无线传感器网络中的 sinkhole 攻击检测

周玲玲[1],张建明[1],王良民[1,2]
ZHOU Ling-ling[1],ZHANG Jian-ming[1],WANG Liang-min[1,2]

1.江苏大学 计算机科学与通信工程学院,江苏 镇江 212013
2 东南大学 计算机科学与工程学院,南京 210019
1.School of Computer Science and Communication Engineering,Jiangsu University,Zhenjiang,Jiangsu 212013,China
2.School of Computer Science and Engineering,Southeast University,Nanjing 210019,China
E-mail:zlllmm@163.com

ZHOU Ling-ling,ZHANG Jian-ming,WANG Liang-min.Research on sinkhole attack detection in wireless sensor networks.Computer Engineering and Applications,2008,44(22):135-138.

Abstract: To study sinkhole attack,a light-weight method based on multipoint monitoring and acknowledge information is proposed.Through the transmission and acknowledgement of packets between base station and sensor nodes,combined with multipoint monitoring,the author makes the statistical analysis of the packets sent and received to detect the sinkhole attack.The method avoids from complicated encryption and identity certification proposed in some other methods.By comparison,the reliability of the method is relatively higher than that of multipath security mechanism .The author also examines the security probability of the method using both theoretical analysis and simulations.

Key words: wireless sensor networks;intrusion detection;sinkhole attack;multipoint monitoring

摘 要:对 sinkhole 攻击进行了研究,提出了基于多点监测与回复信息的攻击检测方法。利用基站和节点间数据包的传输与确认,结合邻节点的监视机制对节点收发的数据包统计分析,检测 sinkhole 攻击。这种方法避免了复杂的加密算法与身份认证,与多路径安全机制相比有着更高的可靠性。对安全概率进行了理论分析,并进一步通过仿真实验对方法进行了验证。

关键词:无线传感器网络;入侵检测;sinkhole 攻击;多点监测
DOI:10.3778/j.issn.1002-8331.2008.22.040 **文章编号**:1002-8331(2008)22-0135-04 **文献标识码**:A **中图分类号**:TP393.08

1 引言

Karlof[1]最先指出了无线传感器网络中的 sinkhole 攻击,该攻击者声称能够提供一条到基站节点的单跳高质量路径,从而吸引攻击节点的每个邻居节点改变网络传输方向,将发往基站节点的包转发给 sinkhole 攻击者。严重破坏了网络的负载平衡,也为其他攻击方式提供了平台。

目前,国内外针对防范无线传感器网络 sinkhole 攻击的研究较少。多路径路由[2,3]和概率路由[4,5]是抵御 sinkhole 比较有效的方法。地理路由[6,7]也用于抑制 sinkhole 攻击的发生。多路径路由[2,3]中,数据包通过多条路由进行数据传输,目的节点至少得到一份正确的报文。在概率路由[4,5]中,节点通过某一固定概率动态选择下一跳路由节点。每一个节点均有机会选为下一跳节点,从而减小 sinkhole 攻击者控制数据流的机会。地理路由[6,7]中,每个节点都保存自己绝对或是彼此相对的位置信息,当攻击者企图跨越物理拓扑时,局部节点可以通过彼此间的拓扑信息识破这种破坏。但地理信息协议如 GPSR[8]有很多缺陷:安装、配置和维护另外的设备(GPS)在一些情况下是不现实的,而且地理定位信息需要通过复杂的数据加密算法传播。

2 预备工作

首先定义了适用于检测方案的假设,然后简要描述了本文采用的 μTESLA 协议,最后对总体检测方案进行初步阐述。

2.1 检测机制的几个假设

仿照文献[9],本文方案基于以下无线传感器网络假设而提出的:

(1)在部署阶段,传感器网络处于完全安全状态,攻击节点无法俘获网络节点。

(2)网络节点中只分为两种:正常节点与恶意节点。网络中只有源节点和基站可信,并且已知其大致定位,其余节点均可能被俘获。

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60703115);国家博士后科学基金(No.20070420955);江苏省博士后科研资助计划(No.0702003B);江苏省自然科学基金青年科技创新人才启动项目(No.BK2007560);江苏大学高级专业人才科研启动基金(No.05JDG020,No.07JDG080)。

作者简介:周玲玲(1983-),女,硕士研究生,主要研究领域:传感器网络安全技术;张建明(1964-),男,博士,教授,主要研究领域:模式识别、虚拟现实与系统仿真技术等;王良民(1977-),男,博士,讲师,博士后,主要研究领域:安全无线传感器网络、容忍入侵等。

