

能耗均衡的无线传感器网络的入侵检测机制

彭春燕, 杨志强, 张效娟

(青海师范大学 计算机学院, 青海 西宁 810008)

摘 要: 针对无线传感器网络中能量有限和安全问题, 本文提出了一种基于能耗均衡的无线传感器的入侵检测机制. 首先在无线传感器现有的分簇模型上划分若干 Sector, 然后在某些节点上部署 IDS, 提出入侵检测的算法, 利用仿真验证了本文所提出的模型与算法, 结果表明可使网络节点的能耗得到有效的降低, 同时提高了检测错误数据和异常节点的准确率.

关键词: 无线传感网络; 能耗节省; 入侵检测

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2013)01-0041-04

An Energy-Balancing Intrusion Detection Mechanism of Wireless Sensor Network

PENG Chun-yan, YANG Zhi-qiang, ZHANG Xiao-juan

(School of Computer, Qinghai Normal University, Xining 810008, China)

Abstract: Based on energy-limited and security of the wireless sensor network, a intrusion detection system is proposed based on the energy consumption of the equilibrium in wireless sensor network in this paper. At first, we put forward a cluster of WSN is divided into several Sectors, and only a few nodes are deployed with IDS. The result show that the proposed model and algorithm can reduce energy consumption effectively and improve the efficiency of the testing error data and anomalous node.

Key words: wireless sensor network; power saving; intrusion detection

1 引言

无线传感器网络(Wireless Sensor Networks, WSN)是由一组廉价、低功耗且具有传感、数据处理和短距离无线通信功能的传感器节点构成的网络系统. 在无线传感器中, 所有节点均可以获得重要数据, 并将这些数据通过 Sink 节点发送到另一个网络或者传送给终端控制室. 传感器节点的运作通常是由电池供电, 因此资源宝贵而有限. 无线传感器网络很容易受到各种各样的攻击, 如伪造路由、选择性转发、伪造基站、虫洞、黑洞和泛洪等都是常见的攻击. 传感节点具有非常有限的计算能力、记忆能力和电力资源, 在无线传感器网络中无法使用复杂的安全机制, 因为如果安全机制太过复杂, 常会导致某些节点能量过早枯竭, 影响整个网络的寿命, 也进一步增

加了无线传感器网络的不安全性.

许多学者已经提出多种入侵检测算法^[1-5], 但这些检测技术都不能满足能量均衡的实际需要. 本文提出了一种基于能量均衡的分簇入侵检测模型, 是一种分布式的基于异常检测的模型, 可以克服传感器节点因能量耗尽引发的突然崩溃, 在这个模型中, 若干节点联合检测, 减少了单个节点的负担, 能够排除恶意节点攻击及检测异常行为, 检查出虚假信息包.

2 网络模型

2.1 提出模型

现有的传感器网络大多属于非对称无线传感器网络, 本模型依然将无线传感器网络按照地域相邻性分成不同的簇, 再根据剩余的能量将传感器节点

收稿日期: 2012-05-13; 修回日期: 2012-06-07

基金项目: 国家自然科学基金项目(61162003); 青海省自然科学基金(2012-ZR-3017)

分成不同的角色,如 Sink 节点(SinkNode, SN)、簇首节点(ClusterHead, CH)、Sector 监视器(Sector-Monitor, SM)、Sector 头节点(SectorHead, SH),以及叶子节点(LeafNode, LN). 其中,为了避免资源耗尽,CH、SM、SH 的角色将动态改变,SN 被看做是具有网关功能的节点,将汇聚的数据转发到另一个网络. 在一个簇中,CH 节点由 Sink 节点来选举,又将簇内的传感器节点分成若干个段(即 Sector),每一个段中由 CH 来选举 SM、SH 节点,在一个 Sector 段中的普通节点将数据发送给各自的 SH 节点,各 SH、SM 节点经过数据异常检测把数据传输给 CH,CH 和 SN 之间进行直接的通信,这样不是所有节点都向某一节点发送数据,形成的这种层次结构就可以帮助某些节点维持自己的剩余电量,从而减少了传感器节点的资源耗尽,延长了整个网络的生存时间. 检测模块将被安置到 SH、SM、CH 中,其余都为叶子节点 LN,只用来感知收集信息并向上一层传递信息. 提出的模型如图 1 所示.

