无线传感器网络内部攻击检测方法研究

王良民[1,2] 李 菲[1] 熊书明[1] 张建明[1]
(江苏大学计算机科学与通信工程学院 镇江 212013)[1] (东南大学计算机科学与工程学院 南京 210096)[2]

摘 要 随着无线传感器网络软硬件技术的发展,内部攻击逐渐成为无线传感器网络面临的主要安全威胁之一。综述了内部攻击检测技术的研究,根据攻击检测的对象将检测方法分为攻击行为检测、攻击节点检测和复件攻击检测,并指出了检测悖论、数目占优和中心模式等作为这些检测方法的安全假设制约了方法的性能。同时,概述了现有的关于移动无线传感器网络的攻击检测方法以及移动节点的加入给无线传感器网络解决内部攻击问题带来的变化,在此基础上,讨论了移动节点给内部攻击检测带来的机遇与挑战,指出了相关研究的未来发展方向。

关键词 无线传感器网络,内部攻击,移动节点,攻击检测
中图法分类号 TP393 **文献标识码** A

Research on Detection Methods for Insidious Attack of Wireless Sensor Networks

WANG Liang-min[1,2] LI Fei[1] XIONG Shu-ming[1] ZHANG Jian-ming[1]
(School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)[1]
(School of Computer Science and Technology, Southeast University, Nanjing 210096, China)[2]

Abstract Insidious attack becomes more and more important to the security question of wireless sensor network with the developments of its hardware and software. A comprehensive survey on the detection methods for this attack was presented in this paper. Firstly, these methods were introduced in 3 classes: detection on attack behaviors, compromised nodes and replica nodes. Then it was pointed out that the detection assumption of pre-known attack behavior, outnumbered benign nodes or absolutely secure sink or base station bottlenecks the application of these methods. Furthermore, the issues about attack detection in the mobile wireless sensor networks were introduced, and then the challenges and advantages about mobile nodes over the attack detection for wireless sensor network were discussed. Finally, the possible developments of methods for detecting insidious attack were presented.

Keywords Wireless sensor networks, Insidious attack, Mobile nodes, Attack detection

1 引言

无线传感器网络(Wireless Sensor Networks, WSN)的安全问题是近年来的热点研究领域,尤其是在物联网产业发展的趋势下,作为关键技术的无线传感器网络的软、硬件都有了快速发展,这些发展也给无线传感器网络的安全带来变化。整体来说,随着硬件设计与制造能力的发展,无线节点的能力逐步增强,使得无线传感器网络的安全问题呈现两个方面的变化:一方面,增强后的计算能力和存储能力让公钥密码系统的应用得到开展[1-3],基于密码学的安全结构可以有效防范外部攻击,安全研究的重点延伸到对物理俘虏方式获得的变节节点(Compromised Node)[4-7]及克隆出来的复件节点(Replica Node)[8-11]的检测、撤销(Revoke)与容忍(Tolerant);另一方面,移动节点的造价也大大降低,在无线传感器网络中装备移动节点增强网络功能成为一种趋势[11-13]。然而,移动节点的加入也带来了新的安全威胁[13,14],如移动攻击者(μADV)[14]、移动复件攻击[11]、数据攻击[15]等,使得相应的攻击检测与容忍成为当前研究的难点问题。本文针对无线传感器网络内部攻击进行综述,探讨了移动节点给无线传感器网络内部攻击检测技术带来的挑战,指出了相应研究的发展方向。

2 内部攻击研究的现状

无线传感器网络的内部攻击,是指攻击者已经突破身份认证等依托现代密码技术而设置的第一层安全防护,掌握了相应的安全秘密,并以所拥有的合法身份,从网络内部主动地发起有针对性的、蓄意的、串谋的攻击行为。如图1所示,通常这种盗用的节点身份通过物理俘获(Physical Capture)的方式获得,拥有合法身份的节点可以参与数据采集、数据传输等网络关键服务,从而可以实现对转发数据的篡改、注入和丢弃等;此外,攻击还可以通过复件克隆所获得的合法身份,通过增加复件节点的数目提高内部攻击的能力。