收稿日期:2007-10-15 **修回日期**:2007-12-29

(3)传感器节点间的链路是双向的,节点间不存在单向链路,即 A 节点能与 B 节点通信,B 节点也能与 A 节点进行通信,各节点在网络初始阶段具有相同的传输半径。

2.2 μTESLA 协议

μTESLA 协议[10]是在松散时间同步的基础上,通过延迟公开密钥的方式实现认证广播的。算法首先通过单向 Hash 函数 h 构建一个密钥链$<k_1,k_2,k_3,\cdots,k_n>$其中 $k_i=h(k_{i+1})$。在节点被散布之前,密钥 k_n 将加载到每个节点中。除了 k_n 之外,密钥链中的每个密钥都与一个时间间隔相对应,并且所有在同一个时间间隔内发送的报文将被同一个密钥所鉴别。μTESLA 通过如下两步进行广播的鉴别:首先,发送者在时刻 t_v 首先发送消息和 MAC(Message Authentication Code)广播报文 P_V。因为在发送时刻消息被 k_v 加密,节点无法判断消息的真伪。然后,经过一个时间间隔 δ 后,发送广播密钥 k_i。而以前收到消息的节点通过等式:$k_i=h^{v-i}(k_v)$验证 即可鉴别其在时刻 δ 之前收到的报文是否是发送者实际广播的报文。但是这需要基站和节点的时间同步(至少是松散的同步)。否则,敌方就可以伪造消息(时间延迟大于 δ)对接收节点进行攻击,见图 1。

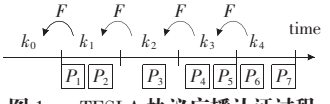

图 1 μTESLA 协议广播认证过程

本文利用 μTESLA 协议进行 ACK 包的数据认证,防止恶意节点伪造 ACK 包。

2.3 总体设计方案

提出了多点监测与回复信息相结合的攻击检测方法,用于发现网络中的异常,鉴别入侵者。sinkhole 攻击检测主要包括以下两个阶段:

(1)初始化阶段:网络的邻居发现,安全时间同步,μTESLA 协议密钥链的建立。

(2)攻击检测阶段:通过多点监测与回复信息,判定网络中是否存在攻击,若存在,隔离恶意节点并发出告警信息。

3 基于多点监测与回复信息的 sinkhole 检测

3.1 包的定义

对文中出现的两种数据包作如下定义。包的格式如图 2,图 3 所示。

Dst_ID	Packet_ID	Node_ID

图 2 路由测试包

Packet_ID	Dst_ID	Node_ID	OHC_number	MAC_{OHC}

图 3 应答包

测试包(Test_Packet)是在节点收到路由公告后,通过公告节点发往基站的数据包,用于测试路由公告是否可信。包的格式如图 2 所示。Node_ID 字段表示发送路由测试包的节点。Dest_ID 字段表示目的节点地址(基站地址),Packet_ID 字段表示包的 ID。

应答包(ACK)是基站对 Test_Packet 的回复包,利用μTESLA 协议进行数据认证,防止恶意节点伪造回复信息。包的格式如图 3 所示。OHC_number 和 MACOHC 是 μTESLA 协议中使用到的两个字段,OHC_number 是节点在密钥链中选用的密钥,MACOHC 是使用该密钥生成的 MAC 码,用于为整个 ACK 生成签名摘要,防止恶意节点编造应答包[11]。MACOHC 字段的内容如图 4。

MAC_{OHC}(Dst_ID,Packet_ID,Node_ID)

图 4 MAC_{OHC} 字段

3.2 检测原理

通过多点监测以及对回复信息的统计策略,对网络中可能存在的 sinkhole 攻击进行检测。检测按所处的网络状态分为两种类型:

(1)路由选择阶段:监测点发出 Test_Packet 到基站,对路由公告节点进行测试。基站回复 ACK 后,统计 ACK 的数目。通过计算比较,判定网络中是否存在恶意节点。若认为存在恶意节点,向全网发出警报。否则将其视为正常节点。

(2)数据传输阶段:监测点对节点收发数据包的情况进行监测,发现异常后向统计节点报告,统计节点根据收到的报告,判断络中是否存在 sinkhole 攻击。

3.3 检测步骤

以图 5 为例,对本文的 sinkhole 攻击检测方案进行分析说明。

图 5 中,假定节点 C、D、E 在节点 B 的通信范围之内,当节点 A 发出路由公告时,节点 B、C、D、E 均能收到路由公告,并将它们作为节点 A 的监测节点。

