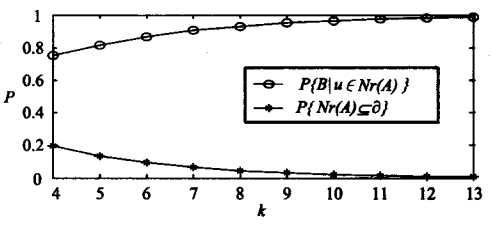

图 3 两条概率曲线

定理 2 若 $G_{Nr(A)}$ 全连通，$Nr(A)$ 中所有节点最终对 M 是否是假冒消息的判断结果是一致的；若都报警，其最终测定集相同。

证明：(1)假设 $Nr(A)$ 中的节点最终对 M 是否是假冒消息的判断结果不一致。不妨设 $i,j\in Nr(A)$，i 对消息 M 不报警，j 是离 i 最近的对 M 报警的节点，则 $G_{Nr(A)}$ 中必然存在一条从 j 到 i 的路径 $j,j_1,\cdots,j_n,i$，路径中相邻两点互为邻居，并且 $j_1,\cdots,j_n$ 均能收到消息 M，但对消息 M 均不报警。然而根据从动报警规则，当 j 报警时，由于 $j_1\in Nr(j)$，j_1 会从动报警，依此类推，i 必将从动报警。这与假设矛盾，因此 $Nr(A)$ 中所有节点最终对 M 是否是假冒消息的判断结果是一致的。

(2)同理假设 $Nr(A)$ 中报警节点最终测定集不同，则必有路径 $j,j_1,\cdots,j_n,i$，其中存在节点 $u\in S_{suspect}(i)$，但 $u\notin S_{suspect}(j)$。根据测定集传递规则，同一连通分支的所有报警节点都应广播自己的测定集。这样在路径中当 j_1 收到 $S_{suspect}(j)$ 并求交测定集后必有 $u\notin S_{suspect}(j_1)$，依此类推，必得 $u\notin S_{suspect}(i)$。这与假设矛盾，因此，所有报警节点最终测定集相同。证毕。

定理 3 当 $G_{Nr(A)}$ 全连通时，若存在节点 $i\in Nr(A)$ 最终未报警，则必有 $Nr(A)\subseteq Nr(b)$。

证明：由于节点 $i\in Nr(A)$ 最终未报警且 $G_{Nr(A)}$ 全连通，根据定理 2 可知，$Nr(A)$ 中任意节点 j 均不报警。由此，根据基本报警规则必有 $j\in Nr(b)$，所以 $Nr(A)\subseteq Nr(b)$。证毕。

定理 3 表明，当 $G_{Nr(A)}$ 全连通时，若存在漏报节点，则 $Nr(A)$ 中所有节点均需落入节点 A 和 b 通信可达的公共区域中，如图 4 所示。令 ∂ 表示该公共区域，令 Δ 表示 A 可达 b 不可达的区域，那么它们的面积分别表示为：

$$\partial=2R^2\cos^{-1}\left(\frac{r}{2R}\right)-r\sqrt{R^2-\left(\frac{r}{2}\right)^2}\quad (R<r<2R) \tag{6}$$

$$\Delta=\pi R^2-\partial>(\pi-2\cos^{-1}(\frac{1}{2})+\frac{\sqrt{3}}{2})R^2 \tag{7}$$

根据式(4)、(6)和(7)，$Nr(A)$ 中所有节点均落入区域 ∂ 的概率为：

$$P\{Nr(A)\subseteq\partial\}=1-P\{\exists v,v\in\Delta|v\in Nr(A)\}=1-(1-e^{-\lambda\Delta})/(1-e^{-\lambda\pi R^2})<(e^{-k/\pi*(2\cos^{-1}(1/2)-\sqrt{3}/2)}-e^{-k})/(1-e^{-k}) \tag{8}$$

图 3 中星点线标注了式(8)的上界概率曲线，可以看出，当 $k>5$ 时，当 $G_{Nr(A)}$ 全连通时，存在漏报节点的概率小于 15%。由此，我们认为存在节点 $v\in S_{miss}$ 的概率小而推导出 $\mathrm{card}(S_{miss})$ 小。

图 5 中，以点 A 为圆心，分别以 $R/\sqrt{k}$，$R-R/\sqrt{k}$，R 为半径作 3 个同心圆，可将节点 A 通信可达区划分为 3 个区域，面积分别为 $\pi R^2/k$，$\pi R^2(1-2/\sqrt{k})$，$(2\sqrt{k}-1)\pi R^2/k$。由节点均匀分布且密度 $\lambda=k/\pi R^2$，所以落入每块区域的节点数期望分别为：1，$k-2\sqrt{k}$，$2\sqrt{k}-1$。

