面向主动防御的无线传感器网络安全框架

高建斌[1,2],娄渊胜[2]
(1. 海军 91669 部队,海南 海口 571100;
2. 河海大学 计算机与信息学院,江苏 南京 210098)

摘 要:无线传感器网络的部署和应用受通信信道开放、动态拓扑和节点资源严格受限等因素制约,其安全性面临着巨大的威胁和挑战。文中在分析了现有 WSN 安全防御的特点和难点的基础上,针对目前无线传感器网络安全技术处于被动防守、扩展性差、动态防护能力不强的问题,分析并设计了面向主动防御的 WSN 安全框架。通过各模块协同联动,运用“预防->入侵探测(预测)->防御响应->动态加固”多重手段,提供了一个全方位多层次的主动防御安防模式。

关键词:无线传感器网络;主动防御;入侵检测
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)09-0228-04

Security Framework Oriented Active Defense for Wireless Sensor Network

GAO Jian-bin[1,2], LOU Yuan-sheng[2]
(1. China Navy Serial No. 91669, Haikou 571100, China;
2. College of Computer & Information, Hohai University, Nanjing 210098, China)

Abstract: Due to completely open of communication channel, limitation of dynamic topology and node resources etc, the deployment and application of wireless sensor network faces enormous threats and challenges in its security. The existing wireless sensor network security system has poor scalability and protection capability, in order to solve these problems, it analyzes the characteristics and difficulties of the network defense. Then undertakes analysis and design the security framework oriented active defense for WSN. Through collaborative interaction of modules, the framework in this paper recycles multiple means including prevention, intrusion detection, defense response and dynamic consolidation to provide a comprehensive multi-layered security model of active defense.

Key words: wireless sensor network; active defense; intrusion detection system

0 引 言

无线传感器网络[1](WSN)是信息感知和采集手段的一场革命,给人类的生活和生产带来了深远的影响。但是,受通信信道完全开放、缺乏固定基础设施、节点资源严格受限等因素影响制约, WSN 的安全面临巨大的威胁和挑战。

1 相关的研究

目前,相关机构围绕无线传感器网络安全的研究不断发展,并取得了一些有价值的成果。主要在以下四个方面:

(1)WSN 基本安全技术方面[2~4];

(2)WSN 密钥管理方面[5];

(3)WSN 安全路由方面[6];

(4)WSN 服务组件安全方面[7~9]。

以上四个方面分别针对各自的安全重点都取得了一定的安全效果。但安全防范措施都是静态预置的,扩展性和自适应性不好,不具备防御新型威胁的能力。这种传统的“破坏-加固-再破坏”的被动解决方式对 WSN 可能会造成网络瘫痪、应用完全失效等灾难性的后果。因此,立足现有安全基础设施,探索一种面向未来的弹性的主动安全防护机制,是本研究要解决的问题。

2 面向主动防御的 WSN 安全框架设计

2.1 设计目标与原理

主动防御指在网络遭受攻击以前,通过网络节点相互合作,合理采用包括预防、检测、响应等多个安防体系,动态主动防御,保证 WSN 的安全运行。因此,相应的设计目标为:

收稿日期:2012-02-05;**修回日期**:2012-05-10
基金项目:国家高技术“863”发展计划项目(2007AA01Z178)
作者简介:高建斌(1976-),男,硕士,主要研究方向为无线传感器网络;娄渊胜,博士,副教授,CCF 会员,主要研究方向为分布式计算。

(1)审计信息本地化,资源消耗最小化;

(2)多层防御体系;

(3)各安全组件实现互动;

(4)防御能力动态提升。

2.2　安全框架设计

面向主动防御的 WSN 安全框架如图 1 所示。该框架分为 5 大模块,安全预防模块、入侵检测模块、预测模块、防御响应模块和动态安全加固模块。根据需要部署在网络的不同节点上,其体系结构可以较好地抵御已知攻击和未知攻击。