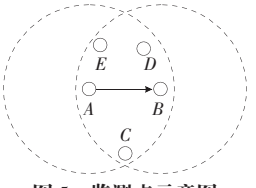

图 5 监测点示意图

为清晰说明本文的检测方案,给出主要符号描述算法过程。该算法中,首先假定监测点的监测时间均为 w 个时间单位,字符定义如下:

node_length:监测点总数;

chan_Lratio:信道丢包率;

Navai.:收到有效 ACK 包的监测点的统计值 node_NW 在检测期间,公告节点实际收到数据包的统计值;

node_Nforw:在检测期间,公告节点实际转发的数据包总数;

node_LW:公告节点在 w 个单位时间里的丢包率;

Nalarm:统计节点收到的报警总数;

node_ids:传感器节点的 id;

node_idcompr:检测出的被俘节点的 id;

compromised[ ]:存储被俘节点的 id;

node_idp:收到包的节点的 id;

node_idb:发送 alert 信息的节点的 id(即统计节点 id);

alert_buffer[ ]:存储收到的 alert 信息。

路由选择阶段:监测节点 B、C、D、E 收到 A 的路由公告后不立即认为其可信,而是将该公告存入 Cache,并发出 Test_Packet,用以测试路由是否可信。Test_Packet 通过公告节点 A 发往基站,若基站收到消息,向监测点发送 ACK 报文,统计节点 B 搜集 ACK 信息,统计 ACK 的数目。当 $N_{avai}\geqslant node\_length*(1-$

chan_Lratio)时,*B* 相信此公告,并用其更新路由表。否则将节点 *A* 视为恶意节点,并向全网发出告警。伪代码如下:

```
Code executed at node_id_p
On {arrival of} broadcast packet
If (node_id_p NOT in compromised[ ])
CreateSend(Test_Packet(Dst_ID,Packet_ID,Node_ID))
waiting for ACK=true
for( i=1;i<Node_length;i++ )
    if(wait for ACK)
        if (ack node=MAC_OHC(Dst_ID,Packet_ID,Node_ID))
         N_avai++;
       else
         drop false ACK;
    else N_alarm++;
Code executed at node_id_p when ACK timer expires:
waiting for ACK=false
if(N_avai<node_length*(1-chan_Lratio))
node_id_b report to source node loss and return
On{arrival of} compromise_found_node(node_id_compr)
Add node_id_compr to compromised[ ]
Send alert(compromised[ ] )
```

数据传输阶段:监测节点 *B*、*C*、*D*、*E* 监视节点 *A* 收发数据包的情况。根据上述定义 $node\_L_W=(node\_N_W-node\_N_{forw})/node\_N_W>chan\_Lratio$ 时,各监测节点分别向统计节点 *B* 发出告警信息。若报警总数 $N_{alarm}<node\_length/2$ 时,则认为 *A* 为正常节点,否则将其隔离。

伪代码如下:

```
Code executed at node id_s when
forwarding message
node_L=(node_N_W-node_N_forw/node_N_W);
for(i=1;i≤node_length;i++)
    if(node_L_W>chan_L_ratio)
      N_alarm++;
    if(N_alarm>node_length/2))
node_id_b report source node Loss  and return
```

4　性能分析与仿真

本文提出的方案是以检测网络中受到的 sinkhole 攻击为切入点提出的,因此,本章中,首先,对方案所能达到的安全概率进行理论分析。然后,通过仿真比较,对网络安全性能参数作进一步的评定。

4.1　性能分析

假定网络在正常情况下信道的丢包率为 *L*,且监测点的失效仅由信道的丢包引起,监测点失效后,不能作为判断节点是否被俘的依据;假设当有效监测节点总数大于某一阈值时(设为事件 *P*),检测机制总能作出正确的入侵判断。本文称事件 *P* 发生的概率为安全概率。下文对邻居节点数量和丢包率在不同的阈值下对安全概率的影响分别做出分析。

假设网络中每个节点的平均邻节点数为 *W*,则公告节点的监测节点数也为 *W*,其中,阈值为 *M*,信道的正常丢包率为 *L*。

把单个点的监测行为看成一次实验,则单个点的监测有效性 $X_k(k=1,2,\cdots,W)$服从(0-1)分布,即 $X_k=\begin{cases}1 & \text{监测点有效}\\ 0 & \text{监测点无效}\end{cases}$。

若设 *X* 为检测机制中,有效监测点的总数,因此,$X=\sum_{k=1}^{W}X_k$ 服从二项分布 $B(W,(1-L))$。

由棣莫弗-拉普拉斯(De Moivre-laplace)定理,可得

$$P_{det}(k)=P\{X>M\}=1-P\{X\leqslant M\}=1-\Phi\left(\frac{M-E(X)}{\sqrt{D(X)}}\right) \tag{1}$$

