无线传感器网络中一种基于接收功率异常的入侵检测算法

王 骐[1,2] 王 殊[1] 孟中楼[1]

(华中科技大学电子与信息工程系 武汉 430074)[1] (湖北第二师范学院物理与电子工程系 武汉 430074)[2]

摘 要 虽然静态传感器节点计算能力和通信能力较差,但是它们具有自己独特的特征,可以获取比较稳定的临域节点信息。利用这个特征可以检测网络异常情况以及临域节点的通信行为,为传感器网络提供安全保障。为了使传感器节点能够检测出入侵者,需要先建立一种简单的基于临域节点的动态统计模型,然后用一种低复杂度的检测算法监测已接收到的数据包的接收功率。首先介绍了一种基于无线传感器网络安全的入侵检测算法,然后介绍了一种基于该算法的节点协作检测技术,节点协作指的是对攻击的联合确认,以及邻居节点共同反抗入侵者的协作行为。

关键词 无线传感器网络,接收功率异常,入侵检测 算法仿真,节点协作检测技术

中图法分类号 TP301.6 **文献标识码** A

Intrusion Detection Algorithm Based on Reception Power Anomaly in Wireless Sensor Networks

WANG Qi[1,2] WANG Shu[1] MENG Zhong-lou[1]

(Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, China)[1]

(Department of Electronics and Physics Engineering, Hubei University of Education, Wuhan 430074, China)[2]

Abstract Although static sensor nodes have low computation and communication capabilities, but they have specific properties, and can acquire stable neighborhood information, which can be used for detection of anomalies in networking and behaviors of the neighbor nodes, to provide security for wireless sensor network. To make a sensor node capable of detecting an intruder, a simple dynamic statistical model of the neighboring nodes is needed to build, with a low-complexity detection algorithm to monitor received packet power levels. A detection algorithm based on security scheme for wireless sensor networks was introduced, and then a novel node cooperative detection technology based on this detection algorithm, which refers to affirm and stand against intrusion together, was proposed.

Keywords Wireless sensor networks, Reception power anomaly, Intrusion detection, Algorithm simulation, Node cooperative detection technology

1 引言

无线传感器网络是一种特殊的 Ad Hoc 移动网络,是一个分布式的感知探测系统,一般部署在无人值守的环境中。网络部署区域的开放特性和无线电通信的广播特性给网络安全带来了极大的隐患。作为一种起源于军事应用领域的新型自组织网络,无线传感器网络主要采用射频无线通信组网,其安全性问题显得尤为重要。尽管无线传感器网络的安全技术取得了很多进展,但还有一些问题尚未完全解决。在复杂的安全环境、多样的安全需求和资源限制等因素的综合影响下,无线传感器网络的安全技术仍然面临着很多挑战[1],在网络协议栈的各个层次中都可能受到攻击,而且攻击手段多种多样[1]。

鉴于各个层次面临的种种攻击,无线传感器网络采取了多种手段来保障网络的安全。一般来说,网络安全方案可分为两大类:预防和检测。预防技术,比如加密、认证、防火墙、物理隔离等,通常是防止攻击的第一道防线。这些入侵预防措施虽然可以减少入侵,却不能够绝对消除入侵。从安全研究的经验来看,WSNs 无论采取多少安全预防措施,它们总会存在一些能够被入侵的物理链路,因此预防技术总显得比较脆弱。入侵检测成为 WSNs 安全的第二道防线,特别是那些对网络生存期要求比较高的 WSNs,入侵检测显得尤为必要。检测技术所要达到的目标是当预防措施失效时识别和抵挡攻击者的攻击行为。入侵检测可定义为:"识别那些未经授权而使用计算机系统的非法用户和那些对系统有访问权限但滥用其特权的用户"。

入侵检测技术可分为特征检测(Misuse detection)和异常检测(Anomaly detection)两种[1]。特征检测假设入侵者的活动可以用一种模式来表示,系统的目标是检测主体活动是否符合这些模式。其优点是能准确和有效地检测出已知的入侵,缺点是不能检测新出现的攻击,其难点在于如何设计模式,使其既能表达"入侵"现象又不会将正常的活动包含进来。