当 $k>5$ 时，区域 3 中的节点数期望超过 3 个，并随节点邻居数期望而增加。而区域 3 中的节点同样服从均匀分布，如图 5 中点 a,b,c，不难得出超过 3 个节点的交集区域面积不会比区域 1 大，因此，$G_{Nr(A)}$ 中节点的邻居集交集中很大可能只有 1 个节点，即节点 A。

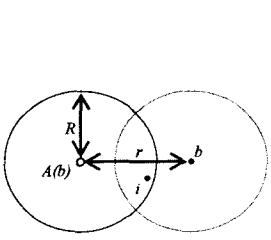

图 4 A 假冒 b，$i\in$Nr(A)落入公共区域

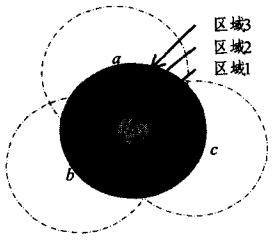

图 5 节点 A 通信可达区域划分

当 $G_{Nr(A)}$ 为连通图时，若任意节点 $i\in Nr(A)$ 均报警，由定理 2，图 5 中区域 1，2 中的节点和区域 3 中节点的测定集结果相同，因此，$S_{suspect}(i)$ 为一元集的可能性也很大。

6 实验和结果分析

我们在 100 * 100 的区域内，以二维均匀分布随机撒布 500 个传感器节点。每次仿真随机选择一个恶意节点实施假冒攻击。按照 Krontiris 算法和 CNAMDI 算法两种策略、攻击源与假冒对象的 3 种距离矢量关系共进行 6 轮实验，每轮进行 10000 次仿真，每轮实验后按攻击者的邻居数($k-1$)分类统计，样本数分布如图 6(a)所示。实验中我们取样本数大于 500(即 $4\leqslant k\leqslant 13$)的仿真进行统计分析。

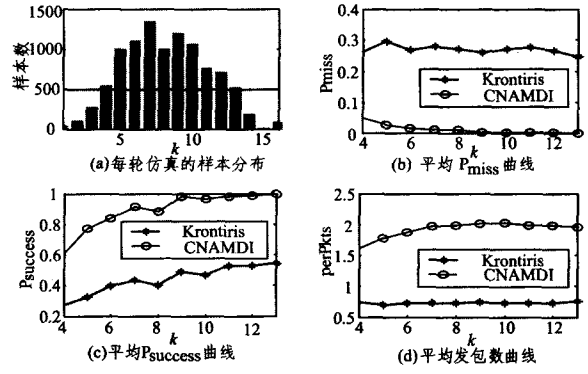

图 6 样本数大于 500 时，两种算法的 3 个指标曲线对比情况

图 6(b)、(c)、(d)直观表现了随着 k 的变化，Krontiris 和 CNAMDI 两种算法在 3 种性能指标下平均性态的对比情况。可以看到，后者比前者在 P_{miss} 和 $P_{success}$ 两指标上取得的显著效果，图示区间中，P_{miss} 平均降低了 25.8%，$P_{success}$ 平均提高了 45.5%。在通信开销方面，后者也保持了轻量的表现，平均发包数比前者增加了 1.19 个，仅为 1.92 个。需要说明的是，Krontiris 算法中攻击者和假冒对象的公共邻居没有从动报警而产生漏报，由于公共节点占攻击者邻居的比例只与它们之间的距离 r 有关，而与网络密度无关，因此图 6(b)中该算法的 P_{miss} 的走势和 k 关系不明显，但随之 k 的增大，报警节点总量会随之增加，图 6(c)中相应的 $P_{success}$ 会表现出增大的趋势。总体上，随着 k 的增大，攻击者 A 的邻居数增多，CNAMDI 算法中参与报警和测定集求交的节点数增多，P_{miss} 下降趋势和 $P_{success}$ 上升趋势明显，当 $k>8$ 时，$P_{success}>96.5\%$，$P_{miss}<5.3\%$。

结束语 传感器网络中的假冒身份攻击会极大地威胁节点间的协同工作效果。目前，这方面的研究工作开展较少。本文提出的 CNAMDI 算法不仅具有良好的假冒攻击源测定

(下转第 124 页)

数据()，由客观情况构建需求数据()}，接下来再观察它的执行结果。接下来如果观察到实际执行结果为：{获得大量的直接需求数据}，则根据 ControlTree 知：再下一步需要执行的过程活动集为{从大量需求中提取出合理的需求()}，执行完这一活动集后即可实现目标要求。