安全预防模块在物理层负责数据通信的机密性、完整性和访问控制,增强通信抗干扰性,防止物理俘获的抗毁性。在网络层保证路由的安全性,在应用层提供安全定位、安全数据融合及安全时钟同步等保障。入侵检测模块的功能是对入侵攻击活动进行检测,对已知攻击触发响应模块进行有效阻击,对未知异常情况发出告警,提取攻击特征和日志,通知管理中心。预测模块主要提供对入侵攻击等异动情况的预警,为防御响应赢得时间。响应模块依据攻击的性质、种类,实施适当的安全防护和反击。动态安全加固模块负责系统安全漏洞的修补、入侵检测规则库的更新和软件 Bug 的修复,动态提升 WSN 的安全防御能力。

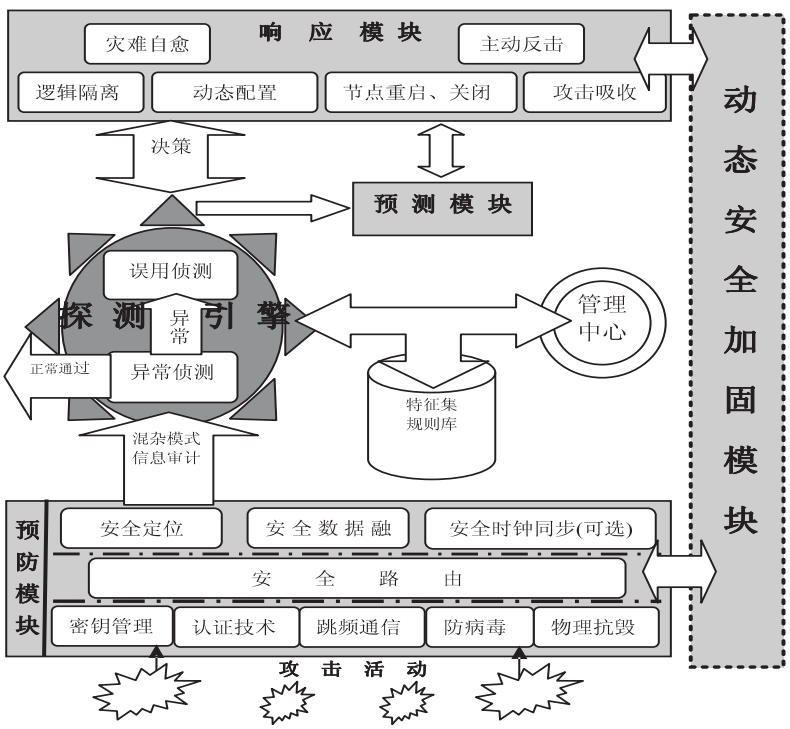

图 1　面向主动防御的 WSN 安全框架

安全框架中,安全预防模块是安全保障的基础,是整个安全体系的支撑和依托。入侵检测模块是框架的核心,是后续预测模块、防御响应模块工作的前提。动态安全加固模块是主动防御框架的灵魂,是 WSN 安全能力动态提升的关键。

通过多个安全模块的协同联动,循环运用“预防->入侵探测(预测)->防御响应->动态加固”多重手段的主动防御模式,并结合传统的被动防御方法,为 WSN 提供全方位多层次的安全防护。

3　框架的运行机制和工作流程

框架除了在标准的网络层工作,还能够在物理层、应用层操作处理,并且能区分攻击和正常事件。各模块运行机制如下:

1)安全预防模块。安全预防模块是整个安全框架的基础,对其它模块和整个 WSN 系统安全起到支撑的作用。密钥管理作为确保无线传感器网络安全的第一道屏障,其目标是为安全的数据传输、安全路由、组播多播等提供底层的安全支持,从而有效地防御外部攻击。密钥管理包括密钥的生成、存储、分配、使用、更新、销毁等。对称密钥体制加密、解密速度快,密钥长度短,计算、通信、存储等开销小,比较适用于传感器网络。

针对物理俘获和破坏,需要 WSN 采用抗毁保护机制,如采用坚固的外壳保护、伪装隐蔽部署或者增加物理损害感知机制。节点能够根据其收发资料包的情况、外部环境的变化和一些敏感信号的变化,判断是否遭受物理侵犯,自动销毁敏感数据。