到稿日期:2008-04-17 本文受国家 985 工程项目(基于网格的高性能计算与复杂系统仿真平台建设)资助。

王 骐(1970—),讲师,博士研究生,主要研究方向为无线传感器网络安全、嵌入式系统应用等,E-mail:wangqi_wh@163.com;王 殊(1956—),教授,博士生导师,主要研究方向为无线传感器网络、智能信号检测、传输、处理及应用等;孟中楼(1976—),博士研究生,主要研究方向为人工智能与生物仿生。

基于异常的检测技术则是先定义一组系统"正常"情况的数值[2]，如CPU利用率、内存利用率、文件校验和等(这类数据可以人为定义，也可以通过观察系统并用统计的办法得出)，然后将系统运行时的数值与所定义的"正常"情况比较，通过监测明显异于正常行为的活动来预测入侵。这种检测方式的核心在于如何定义所谓的"正常"情况，对用户要求比较高。其主要优点是不需要入侵检测的前期知识，而且可以检测到新的入侵；最主要的缺点是它不能描述入侵的形式并且可能出现很高的差错率。

概念上，一个入侵检测模型主要包括两个单元[3,4]：(1)特征(属性)。描述典型活动的特性，例如"错误录入的尝试次数"、"命令访问的平均频率"。(2)模型算法。使用特征进行入侵检测和抑制入侵的算法。

目前，移动Ad Hoc网络在安全方面已经有了许多基于预防性的解决方案。尽管Ad hoc网络和传感器网络都属于无线网络类别，但由于二者之间存在较大差异，移动Ad Hoc网络的安全机制，无论是预防技术还是检测技术，都不能直接用于无线传感器网络[5]。

本文介绍一种基于简单而资源有限的无线传感器网络异常入侵检测技术。假定传感器网络由静态传感器节点组成，并且每个节点能够提供稳定的临域节点信息。那么在这种分布式传感器网络中，传感器节点对临域节点的行为进行简单的统计，并根据统计模型检测邻居节点是否存在异常。由于异常行为可能发生在网络的各层，只要实现方式是资源感知的[6]，那么每一层都可以确定本层的正常变量值，入侵检测对偏离正常值的异常行为将发出入侵警报。

2 异常检测算法

2.1 网络模型

根据网络结构的具体情况，节点具有以下特征[7,8]：

1)某个特定节点的邻居节点保持不变。这意味着节点是静态的，而且传输功率不会改变。当网络布置完毕后，网络内不会再有新节点加入。

2)每个节点都能够很精确地识别它的邻居节点(比如通过节点的ID)。

3)信息数据包和控制数据包是有方向性的，节点路由采用树状转发结构[9]。

4)所有的节点都是对等实体。节点的硬件相同，运行相同的协议栈，且具有恒定的传输功率。

5)每个节点都有一个内部时钟，但节点之间并不需要保持同步。

本文研究基于以下类型的攻击：

1)节点伪装。攻击者为了使用或者破坏一个传感器网络，必须把自己伪装成一个合法节点。通常的作法是通过欺骗的手段得到某个节点的ID，然后攻击者开始耗尽网络的资源或者在网络内传播错误的警报。

2)资源耗尽。这种攻击也可以看作当一个节点伪装成功后下一步所要采取的行动。由于传感器网络具有规模大、多跳以及协作等特性，入侵节点会创建大量的无用信息数据包和控制数据包，快速消耗许多节点的能量，从而破坏传感器网络。