到稿日期:2010-05-25 返修日期:2010-08-31 本文受国家自然科学基金项目(60703115),国家社科基金项目(09CTJ006)资助。
王良民(1977-),男,博士后,副教授,CCF高级会员,主要研究方向为无线传感器网络及安全协议,E-mail:wanglm@ujs.edu.cn;李 菲(1987-),女,硕士生,主要研究方向为无线传感器网络安全;熊书明(1974-),男,博士生,副教授,主要研究方向为无线传感器网络应用技术;张建明(1964-),男,教授,主要研究方向为人工智能。

图1 内部攻击模型

2.1 攻击行为检测

攻击者获得了拥有网络合法身份的节点后，为增加各类攻击效果，往往在运行一些本地协议时采取一些攻击行为，以期获得更多参与网络任务的机会或减少被发现的危险。这些攻击行为包括：节点可以进行 Sink Hole 攻击[16,17]、Sybil 攻击[18-20]、选择转发[21-22]、病毒传播[23]、虫洞[24]、DOS 攻击[25-26]和数据篡改攻击[27-29]等。

最早的攻击检测就是针对这些攻击行为的特征，检测节点是否存在这些特定的攻击行为。通常制定一些规则，选定一些节点监视其它节点，通过运行本地协议以及节点间的协作，判定被检测节点是否具有特定攻击行为的特征性操作，从而判定该节点是否在发起对某个特定类型的攻击。文献[16-29]分别针对特定的攻击行为进行检测，在可以接受的安全代价下均可获得较好的检测结果。

但是此类检测方法主要检测网络中节点是否具有某个特定类型的攻击行为，任何一种单独的方法可证实某个节点是否内部攻击节点。也就是说只有已知某个节点可能采取某个攻击行为才能采取有针对性的特征检测。而事实上，在攻击被检测出来以前，检测者无法知道攻击类型，这就产生了一个“检测悖论”。

2.2 攻击节点检测

针对“检测悖论”一个显然的解决方案是针对所有攻击类型逐一检测，然而这样安全代价太大了。通常，一类攻击的检测需要增加系统15%～25%的能耗，逐一检测累积的能耗将大大缩短网络寿命。因此一些研究人员致力于研究通用的检测方法，这类方法的核心是利用节点间的监视和协作，发现该节点行为是否异常，从而判断是否正常的内部节点（Benign Node）。

最常用的方法是使用信誉系统[30-32]，通过节点对交互事件的记录，采用一定的信誉模型，计算各自信任度；根据节点间的信任度，利用信誉模型在网络的局部或者全网中心求出信誉度，并根据信誉度对节点是变节节点（Compromised Nodes）还是正常节点进行决策判定。Zhang[5]等认为由于网络节点能力的限制以及网络部署在恶意环境中易造成误判，因此信誉系统并不适用于无线传感器网络。于是提出了一种基于图的推理算法作为鉴别变节节点的通用框架，让所有节点进行相互监测，利用检测结果构造观测图（Obverse Graph），在观测图的基础上对节点是否变节进行逻辑判断，相关实验显示其效果非常好。杨峰[7]等提出了一种基于概率包标记的恶意节点追踪方法，其基本策略是通过综合包的数据源头信息发现所有类型攻击的发起节点。

总体来说，这些方法都基于一个假设——正常节点（Benign Node）和变节节点比起来“数目占优”，也就是说假设攻击者只能俘获极少数量的节点，因此无论是从整体还是从局部上，正常节点相对于恶意/变节节点在数目上占优，从而可以通过相互的协作发现少量的破坏者（攻击节点）。如果网络中存在数量上相近或者局部占有的恶意节点，那么会导致上述方法整体失效。

2.3 复件攻击检测

在2005年的 IEEE P&S 大会上，Perrig[8]指出攻击者可以大量复制所俘获节点的身份，从而在局部甚至整体上拥有数量占优的恶意的复件节点（Replica Nodes），这让“数目占优”的安全假设失去了成立的现实条件。