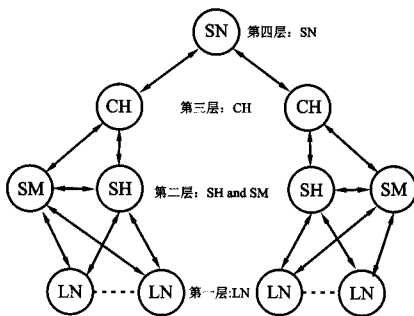


图 1 四层模型

2.2 节点的定义与选举

定义 1 如果一个节点 N 的子节点不为空,父节点为空,则这个节点被称为 SN. 记作: 如果 $ChildN\{\} \neq \{\Phi\}$ and $ParentN\{\} = \{\Phi\}$, 那么节点 N 是 SN 节点.

在选举过程中,首先由 Sink 节点将它的节点 ID 和查询信息广播到每一个能收到信息的节点,获取该范围内每一个可达节点的当前能量信息. 其次, Sink 节点根据接收的各传感器节点的回应包信息,按照传感器节点的剩余能量进行分类,选出能量较高的节点作为备用节点.

定义 2 如果一个节点的剩余能量是簇中所有能量最多的,并且他的容量最大,则这个节点被称为 CH. CH 的选择非常关键,需要满足以下两个条件:

$$Rem_engN\{\} = \text{Max_eng}\{N[\]\} \quad (1)$$

$$CapacityN = \text{Max}\{((\text{Deg}N/\text{Initial_eng}N) * \text{Rem_eng}N)\} \quad (2)$$

其中, $\text{Deg}N$ 是在射频范围内所有的节点数量. 在上一步 SN 选出的所有备用节点中,和 Sink 节点距离最短、剩余能量最高且信誉最高的节点作为簇头节点. 满足这两个条件的节点 N 就是这里的簇头节点 CH.

定义 3 如果一个节点 N 在这一个段中,拥有最大的入侵检测能力,则称为段监视器 SM. 记作: $\text{Detect_power}N = \text{Max}\{N[\]\}$ and $N \notin \{\text{CH}, \text{SN}\}$, 该节点是 SM.

在选举 SM 的过程中,除已选出的 CH、SN 节点外,如果该节点有着最高的检测能力,其次距离 CH 较近的节点则被选举为 SM 节点.

定义 4 如果一个节点 N 的剩余能量是该 Sector 中所有节点中是最大的,则这个节点被称为 SH. 记作: 如果 $\text{Rem_eng}N\{\} = \text{Max_eng}\{N[\]\}$, 那么节点 N 则为 SH.

定义 5 如果一个节点 N 的子节点为空,父节点不为空,并且它不具备任何检测入侵的能力,则这个节点被称为叶子节点 LN. 记作: 如果 $ChildN\{\} = \{\Phi\}$ and $ParentN\{\} \neq \{\Phi\}$, 那么节点 N 是 LN.

在剩余的节点中,有着最大的剩余能量的节点被选举为 SH; 其他没有被选中的节点都是叶子节点.

3 基于能耗的入侵检测算法

在该模型的最底层, LN 主要用来感知环境数据并将数据传输到它的上一层,这一层没有异常检测能力. 第二层由若干个 Sector 的 SH 组成, SH 负责收集从最底层传来的数据并检测有无任何异常. 每一个 SH 都维持一张成员列表 $\text{memberlist}[\]$, 包含了该 Sector 中所有的叶子节点的属性,如位置、频率、能量值等. 它具有一定的检测能力,会对数据做一个初步的检测,若数据安全合理,将直接发送给上一层 CH; 若检测数据异常则发送给 SM 进一步检测,并将发送异常数据的节点信息追加 $\text{suspectedlist}[\]$ 中. 在整个模型的联合检测中, SM 拥有 80% 的检测能力,当有数据发送过来时, SM 继续检测数据,将正确有效的数据传输给 CH, 若数据异常,丢弃数据包,并将发送虚假信息节点加入到 $\text{isolatedlist}[\]$ 中. 在第三层中,再对数据做最后的检测,有效数据传输到上一层 SN 节点,有问题的数据丢弃且记录虚假节点信息. 第四层的 Sink 节点收集来自低三层的数据,并作为网关将数据发送给其他传感器网络或作为存取点发送给数据处理中心. 算法处理过程如图 2 所示.