节点保存着它们的邻居节点的统计信息。邻居节点一旦偏离了正常节点的收发模式和流量行为，以上列举的攻击行为就会暴露出来。

2.2 检测算法

检测算法根据某种判别规则对入侵模式进行检测，这里选取平均接收功率(单位为dBm)来表征邻居节点的行为。算法采取基于滑动窗口的数据包计数方式。每个节点所接收的来自邻居节点的数据包中，只有最后的N个数据包才被用于计算该邻居节点数据包的统计量，以后每个到达的数据包和这些统计量值相比较。N称作数据包主缓冲区长度。如果数据包符合邻居节点的统计量值，那么该数据包被认为是正常的数据包，并被用于计算新的统计量值。最开始的数据包的统计量值也会从列表中清除。实验中，记录下每个到达的数据包的到达时间和接收功率。

为了监视异常数据包的接收功率，数据包接收功率的最小、最大值需要不断更新，使之与每个正常数据包的接收功率值相匹配。当前存储在长度为N的数据包主缓冲区中的异常数据包，它的接收功率要么小于正常接收功率的最小值，要么大于最大值。根据传感器网络的布置环境和应用场合，在下列情况下传感器网络将发出入侵警报：检测到单个异常数据包时，或者预定义数量的连续数据包均显示为异常模式之后。在后一种情况下，在系统采取某种决策之前，异常数据包必须和正常到达的数据包保持隔离。用于隔离异常数据包的缓冲区称作入侵缓冲区，长度定义为$N1$。

接收功率异常的检测流程：

1)接收数据包。

2)根据IDS规则进行判别。如果是正常数据包，如果数据包主缓冲区未满，则存储于数据包主缓冲区；如果是异常数据包，则存储于异常缓冲区。

3)报警。如果入侵缓冲区中连续收到的异常数据包数量小于$N1$，则将所有异常数据包插入数据包主缓冲区；如果连续收到的异常数据包数量等于$N1$，则$N1$个连续数据包保存于入侵缓冲区，并使之与正常数据包保持隔离，系统将发出入侵警报。如果连续收到数量小于$N1$的异常数据包后系统接收到一个正常数据包，那么入侵缓冲区将会被清空。

4)修改IDS判别规则(即修改模型的统计量值)。根据数据包主缓冲区中异常数据包的每次插入情况修改IDS判别规则。

检测失效的数据包的数量称为失误门限值(miss threshold)，其长度定义为$N3$。如果未被检测出来的异常数据包有N个，这N个数据包将修改数据包主缓冲区的特性，并且以后再也不会被检测到。因此，$N3$必须小于N。选取合适的$N1$和$N3$(这些值的大小取决于系统的安全漏洞)非常关键，因为这些值对检测概率以及检测次数(这在下一节会提到)有较大影响。

在接收功率异常的检测方案中，为了发起成功的攻击，攻击者必须使它与被伪装节点的每一个邻居节点的相对距离基本保持不变。如果入侵者所处的位置变化较大，那么由于接收功率异常，数据包被检测的可能性将会提高。为了侵入网络，攻击者要么采用与节点收发器相同的硬件结构，要么具有功率控制能力，来效仿被伪装节点的收发器。

3 算法仿真

3.1 传输模型

假定在整个数据包的传输过程中无线信道不会发生改

变，事实上无线信道在数据包的传输过程中是随机和独立的。仿真采用对数正态分布的阴影路径衰落模型，来计算不同数据包的接收功率。假定平均接收功率随着距离 d（表现的形式为$(1/d)^{\beta}$）增大而减小，平均值的随机波动值定义为标准差为 σ（单位为 dB）的零均值高斯随机变量 X_σ（单位也为 dB），模型的通用公式如下[10,15]：

$$PL(d)(\mathrm{dB})=PL(d_0)+10\beta\log(d/d_0)+X_\sigma \quad (1)$$

其中，$PL(d)$是距离为 d 的路径衰落，是根据近距离参考值 d_0 计算出来的。变量 β 称作路径衰落指数，标准差 σ 称作阴影偏差。距离为 d 的信号接收功率 P_r 由下式计算[11,15]：

$$P_r(d)(\mathrm{dBm})=P_{tr}(\mathrm{dBm})-PL(d)(\mathrm{dB}) \quad (2)$$

这里 P_{tr} 是发射器的输出功率。另外，当且仅当数据包的接收功率大于门限值，这个数据包才能够被接收。根据低功率传感器的收发器运行结果，以及文献[12,13]对链路特征的研究，实验选取的参数值如下：β,σ,d_0，发送功率 P_{tr}，接收功率门限值分别为 2.5，5dB，1m，5dB，－90dBm。