其中

$$E(X)=W*(1-L) \tag{2}$$

$$D(X)=W*(1-L)*L \tag{3}$$

将式(2)、式(3)代入式(1)中,得式(4)

$$P_{det}(k)=1-\Phi\left(\frac{M-W(1-L)}{\sqrt{M(1-L)L}}\right) \tag{4}$$

从式(4)可以看出,安全概率取决于信道的丢包率 *L* 和节点的邻节点数目 *W*,以及阈值 *M*。

以下分析了参数 *L*,*W* 以及 *M* 对安全概率的影响。

从图 6,图 7 中,可以得出如下结论:

(1)邻居节点数目增多,安全概率 P_{det} 增加;

(2)丢包率增大,安全概率 P_{det} 降低。

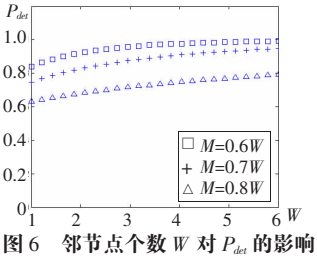

图 6　邻节点个数 *W* 对 P_{det} 的影响

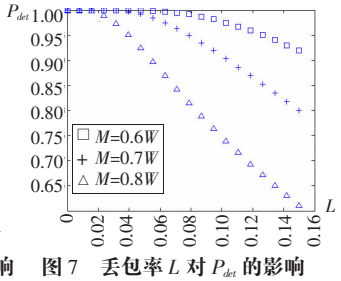

图 7　丢包率 *L* 对 P_{det} 的影响

本文的检测方案的安全概率取决于邻节点数及丢包率,因此,在通信环境比较恶劣的环境下,失效节点增多。在以下的仿真中,将考虑失效节点比例对安全概率的影响。

4.2　仿真环境与实验分析

加州大学的 Berkeley 分校开发的 TinyOS[12]是一个开源的嵌入式操作系统,是一种基于组件(Component-Based)的架构方式,能够快速实现各种应用。

TOSSIM 是直接从 TinyOS 代码中编译而来的 TinyOS 模拟器,TOSSIM 通过设置无线传感器网络中每条链路的比特出错率,模拟真实的无线传感器网络链路通信质量。TOSSIM 中提供了一个 GUI TinyViz,实现对网络的动态配置和实时交互显示。

以下仿真均是使用 TinyOS 自带的 TOSSIM 模拟网络的情况,证明检测方案的正确性。在相同的网络环境下,实验通过与文献[3]中的多路径方法进行对比,说明本文方法的可行性。

4.2.1　仿真模型的建立

在仿真环境中,为了能够了解检测方案的性能,建立具体的仿真模型如下:

(1)在 100 m×100 m 的区域内分布 50 个传感器节点。Sink 点位置固定,区域内节点的平均密度相同。

(2)每个节点的初始能量一致,通信范围相同。网络中的数据包以 19.2 kb/s 的速度逐跳传输。

TOSSIM 模拟器上运行,调试编写的程序,使用 make pc 对文件进行编译,得到可执行文件。用 TinyViz 可视化窗口显示了模拟过程,如图 8 所示。

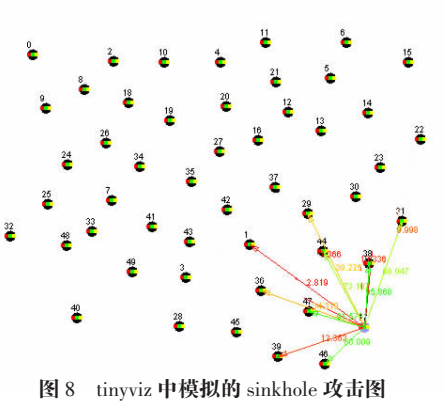

图 8 tinyviz 中模拟的 sinkhole 攻击图

4.2.2 仿真比较与分析

文献[3]将不相交多路径(DM)和缠绕多路径(BM)的方法用于安全路由算法中,避免传感器网络中存在的攻击。将本文所提方法与文献[3]的方法比较并仿真实验,对网络中存在不同的失效节点比例的情况下,进行安全概率的研究。