针对 Replica Attack 的复件节点检测[8-10]成为研究的热点。复件节点检测，从本质上来说，都是根据复件攻击的定义——同一个 ID 的大量复制使用——来检测的。根据“同一个身份 ID 的节点不可能出现在多个不同位置”的安全假设来鉴别节点是否为复件攻击节点。但是这种鉴别需要在全局范围内统一排查，因此具有很大的计算量和通信量。为了降低这种检测方法带来的安全代价，通常采用概率抽取的方法让节点汇报，而检测的准确率或者精度通过“生日悖论”[8]、随机概率[9,10]来保证；文献[10]则在概率选取的基础上，利用群部署（Group Deployment）的先验知识进一步降低安全代价并提高检测率。

无论如何，这类检测需要一个在线的基站（Base Station）或者全局的汇聚节点（Sink Node），作为处理问题的中心（我们称之为“中心模式”），所有网络节点的 ID 都要发送到这个中心进行匹配，从而判断是否重复出现。这种模式使得中心的基站成为系统的安全脆弱点，易导致“单点失败”（Sing-point Failure）；同时检测数据增加了网络通信量，使得靠近基站的节点通信能耗大大增加，容易成为决定整个网络性能及寿命的“瓶颈”节点。

3 移动节点带来的发展动态

移动节点的出现则增强了网络节点的能力，扩充了网络的应用范围，同时也改变了网络结构，给网络安全及攻击检测带来了新的变化。

3.1 移动无线传感器网络的结构

目前文献中常见的移动无线传感器网络主要有两类，一类是所有无线传感器节点都可移动；另一类是仅少数节点可以移动。在第一类情形中，移动无线传感器网络和通常讨论的移动 Ad Hoc 网络（MANET：Mobile Ad hoc Netwroks）基本相似，仅仅是节点具有感知能力，而计算能力、通信能力及供电等能力要弱得多。

第二类情形中，移动节点有两类不同的使用方式。一种是移动节点和其他节点对等，仅仅是利用可移动性来实现网络覆盖洞修补[33]、拓扑连通性桥接[34]以及网络能量均衡[35]等。另一类是移动节点作为 Sink 节点，承担起基站功能，每隔一个时间段去访问各个节点，读取感知数据，这种应用中的无线传感器网络中，基站或者 Sink 节点不是一直在线，因而也不能一直以全网可信中心的角色照料整个网络，因此也称为无人照料的无线传感器网络[14,15]（UWSN：Unattended Wireless Sensor Networks）。在这种模式中，仅汇聚节点为移动节点取代，网络成本上的变化并不大，因此这种基于移动节点的无线传感器网络具有广泛的前景。

3.2 移动节点带来的变化

首先讨论所有节点均为移动节点时的内部攻击检测，由于此时网络极其类似 MANET，其关于节点攻击行为及变节节点的检测与 MANET[36]近乎一致。而复件节点检测在 MANET 中很少涉及到，这一问题在 Infocom2009 得到了重

视。由于节点移动，因此以“同一个身份 ID 的节点不可能出现在多个不同位置”的安全假设来检测复件攻击已经行不通了。Jun-Won[11]提出使用 SQRT 的方法，以移动速度不能超过系统设置的最大值为检测标准进行检测。但是，上述方法依然是基于“中心模式”的。

UWSN 中同时存在两类节点：移动节点和静态节点，网络结构非常新颖，给其安全性带来了很多新的问题，攻击的种类及检测方法均有很大变化。首先移动节点作为 Sink 节点，承担起基站功能，每隔一个时间段去访问各个节点，读取感知数据，移动的汇聚节点即使依然使用“中心模式”来处理检测，但因邻居节点不再固定，也使得该模式下的“瓶颈节点”现象并不严重；同时移动节点周期性访问网络，也可周期性与用户交互，因此单点失败（Single-point Failure）问题也可得到避免。此外，如文献 Conti[37]所指出的那样，移动的 Sink 节点还可以在访问节点时，对被俘获的变节节点进行密钥更新甚至重新进行程序写入。