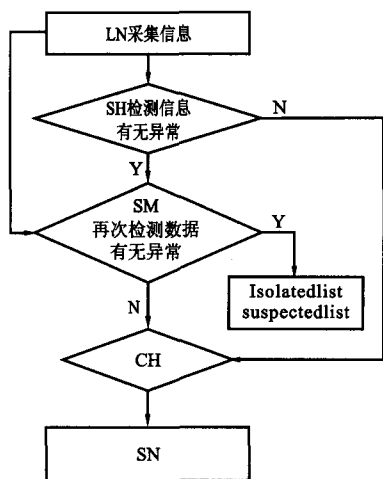


图 2 入侵检测流程图

无线传感器网络中异常检测的目标是对无线传感器网络的传感器节点采集的数据进行异常确认。传感器节点是一个能量有限的装置,当节点的电池被耗尽,该节点将无法使用,从而会影响整个无线传感器网络的信息传输,以至于导致整个网络的瘫痪。在无线传感器网络中,节点感知数据、传输数据、计算数据都需要耗费一定的能量,就要求检测入侵的过程必须节能,而且又可以最大程度的将异常检测出来,我们在设计算法的过程中,综合考虑了能源消耗和剩余能量的两个因素。表 1 中定义了一些分析无线传感器的能量时所使用的参数。

表 1 参数定义

参数	含义
TC	传输过程中能量消耗
CC	计算过程中能量消耗
TA	节点发送的正确数据
RA	节点转发的正确数据
TI	节点发送的错误数据
RI	节点转发的错误数据
RE	节点的剩余能量
RN	WSN 中剩余的节点

在苏等^[4]的文章中提出了能量消耗公式(1),他们利用该公式已计算出每个节点的入侵检测系统的能量消耗:

$$\text{能量消耗} = \sum_{i=1}^n TC_i + CC_i \quad (1)$$

Stresser 等人^[6]用公式(2)提出了无线传感器网络中传输准确率:

$$\text{传输正确率} = \frac{TA+RA}{TA+TI+RA+RI} \quad (2)$$

当攻击发生时,传输错误数据率则为:

$$\text{传输错误率} = \frac{TI+RI}{TA+TI+RA+RI} \quad (3)$$

可以通过公式(4)来计算各个 Sector 中的平均剩余能量:

$$\text{平均剩余能量} = (\sum_{i=1}^n RE_i) / RN \quad (4)$$

4 仿真与结果分析

利用 Matlab7.0 对上述算法进行仿真。假设目标区域面积为 100×100 m,布置了 100 个无线传感器节点,每个传感器节点广播半径为 50 m,初始能量 2 J,发送功率 0.033 W,接收功率 0.026 W。将实验所得到的结果和现有的 ITIDS^[7] 性能作比较分析,得出了以下结论:(1)图 3 中的结果表明在本文所提出的模型中,SM 拥有较强的检测能力,并且整个模型采用了多级联合检测,和 ITIDS 相比,在检测正确率方面有了很大的提高。(2)在本模型中,每一个簇中分成了若干个 Sector,实验表明有 sector 分区的比没有 Sector 分区的情况大大降低了能耗,如图 4 所示。

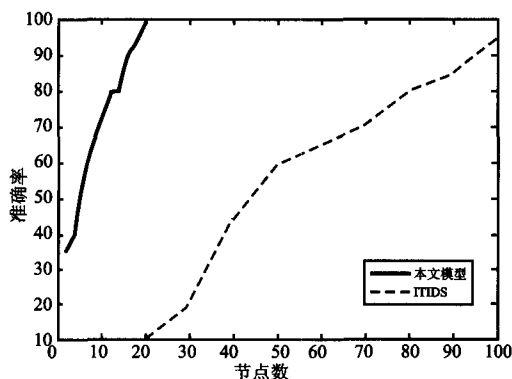


图 3 入侵检测的准确率

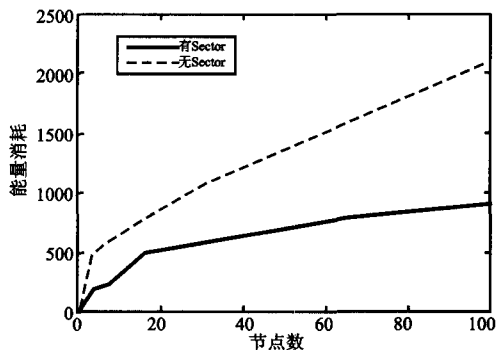


图 4 采用 Sector 前后的能耗对比

我们利用公式(4)在 Metlab7.0 中进行仿真,试图能够得出每一个 Sector 中包含的合适的节点数量,从图 5 中,可以看出,当一个簇内划分了不同的 Sector 后,每一个 Sector 中的节点数目较小如只有