对于通信信号干扰,采用宽带和跳频的方法抵制单频点偶发性攻击,或者主动转换通信模式如备用的光通信和红外线等通信方式对抗全频段持续拥塞攻击。也可以降低自身工作占空比,既节省能量消耗,又避免了干扰。另外,安全路由的选择、相关应用的安全以及防病毒等都应该在网络设计和部署中做好。

2)入侵检测模块。入侵检测模块作为确保 WSN 安全的第二道屏障,其目标是有效地检测传感器网络中的伪造和篡改消息攻击、wormhole 攻击、Hello 消息洪泛攻击等异常行为,有效地防御内部攻击,进一步提高无线传感器网络的安全性。

具体运行机制:探测引擎通过把异常侦测、误用侦测有机地结合起来,采用混合型入侵侦测方案,首先通过异常侦测过滤大量的通信包,使系统要处理的信息量下降,便于后续误用侦测模型继续检测。如果信息包正常则直接通过,发现异动情况时则交给误用侦测子系统进一步检查,通过与特征集和规则库交互,对于已知的攻击形式,明确入侵的性质、

种类,检测算法自动触发响应模块阻止攻击。对于未知的可疑事件,则发出告警,主动提取攻击特征,并通知管理中心。

3)防御响应模块。对网络攻击进行适当响应是主动防御与传统防御的本质区别。防御响应是主动防御技术在网络入侵防护中主动性的具体体现,用来对检测到的攻击事件进行处理。防御响应技术主要有:

逻辑隔离,是在检测出恶意攻击节点后,通过技术手段将恶意节点与其它网络节点在逻辑上进行隔离、断开,使其不再参与正常的数据采集、数据转发等网络活动。一般采用的方法有清除相关节点的路由、降低节点的信任度、优先级等,使恶意节点暂时隔离或者长期失效。

攻击吸收和攻击反击是防御响应模块在入侵响应处理上的两种不同的方式。前者是当系统检测到攻击后,通过技术定位攻击的来源和具体的攻击目标,然后使用蜜罐诱导攻击者到假的目标,达到中止其继续危害网络安全的目的。后者则是利用各种网络攻击手段对网络入侵者进行攻击,迫使其停止攻击破坏行为。

节点重新启动、关闭则是另一种形式的主动阻断攻击、破坏的方法。此外,还有入侵取证、灾难自愈等相关辅助技术手段。

4)预测模块。对网络攻击的预测功能是主动防御的显著特征,在攻击发生前预测攻击信息,取得系统防护的主动权,是主动防御的重要环节。与后期的检测不同,入侵预测在攻击发生前预测将要发生的入侵和安全趋势,为系统安全防护和响应提供线索,争取时间。当前入侵预测主要采用以下三种不同的机制:基于流量检测的预测机制;基于安全事件的预测方法;基于智能模糊推理预测的方法。

5)动态安全加固模块。动态安全加固模块是整个网络安全防护能力提升的关键。依托部署的网络硬件资源和节点软件更新机制,通过无线网络升级的方式,修正软件 BUG、系统安全漏洞,增加对新生攻击的对抗能力,从而保障网络的安全性和可用性。

WSN 重编程[10,11]是动态安全加固模块的主要技术手段。WSN 重编程的设计包括 BootLoader 和代码分发两部分,BootLoader 是一块独立的代码程序,用来确保传感器节点每次启动都被执行。代码分发保证当管理员需要更新节点软件时,能够将代码镜像完整地分发到每个传感器节点,同时还要满足低存储、低能耗和实时性的要求。一般采用增量型代码[10]分发模式。

网络管理[12],是动态安全加固的另一种技术。通过无线交互式管理,使 WSN 具有较高的效率和可靠的工作性能,管理过程通常包括数据收集处理、分析和网络控制等。WSN 网络管理必须进行轻量级操作,同时健壮性和适应性要强,应具有一定的配置和修复、控制的功能。如射频能量的控制、通信模式的转换等。