然而，移动节点的加入提供了安全防卫能力，同时也因为 Sink 节点的缺位使得 UWSN 中出现新的攻击类别。Ma[14]提出了一种移动攻击者模型（μADV：Mobile Adversary），如图 2 所示，由于移动 Sink 周期性收集数据，移动攻击者可以在 Sink 两次巡视的时间空隙里，在传感器网络部署的区域内自由移动，可选择任意节点进行物理俘获或者损害。Ma 在文献[14]中指出，现有的无线传感器网络的攻击防范方式对这种新的 μADV 攻击均无效，这种攻击在一定程度上是能力增强型的物理俘获攻，可随意选择节点进行俘获；也可视为变节的 Sink 节点，可以获取、改变任何静态节点的状态及信息。

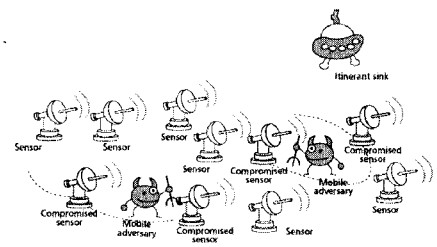

图 2　移动攻击者（μADV）模型

针对 μADV 攻击，目前没有很好的检测方法，当前研究以防守为主。Pietro[13]提出了一种基于加密的方法用以提高数据的可生存性，而在文献[15]中则分析了在 UWSN 内部将敏感数据在节点间转移的 DN、MO 和 KM 方法，以避免被 μADV 攻击。Oligeri[38]针对防止物理俘获的攻击者反动虚假数据注入攻击，提出了基于节点协同的弹性安全加密方法。总体来说，对 μAdv 攻击，目前尚无很好的检测方法。

结束语　前述 2 节讨论了各类型攻击检测方法，指出有针对有移动节点的无线传感器网络和无移动节点的无线传感器网络两类，存在检测攻击行为、检测变节节点及检测复件节点 3 种类型，而不同类型又分别使用了“已知攻击”、“数据占优”和“中心模式”3 种安全假设，可能存在“检测悖论”、“瓶颈节点”、“单点失败”、“安全代价”等四方面的主要问题。表 1 对此进行了归纳，其中“/”表示无相应数据。

由表 1 可以清楚地看到，没有移动节点的无线传感器网络中的内部攻击方法均依赖于一个或多个安全假设，存在无法克服的主要问题；而移动节点给克服这些实际问题带来新的可能，但关于移动攻击，尚没有更好的解决方法。

表 1　典型攻击检测方法缺陷

检测类型		无移动节点			有移动节点		
		攻击行为	攻击节点	复件节点	攻击节点	复件节点	移动攻击者
主要问题	检测悖论	是	无	是	无	是	/
	数目占优	是	是	否	是	否	/
	中心模式	部分	部分	是	否	否	/
	瓶颈节点	有	有	有	无	无	/
	单点失败	部分	部分	有	无	无	/
	安全代价	小	中	较大	/	大	/

为此，我们认为，在未来关于无线传感器网络内部攻击的研究，必然有以下几个方面的发展趋势：

1）移动节点的有效使用：移动节点给攻击检测问题的彻底解决带来了很大机会，如何有效地使用这些契机，将是该领域的研究重点之一；

2）异质节点之间的协作检测：无论是针对变节节点检测，还是针对移动节点防守的策略，都依赖于节点间的监视与合作。移动无线传感器网络中，不仅沿袭 MANET、传感器网络中的协作机制，如何开发移动节点和普通节点之间的协作，发挥更大的效益，也是一个值得关注的研究方向；

3）μADV 攻击的检测和应对措施：移动攻击者的强大破坏能力，让当前相关研究停在被动的安全防范或者主动的容忍阶段，利用 Sink 的移动性及与静态节点的合作，借鉴 MANET 中的攻击检测机制，将是解决该类问题的主要途径。

参 考 文 献

[1] Liu An, Ning Peng. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks[C]// Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN 2008). SPOTS Track, April 2008: 245-256