结束语 本文提出了一种过程活动流实时规划算法，以对过程活动流的安排做出实时自动规划。可以对过程活动执行中出现的各种可预见的实际效果做出实时反应，使软件开发始终处于有序的过程活动控制之中，并取得既定目标。试验表明，所产生的规划有助于减少软件开发中过程活动安排的盲目性，提高执行每个过程活动时的全局意识。另外过程活动常常会出现重复执行或者多次执行，已有的一些相关规划工作[13-15]都没有谈及如何解决这个问题，本文提出的实时规划算法较好地解决了该问题，如果有可能再次执行某过程活动，则该过程活动的前提条件一定会被产生，将这些前提命题加入到能够实时地产生它们的那些相应动作的实时情形集中即可。

但本文也存在一些不足之处，项目的软件过程要考虑时间、成本和资源的约束，这些都是很重要的因素，本文暂时还没有加入这些因素。这些方面的解决可以考虑通过引入时序约束和条件约束的方法，这些方面将作进一步的深入研究。

参 考 文 献

[1] Li Mingshu, Boehm B W, Leon J. Osterweil. Unifying the Software Process Spectrum [J]. Journal of Software, 2006, 17(4): 649-657

[2] Fuggetta A. Software process: A roadmap. The Future of Software Engineering[C]// 22nd International Conference on Software Engineering. ACM Press, 2000: 25-34

[3] Boehm B. The Future of Software Processes. Keynote Address [C]// SPW2005. Beijing, May 25, 2005

[4] Blum A, Furst M. Fast planning through planning graph analysis[J]. Artificial Intelligence, 1997, 90: 281-300

[5] 赵欣培，李明树，陈振冲，等. 一种基于协商的软件过程协同方法[J]. 计算机研究与发展，2006，43(2)：314-320

[6] 李健，金茂忠. 有效改善软件过程方法研究[J]. 计算机研究与发展，2001，38(1)：26-35

[7] 黄罡，梅宏，杨芙清. 基于反射式软件中间件的运行时软件体系结构[J]. 中国科学 E 辑，2004，34(2)：121-138

[8] 吕建，陶先平，马晓星，等. 基于 Agent 的网构软件模型研究[J]. 中国科学 E 辑，2005，35(12)：1233-1253

[9] 吕建，徐家福. 软件自动化的智能化途径[J]. 科学通报，1993，38(2)：184-185

[10] 柳军飞，唐稚松. 软件过程建模语言研究[J]. 软件学报，1996，7(8)：449-457

[11] 王青，李明树，刘霞. 一种支持软件过程控制和改进的主动度量模型[J]. 软件学报，2005，16(3)：407-418

[12] 袁峰，李明树. 基于 MDA 的 TRISO-Model 模型管理方法及应用[J]. 软件学报，2007，18(7)：1612-1635

[13] Jasper H. Active databases for active repositories [C]// Proc. 10th International Conference on Data Engineering. Houstong. IEEE Computer Society Press, Feb. 1994: 375-384

[14] Al-Emran A, Pfahl D, Ruhe G. DynaReP: A Discrete Event Simulation Model for Re-planning of Software Releases [C]// ICSP2007. Minneapolis, USA: 246-258

[15] Gupta M, Bastani F, Khan L, et al. Automated test data generation using MEA-Graph Planning [C]// Proc. of the 16th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'04). Boca Raton, Florida (USA), 2004: 174-182

(上接第 71 页)

效果，而且其时空复杂度仅为 $O(k)$，通信开销方面平均发包数低于 2 个。因此，它适于在资源受限的传感器节点上实现。

虽然基于特定消息的报警处理有利于区分两次不同的假冒行为，但在同一局部区域同时测定多个假冒行为甚至假冒报警行为仍然需要进一步研究，这将是我们今后需要解决的问题。

参 考 文 献

[1] Akyildiz I F, Weilian S, Sankarasubramaniam Y, et al. A Survey on Sensor Networks[J]. IEEE Communications, 2002, 40(8): 102-114

[2] 郎为民，杨宗凯，吴世忠，等. 无线传感器网络安全研究[J]. 计算机科学，2005，32(5)：54-58

[3] Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures[J]. Ad Hoc Networks, 2003, 1(1): 293-315

[4] 曹晓梅，何欣，陈贵海. 传感器节点定位系统攻防机制研究[J]. 计算机科学，2008，35(7)：36-41

[5] Bhuse V, Gupta A, Al-Fuqaha A. Detection of Masquerade Attacks on Wireless Sensor Networks[C]// Proceedings of the IEEE International Conference of Communications (ICC '07). June 2007: 1142-1147

[6] Krontiris I, Dimitriou T, Giannetsos T, et al. Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks[C]// ALGOSENSORS 2007, LNCS 4837. 2008: 150-161

[7] Clark B N, Colbourn C J, Johnson D S. Unit Disk Graphs[J]. Discrete Math., 1990, 86: 165-177

[8] 路纲，等. 无线网络邻近图综述[J]. 软件学报，2008，19(4)：888-911