3.2 算法的性能仿真

本节阐述算法对接收功率异常的检测结果。算法的仿真参数值如下：初始发送功率（训练功率）P_{tr}，d，N，$N3$ 分别为 5dBm，25m，100，25。图 1 给出了当入侵缓冲区长度 N 发生改变时系统的误报警概率。如果功率变化仅仅由信道变化引起，如阴影模型所示（P_{tr} 恒定为 5dBm），那么在这种情况下一旦发生误报警，算法仍将把正常的发送节点当成入侵节点。

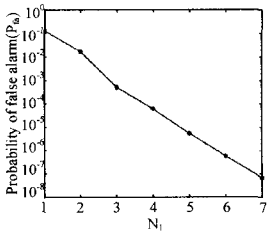
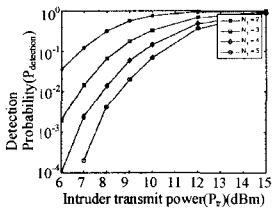


图 1　缓冲区长度 $N1$ 与误报警概率的关系

当发送节点的实际传输功率发生改变，在入侵缓冲区长度（$N1$）取不同值时，算法的性能如图 2、图 3 所示。实验需要通过一个初始的训练期，来告诉检测节点的邻居节点正常的接收功率大小。对于最初开始的 N 个数据包，发送节点的初始功率保持在 5dBm 不变，然后增大发送功率，实验记录下检测概率和检测次数。检测失效的异常数据包（$N3$）保持为常数 25。



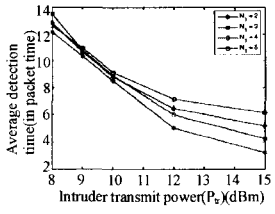


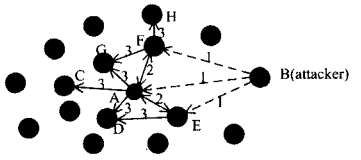
图 2　入侵功率与检测概率的关系　图 3　入侵功率与检测次数的关系

当入侵的异常度提高时，数据包将会在较短时间内被检测到，而且检测概率会随之增大，这跟预期结论是一致的。另外，如果减小入侵缓冲区长度 $N1$ 的值，那么检测概率将增大，检测延时将减小，但同时也将导致误报警率增大。因此，在实际的网络布置中，这些指标需要根据应用安全的需求来进行权衡。

4　传感器网络的节点协作检测技术

上节阐述的是一种入侵检测算法，本节阐述基于这种算法的入侵检测技术——节点协作检测技术。该技术主要检测邻居节点的行为是否存在偏差。一旦检测到偏差，将被定义为入侵节点。这里节点协作指的是对攻击的联合确认以及邻居节点共同反抗入侵者的协作行为。这个方案的关键点在于：1）节点知道需要从其它节点获取什么信息，特别是它们的邻居节点。节点检测以后，如果发现异常情况，将会相互报告。如果节点需要作出判决，传感器网络为每一个节点提供的邻居节点信息必须相对稳定。2）如果邻居节点出现了异常，节点将会通知其它节点。这种机制有利于确认入侵行为，并相互协作，共同抵抗攻击者。