[2] Wang Haodong, Tan Bosheng, et al. Comparing Symmetric-key and Public-key Based Security Schemes in Sensor Networks: A Case Study of User Access Control[C]// IEEE ICDCS. 2008: 11-18

[3] Wang Ronghua, Du Wenliang, et al. ShortPK: A short-term public key scheme for broadcast authentication in sensor networks [J]. ACM Transactions on Sensor Networks, 2009, 6(1): 1-29

[4] Zhang Yanchao, Liu Wei, et al. Location-based compromise-tolerant security mechanisms for wireless sensor networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24 (2): 247-260

[5] Zhang Qinghua, Yu Ting, et al. A Framework for Identifying Compromised Nodes in Wireless Sensor Networks [J]. ACM Transactions in Information and Systems Security (TISSEC), 2008, 11(3): 1-37

[6] Curiac D, Banias O, et al. Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique[C]// International Conference on Networking and Services (ICNS '07). 2007: 83

[7] 杨峰，周学海，等. 无线传感器网络恶意节点溯源追踪方法研究[J]. 电子学报，2009，37(1)：202-206

[8] Parno B, Perrig A, Gligor D. Distributed Detection of Node Replication Attacks in Sensor Networks[C]// IEEE Symposium on Security and Privacy. May 2005: 49-63

（下转第 129 页）

and aggregation in large wireless sensor networks[C]// Vehicular Technology Conference. Vol. 7,2004:4602-4606
[16] Braginsky D, Estrin D. Rumor routing algorithm for sensor networks[C]// Proc. of the 1st Workshop on Sensor Networks and Applications. New York: ACM Press,2002:1-12
[17] Das Y H S, Pucha H. Performance comparison of scalable location services for geographic ad hoc routing[C]//Proceedings of IEEE INFOCOM 2005. Miami, FL, March 2005:1228-1239
[18] 石高涛,廖明宏.一种大规模传感器网络节能数据发布协议[J].软件学报,2006,17(8):1785-1795
[19] Lee Yu Won, Lee Ki Yong, Kim Myoung Ho. Energy-efficient Multiple Query Optimization for Wireless Sensor Networks[C]// Third International Conference on Sensor Technologies and Applications. Athens, Glyfada,2009:531-538
[20] Lu Ke-zhong, Lin Xiao-hui. A Multiple Trees-based Data Dissemination Scheme in Wireless Sensor Networks[C]// WRI World Congress on Computer Science and Information Engineering. Los Angeles, CA,2009:1-4
[21] Lee Euisin, Park Soochang, Lee Donghun, et al. A Predictable Mobility-based Communication Paradigm for Wireless Sensor Networks[C]// Asia-Pacific Conference on Communications. Bangkok,2007:373-376
[22] Shen Chien-chung, Srisathapornphat C, Jaikaeo C. Sensor Information Networking Architecture and Applications[J]. IEEE Personel Communication Magazine,2001,8(4):52-59
[23] Ota K, Dong Mian-xiong, Li Xiao-lin. TinyBee: Mobile-Agent-Based Data Gathering System in Wireless Sensor Networks[C]// IEEE International Conference on Networking, Architecture, and Storage. Human, China,2009:24-31

(上接第 99 页)