WSN 安全框架工作流程如图 2 所示。节点工作在混杂模式,对周围的通信进行监听和安全审计。攻击等恶意活动,如果突破了安全预防模块的防线,入侵检测模块自动启动,首先进行异常侦测,如果安全评估是正常的,则相关信息直接通过;否则,有异动情况时继续交由误用侦测子系统进一步检查,通过与规则库交互,对于已知的攻击形式,明确入侵的性质、种类,检测算法自动触发防御响应模块阻止攻击。对于未知的可疑事件,则发出告警,提取攻击特征和日志,通知管理中心。管理中心依托交互式管理工具和节点软件动态更新机制,通过无线网络重编程升级的方式,修正软件 BUG、系统安全漏洞,增加对新生攻击的对抗能力,

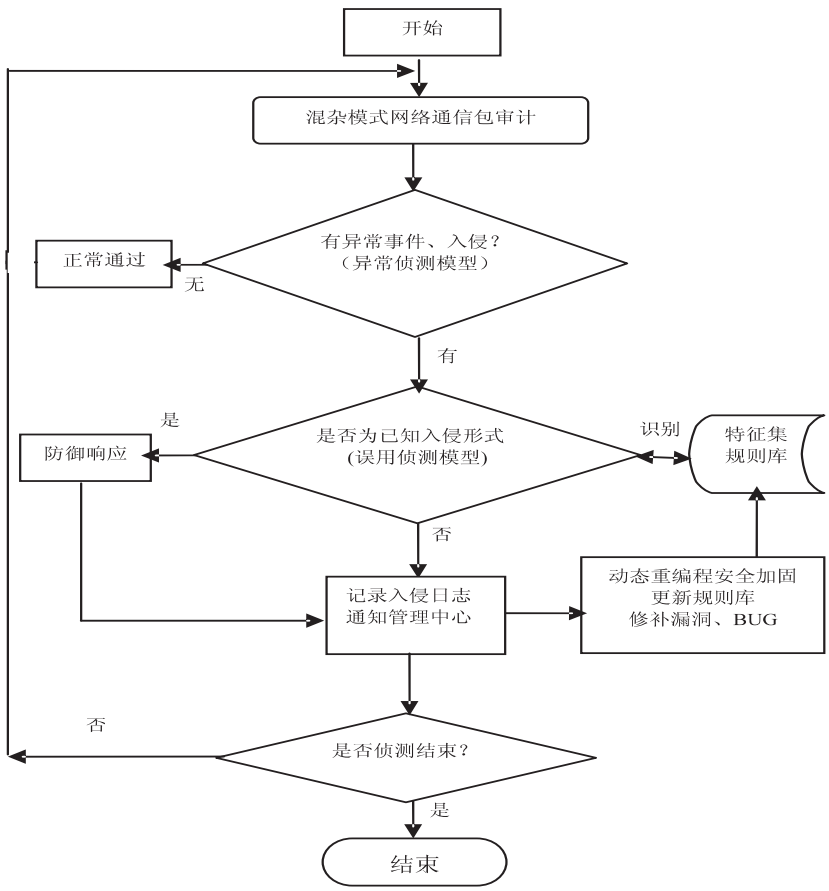

图 2 安全框架工作流程

保障网络的安全性。

4　结束语

针对目前无线传感器网络安全技术处于静态预置安全措施被动防守、动态防护能力不强的问题,文中设计了面向主动防御的 WSN 安全框架,给出了面向未来的弹性的主动防御安防模式。今后研究的重点是进一步强化入侵预测和响应模块的细节。

参考文献:

[1] 孙利民. 无线传感器网络[M]. 北京:清华大学出版社,2005.

[2] Perrig A,Szewczy R. SPINS:Security Protocols for Sensor Networks[C]//Mobile Computing and Networking. Rome,Italy:[s. n.],2001.

[3] Karlof C,Sastry N,Wagner D. TinySec:A Link Layer Security Architecture for Wireless Sensor Networks[C]//Proc. of the 2nd ACM Conference on Embedded Networked Sensor Systems. Baltimore,USA:ACM,2004.

[4] Park T,Shin K G. LiSP:A Lightweight Security Protocol for Wireless Sensor Networks[J]. ACM Transactions on Embedded Computing Systems,2004,3(3):86-88.

[5] 苏　忠,林　闯,封富君,等. 无线传感器网络密钥管理的方案和协议[J]. Journal of Software,2007,18(5):1219-1221.