节点协作方案对入侵者的检测和牵制入侵的策略如图 4 所示。在图 4 中，节点 B 是一个假冒合法节点的攻击者。假设正常节点在没有被毁坏的情况下很容易检测到使用自己 ID 的伪装节点。当节点 A 检测到节点 B 的恶意行为后，节点 A 会把这个消息告诉它的邻居节点 F 和 E。如果其它节点均认定节点 B 存在异常，那么节点 A 就可得出结论：目前有多于固定数量（根据节点分布密度选择）的其它节点都确认节点 B 的行为模式非正常，那么节点 A 就可以断定节点 B 是一个入侵节点。在听到入侵节点被检测到的广播消息后，那些已经检测到节点 B 存在入侵行为但还不能够完全确认的其它节点（因为只有少部分节点确认了入侵行为），现在就可以立即得出结论：节点 B 是入侵节点。然后邻居节点采取联合行动，入侵节点就会被牵制。如果某些邻居节点还没有查觉到入侵节点，那么那些检测节点也会把入侵消息通知给它们。



说明：1）图中的数字表示节点跳数；2）B（伪装成节点 B 的入侵节点）试图和节点 B 的邻居节点通信；3）通过彼此间的互相通信，节点 F，A，E 检测并确认节点 B 的行为模式非正常；4）节点 F，A，E 向它们的邻居节点发出警报，伪装成节点 B 的入侵节点受到牵制。

图 4　入侵节点被牵制的示意图

这里的协作主要指的是发现入侵后节点的共同协作行为，实际上节点执行的检测算法不必相互协作。也就是说，邻居节点在还没有确认入侵的情况下，每个检测节点可能采取独立的行动，这种策略对牵制入侵节点可能已经足够。实际上，低复杂度的协作策略会大大减少错误警报的发生，并且会提高检测的效率[14]。实验数据表明该方案是一种可行性方案，能够检测出节点的入侵，但还存在一定的检测误差和误报警率。如何提高检测效率以及降低误报警，是下一步要具体研究的内容。

结束语　根据网络内邻居节点能够提供稳定信息的这一特征，本文提出了一种基于传感器网络安全机制的异常检测方法。如果每个节点能够建立一个邻居节点行为的简单统计模型，那么就能够通过这些统计模型去检测它们的变化。实践证明，通过对接收到的少量数据包的特性进行分析，一个节点能有效地识别伪装成某个合法邻居节点的入侵者。在实施

方案中，假设异常检测算法在每个节点上独立运行，低复杂度的协作算法可能会改善检测和遏制入侵的过程。一旦发现入侵，邻居节点将共同协作牵制入侵。目前实施方案还不完善，还存在一定的检测误差和误报警率，提高检测效率、降低误报警率将是下一步研究的具体目标。

参 考 文 献

[1] Chee Y, Rabaey J, Niknejad A. A class A/B low power amplifier for wireless sensor networks[C]// Proceedings of the 2004 International Symposium on Circuits and Systems. 2004, 4: 409-412

[2] Karlof C , Wagner D . Secure routing in wireless sensor networks: Attacks and countermeasures[C]// Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications. May 2003: 113-127

[3] Huang Y A , Lee W . A cooperative intrusion detection system for ad hoc networks[C]// Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. ACM Press, 2003: 135-147

[4] Vigna G, Gwalani S, Srinivasan K, et al. An intrusion detection tool for AODV-based ad hoc wireless networks[C]// Proceedings of the 20th Annual Computer Security Applications Conference. 2004: 16-27

[5] 覃伯平，周贤伟，杨军. 无线传感器网络路由协议的攻击检测模型[J]. 计算机工程，2007，33(2)：117-119

[6] Xu Y, Heidemann J, Estrin D. Geography-informed Energy Conservation for Ad-hoc Routing[C]// Proc. of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking. 2001: 70-84

[7] Perrig A, Stankovic J, Wagner D. Security in Wireless Sensor Networks[J]. Communications of the ACM, 2005, 47(6)

[8] Lamport L, Shostak R, Pease M. The Byzantine Generals Problem[J]. ACM Transaction Programming Languages and Systems, 1982, 4(3): 382-401

[9] 裴庆祺，沈玉龙，马建峰. 无线传感器网络安全技术综述[J]. 通信学报，2007，28(8)：113-122

[10] Chan H , Perrig A , Song D . Random Key Predistribution Sch emes for Sensor Networks[C]// IEEE Symposium on Research in Security and Privacy. May 2003