50 个节点时,平均剩余能量下降缓慢,当节点个数增加到 100 和 200 时,随着传输信息数量的增加,平均剩余能量将大幅下降,将很大程度的影响网络的寿命。

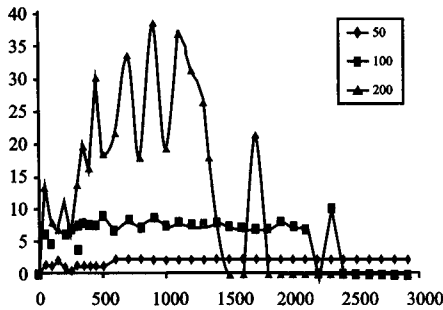


图 5 不同节点数的能量减少

5 结束语

本文提出了一种基于能量均衡的入侵检测系统的网络模型,IDS 分布到重要的节点中进行联合检测,提高检测的准确率^[8],并在传统的分簇基础上提出了分段的概念,降低了传感器节点的能量消耗,延长了网络的生存时间。下一步工作的重点继续优化算法,进行更深入的算法复杂性研究,从而得到更详细的结果。

参考文献:

- [1] Liuf, Chengx, Chend. Insider attacker detection in wireless sensor networks[C] //Proc of the 26th IEEE International Conference on Computer Communications, USA: Washington, 2007:1937-1945.
- [2] Su WT, Chang KM, Kuo YH. eHIP: an energy-efficient hybrid intrusionprohibition system for cluster-based wireless sensor networks[J]. Computer Networks, 2007,51(4):1151-1168.
- [3] Agaha, Das S, Basuk, et al. Intrusion detection in sensor ne-tworks; anon-cooperativegame approach[C] //Proc of the 3rd IEEE International Symposium on Network Computing and Applications, Cambridge, 2004: 343-346.
- [4] Ngai Ech, Liu JC, Lyumr. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks [J]. Computer Communications, 2007, 30(11/12):2353-2364.
- [5] Li Guo-ru, He Jing-sha, Fu Ying-fang. Group-based intrusion de-tection system in wireless sensor networks [J]. Computer Communications, 2008, 31 (18): 4324-4332.
- [6] Mario Strasser, Harald Vogt. Autonomous and distr ibuted node recovery in wireless sensor networks[C]// SASN'06 Proceedings of the fourth ACM worksshop on Security of ad hoc and sensornetworks, ACM New York,2006:113-122.
- [7] 曹峰,刘丽萍,王智. 能量有效的无线传感器网络部署 [J]. 信息与控制,2006,35(2):147-153.
- [8] 王艳丽, 杨顺. 基于能量均衡的无线传感器网络算法的改进[J]. 微计算机信息,2010,8(3):117-119.

作者简介:

彭春燕 女,(1980—),硕士,讲师. 研究方向为计算机网络安全与网络通信。

杨志强 男,(1964—),副教授. 研究方向为嵌入式设计。

(上接第 40 页)

参考文献:

- [1] 罗杰文. Peer to Peer(P2P)综述[EB/OL]. (2012-06-19). <http://download.csdn.net/source/210000>.
- [2] Joseph A Akinwumi. Network coding [D]. Diploma in Computer Science Wolfson College, 2005.
- [3] Ahlswede R, Cai N, Li S Y R, et al. Yeung, Network information flow [J]. IEEE Trans. Inform. Theory, 2000(46):1204-1216.
- [4] Ho T, Medard M, Koetter R, et al. A random linear network coding approach to multicast [J]. IEEE Transactions on Information Theory, 2006 (52): 4413-4430.
- [5] BitTorrent, Inc. BitTorrent web site[EB/OL]. (2012-06-20). <http://www.bittorrent.com>, 2001-2005.
- [6] Ma G, Xu Y, Lin M, et al. A content distribution system based on sparse linear network coding [C]//Proc. 3rd Workshop on Network Coding, Theory, and Applications(NETCOD 2007). USA:California, 2007.
- [7] Cooper C. On the distribution of rank of a random matrix over a finite field [J]. Random Struct. Algorithms, 2000(17):3-4.

作者简介:



张 旋 男,博士研究生. 研究方向为网络编码、闪存编码。