[9] Conti M, Pietro D, et al. A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks[C]// ACM Mobihoc. 2007:80-89
[10] Ho Jun-won, Liu Donggang, et al. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks[J]. Ad Hoc Networks,2009(7):1476-1488
[11] Ho Jun-Wwn, Wright M, Sajal D. Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis[C]//IEEE INFOCOM 2009
[12] Munir A, Ren Biao, et al. Mobile Wireless Sensor Network: Architecture and Enabling Technologies for Ubiquitous Computing [C]// 21st International Conference on Advanced Information Networking and Applications Workshops. AINAW '07
[13] Pietro R, Mancini L, et al. Playing hide-and-seek with a focused mobile adversary in unattended wireless sensor networks[J]. Ad Hoc Networks,2009,7(8):1463-1475
[14] Ma D, Soriente C, Tsudik G. New adversary and new threats: security in unattended sensor networks[J]. IEEE Network,2009, 23(2):43-48
[15] Pietro R, Mancini L, et al. Data Security in Unattended Wireless Sensor Networks[J]. IEEE Trans. Computers,2009,58(11): 1500-1511
[16] Ngai E, Liu J, et al. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks[J]. Computer Communications,2007,30(11/12):2353-2364
[17] 庞辽军,李慧贤,等. Directed Diffusion 协议的安全性分析及改进[J]. 系统工程与电子技术,2009,31(9):135-138
[18] Zhang Qinghua, Wang Pan, et al. Defending against Sybil Attacks in Sensor Networks[C]// ICDCS Workshops. 2005:185-191
[19] 张建明,余群,王良民. 基于地理信息的传感器网络 Sybil 攻击检测方法[J]. 系统仿真学报,2008,20(1):259-264
[20] 冯涛,马建峰. 防御无线传感器网络 Sybil 攻击的新方法[J]. 通信学报,2008,29(6):13-19
[21] 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(09):1542-1552
[22] 王新胜,詹永照,王良民. 无线传感器网络中的选择转发攻击检测[J]. 江苏大学学报,2009
[23] 张书奎,崔志明,等. 传感器网络病毒感染传播局域控制研究[J]. 电子学报,2009,37(04):877-883
[24] 陈鸿龙,李鸿斌,王智. 基于 TDoA 测距的传感器网络安全定位研究[J]. 通信学报,2008,29(8):11-21
[25] 曹晓梅,韩志杰,陈贵海. 基于流量预测的传感器网络拒绝服务攻击检测方案[J]. 计算机学报,2007,30(10):1798-1805
[26] Raymond D, Midkiff F. Denial of Service in Wireless Sensor Network: Attacks and Defenses[J]. IEEE Pervasive Computing, 2008,7(1):74-81
[27] Chan Haowen, Perrig A, Song Xiaodong. Secure hierarchical in-network aggregation in sensor networks[C]// ACM Conference on Computer and Communications Security. 2006:278-287
[28] Zhu Sencun, Setia S, et al. Interleaved hop-by-hop authentication against false data injection attacks in sensor networks[J]. ACM Transactions on Sensor Networks,2007,3(3):14:1-14:33
[29] Chan Haowen, Adrian P. Efficient security primitives derived from a secure aggregation algorithm[C]// ACM Conference on Computer and Communications Security. 2008:521-534
[30] 荆琦,唐礼勇,陈钟. 无线传感器网络中的信任管理[J]. 软件学报,2008,19(7):1716-1730
[31] 杨光,印桂生,杨武,等. 无线传感器网络基于节点行为的信誉评测模型[J]. 通信学报,2009,30(12):18-26
[32] Zahariadis T, Leligou H, et al. Mobile Networks Trust management in wireless sensor networks [J]. European Transactions on Telecommunications, Apr. 2010
[33] Chang Wuyu, Chen E, et al. Deploying Mobile Nodes to Connect Wireless Sensor Networks Using Novel Algorithms[C]// Proceedings of the International Conference on Wireless Algorithms. Systems and Applications table of contents. 2007:199-204
[34] Zhang Hui, Lei Lin. The Study on Dynamic Topology Structure of Wireless Sensor Networks[C]// Second International Conference on Computer Modeling and Simulation. 2010,4:127-129
[35] Nguyen L, Defago X, et al. An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks[C]// 5th IEEE International Symposium on Wireless Communication Systems(ISWCS 2008). Reykjavik, Iceland, October 2008:568-572
[36] Bajwa S. A Survey on Intrusion Detection Systems in Manets [R]. Pakistan Air Force-Karachi Institute of Economics and Technology. Juan. 2010
[37] Mauro C, Pietro R, et al. Mobility and Cooperation to Thwart Node Capture Attacks in MANETs[J]. EURASIP Journal on Wireless Communications and Networking, Article ID 945943, 2009:13
[38] Oligeri G, Pietro R, et al. Intrusion Resilience in Mobile Unattended WSNs[C]//IEEE Infocom2010