从图 9 中可以看出,本文方法的安全概率大于不相交多路径的方法,证明检测有效。

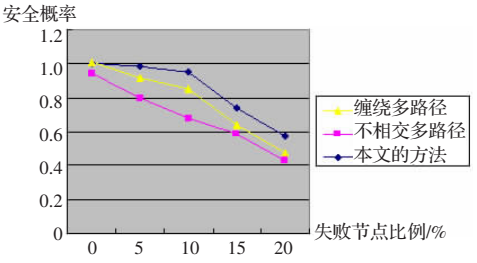

图 9 三种方法下安全概率的比较图

5 总结

依靠基站节点建立初始拓扑结构的协议, 如定向扩散 DD 等极易受到 sinkhole 攻击,本文针对协议的弱点,提出了基于多点监测与回复信息的攻击检测算法,这种方法避免了复杂的加密算法与身份认证,与多路径安全机制相比有着更高的可靠性。分析和实验表明,本方案可得到较高的安全概率。

参考文献:

[1] Karlof C,Wagner D.Secure routing in wireless sensor networks:attacks and countermeasures[C]//IEEE International Workshop on Sensor Network Protocols and Applications,2003,1(5):113-127.

[2] Ganesan D,Govindan R,Shenker S,et al.Highly-resilient,energy-efficientmultipath routing in wireless sensor networks [J].Mobile Computing and Communications Review,2002,1(2):295-298.

[3] 李铁山,张锦,王东,等.传感器网络中容错路由算法分类研究[C]//全国第 16 届计算机科学与技术应用(CACIS)学术会议论文集.合肥:中国科技大学出版社,2004:1039-1044.

[4] Barrett C L,Eidenbenz S J,Kroc L,et al.Parametric probabilistic sensor network routing [C]//Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications,2003:122-131.

[5] Servetto S D,Barrene-chea G.Constrained random walks on random graphs:routing algorithms for large scale wireless sensor networks[C]//Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications,2002:12-21.

[6] Lazos L,Poovendran R.SeRLoc:secure range in dependent localization for wireless sensor networks[C]//Proceedings of the 2004 ACM Workshopon Wireless Security.New York:ACM Press,2004:21-30.

[7] Capkun S,Hubaux J.Secure positioning in sensor networks,IC/200444[R].EPFL,2004-05.

[8] Karp B,Kung H T.GPSR:greedy perimeter stateless routing for wireless networks[C]//Proceeding of the ACM MobiCom,Boston,USA:ACM Press,2000:243-254.

[9] Marti S.Mitigating routing misbehavior in mobile ad hoc networks [C]//Proceedings of the 6th Annual International Conference on Mobile Computing and Networking,Boston,United States,2000:255-265.

[10] Perrig A,Szewczyk R,Wen V.SPINS:security protocols for sensor networks[C]//Proceedings of the ACM Mobicom.Rome,Italy:ACM Press,2001:189-199.

[11] 俞波.杨珉,王治,等.选择传递攻击中的异常丢包检测[J].计算机学报,2006,29(9):1542-1552.

[12] Levis P,Lee N,Welsh M,et al.TOSSIM:accurate and scalable simulation of entire TinyOS applicat-ions[C]//Proceedings of the 1st International Confer ence on Embedded Networked Sensor Systems,2003:126-137.

(上接 134 页)

义恒模算法应用到了多用户检测中去。计算机仿真实验表明该算法无论是在信道噪声为高斯白噪声还是 α-稳定分布噪声的情况下,信干比和误码率均表现出良好的性能,对脉冲噪声不敏感,具有相当强的鲁棒性。

参考文献:

[1] Verdu S.Minimun probability of error for asynchronous Gaussian multiple-access channels[J].IEEE Trans Inform Theory,1986,32(1):85-96.

[2] Verdu S.Multiuser detection[M].[S.l.]:Cambridge University Press,1998.

[3] Poor H V,Verdu S.Probability of error in MMSE multi-user detection[J].IEEE Trans Info Theory,1997,43:858-871.

[4] Lee W,Vojcic B,Pickholtz R L.Constant modulus algorithm for blind multiuser detection[C]//Proceedings IEEE ISSSTA'96,Mainz,Germany,Sept 1996:1262-1266.

[5] Blackard K L,Rappaport T S.Measurements and models of the radio frequency impulsive noise for indoor wireless communications[J].IEEE Journal on Selected Areas in Communications,1993,11(7):991-1001.

[6] Nikias C L,Shao Min.Signal processing with slpha-stable distribution and application[M].[S.l.]:John Wiley & Sons,Inc,1995.

[7] Godard D.Self-recorvering equalization and carrier-tracking in two-dimensional data communication systems[J].IEEE Trans Commun,1980,28:1867-1875.

[8] 张贤达,保铮.通信信号处理[M].北京:国防工业出版社,2000-11:249-256,383-389.

[9] Qiu Tian-shuang,Tang Hong,Zhai Dai-feng.Capture properties of the generalized CMA in alpha-stable noise environment[C]//2004 7th International Conference on Signal Processing,2004,1:422-439.