[11] Zhang Y, Lee W, Huang Y A. Intrusion detection techniques for mobile wireless networks[J]. Wireless Networks, 2003, 9(5): 545-556

[12] Estrin D, Sayeed A, Srivastava M. Wireless sensor networks, Mobicom Tutorial. http://nesl. ee. ucla. edu/tutorials/mobicom02, 2002

[13] Zuniga M, Krishnamachari B. Analyzing the transitional region in low power wireless links[C]// Proceedings of the IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON). 2004

[14] 周贤伟，王培，覃伯平，等. 一种无线传感器网络异常检测技术研究[J]. 传感技术学报，2007，20(8)：1870-1874

[15] Onat I, Miri A. An intrusion detection system for wireless sensor networks[C]// Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005)/IEEE International Conference on Volume 3, Aug. 2005: 253-259

(上接第 29 页)

地计算出要被读、异或和写的页。EOM 通过结合针对受影响的校验页的字计划计算出 I/O 计划。这个可通过从逆矩阵中选择列，并将写策略转换成必要的读、异或和写操作。读操作集在留意干净页向量时被计算。

假如受影响的校验页 k 的子计划表示成 r_k，X_k，W_k，那么组合的 I/O 计划是通过总结所有的单个子计划得来的。

$$r=\bigvee_{k\in parity} r_k; X=\bigvee_{k\in parity} X_k; W=\bigvee_{k\in parity} w_k$$

结束语 已经显示了 EOM 对于在不增加固件复杂性的情况下提供多种 RAID 码的问题，是一个理想的解决方案。根据现有的知识，EOM 在能力上是独特的，同时具有灵活性（支持任何基于异或的 RAID 码）、简单性（统一的无故障和故障清除路径）和自我调节性。相对于现有的 RAID 实现，EOM 不仅具有竞争力，而且对于很多负载提供适当的性能提升。

对于将来可能的工作，是使 EOM 在适应数据布局上平衡一下性能、可靠性和工作效率。

参 考 文 献

[1] Archivas. http://www. archivas. com/

[2] Blaum M , Brady J , Bruck J , et al. EVENODD : An optimal scheme for tolerating double disk failure in RAID architectures. IEEE Transactions on Computers, 1995, 44(2): 192-202

[3] Blaum M, Bruck J, Vardy A. MDS array codes with independent parity symbols. IEEE Transactions on Information Theory, 1996, 42(2): 529-542

[4] Deenadhayalan V, Hafner J L, Rao K K, et al. Matrix methods for lost data reconstruction in erasure codes. Technical Report RJ 10354. San Jose, CA: IBM Research, 2005

[5] Aarohi Communications. http://www. aarohi. net

[6] Corbett P, et al. Row-diagonal parity for double disk failure// Proceedings of the Third USENIX Conference on File and Storage Technologies. 2004: 1-14

[7] Hafner J . WEAVER codes : Highly Fault Tolerant Erasure Codes for Storage Systems// Proceedings of the Fourth USENIX Conference on File and Storage Technologies. San Francisco, CA USA, December 2005: 211-224

[8] Intel Digital Enterprise Group Storage Components Division . SCD roadmap update. Powerpoint slide deck, March 2005

[9] iVivity. http://www. ivivity. com/

[10] Aristos Logic. http://www. aristoslogic. com/

[11] LeftHand Networks. http://www. lefthandnetworks. com/

[12] Patterson D, Gibson G, Katz R. A case for redundant arrays of inexpensive disks (RAID)// Proceedings ACM SIGMOD. ACM, June 1988: 109-116

[13] Isilon Systems. Uncompromising reliability through clustered storage. http://www. isilon. com/media/pdf/Isilon _ Uncompromising_Reliability. pdf, May 2005

[14] Terrascale Technologies. http://www. terrascale. com/

[15] Xu L, Bruck J. X-code: MDS array codes with optimal encoding. IEEE Transactions on Information Theory, 1999, 45: 272-276