[6] 李少衡,张　琨,王翠荣. 无线传感器网络中的一种安全高效的路由协议[J]. 北京化工大学学报,2007,34(Sup):117-118.

[7] Lazos U,Poovendran R. SeRLoc: robust localization for wireless sensor network[J]. ACM Transactions on Sensor Networks,2005,1(1):73-100.

[8] Elson J,Girod L,Estrin D. Fine Grained Network Time Synchronization Using Reference Broadcasts[C]//Operating Systems Design and Implementation. New York,NY, USA:ACM,2002.

[9] Przydatek B,Song D X,Perrig A. SIA: secure information aggregation in sensor networks[J]. Special Issue on Security of Ad-hoc and Sensor Networks,2007,15(1):69-102.

[10] Deng J,Han R,Mishra S. Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks[C]//Proceedings of the 5th international conference on information processing in sensor networks. New York,NY,USA:ACM,2006.

[11] Jeong J,Culler D. Incremental Network Programming for Wireless Sensors[C]//Proc. of the First IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks. Santa Clara,CA,USA:[s. n.],2004.

[12] Tirkawi F,Fischer S. Remote Interaction Tool for Wireless Sensor Networks[C]//3rd IEEE International Symposium on Wireless Pervasive Computing. [s. l.]:[s. n.],2008.

(上接第 227 页)

保存方法。文中提出了 0.5 级环方法,并给出了写入环境;0.5 级环的可信度依赖于操作系统的安全,文中对操作系统本身如何抗病毒也进行了设想;实现 0.5 级环的最佳方法应是在设计操作系统时就将其考虑,使它成为操作系统的一个基本功能。顺便指出,2.3 节所讨论的原始文件若已在磁盘或 Flash 存储器中,在一定的条件下,是不需要回写的。

在进行病毒检测的研究同时,笔者也注意到综合化和智能化的杀毒技术的进展,这是一个值得研究的重要方向。

参考文献:

[1] 刘巍伟,石　勇,郭　煜,等. 一种基于综合行为特征的恶意代码识别方法[J]. 电子学报,2009,37(4): 696-700.

[2] 左黎明,刘二根,徐保根,等. 恶意代码族群特征提取与分析技术[J]. 华中科技大学学报(自然科学版), 2010,38(4):46-49.

[3] 刘　磊,邵　堃. 恶意代码行为分析技术研究与应用[D]. 合肥:合肥工业大学,2009.

[4] Geer D. Behavior-based security become the main-stream of network security[J]. Computer,2006,39(3):14-17.

[5] 李　明,范明钰. 基于网络行为分析的未知恶意代码检测系统的研究与实现[D]. 成都:电子科技大学,2009.

[6] 周　冲,张琼声. 操作系统病毒防御策略的研究[D]. 北京:中国石油大学,2009.

[7] Christodorescu M,Jha S. Static analysis of execut-ables to detect malicious patterns[C] //Proceedings of the 12th USENIX Security Symposium. [s. l.]:[s. n.],2003:169-186.

[8] Karnik A,Goswami S,Guha R. Detecting obfuscated viru-ses using cosine similarity analysis[C]//Proceedings of the 1st Asia International Conference on Modeling and Simulation. Phuket Thailand:[s. n.],2007:165-170.

[9] 张波云,殷建平,唐文胜,等. 基于模糊模式识别的未知病毒检测[J]. 计算机应用,2005,25(9):2050-2053.

[10] 王　维,张鹏涛,谭　营,等. 一种基于人工免疫和代码相关性的计算机病毒特征提取方法[J]. 计算机学报,2011,34(2):204-215.

[11] 洪群业,唐学文. 基于分类的未知 PE 病毒检测技术的研究[D]. 重庆:重庆大学,2010.

[12] 张　勇,张卫民,欧庆于. 基于主动学习的计算机病毒检测方法研究[J]. 计算机与数字工程,2011,39(11):89-93.

[13] 庄蔚蔚,姜青山. 基于增量学习关联分类规则的病毒检测方法研究[D]. 厦门:厦门大学,2009.