无线传感器网络中的跨层安全设计*

杨光松[1], 陈朝阳[1], 肖明波[2]
(1.集美大学 信息工程学院, 福建 厦门 361021; 2.厦门大学 通信工程系, 福建 厦门 361005)

摘　要: 无线传感器网络(WSNs)发展迅速, 可广泛应用于军事、工业及科学等领域。传感器网络在无线信道中工作, 其节点有限的能源、计算能力、存储能力使得其面临着严重的安全问题。已提出的许多安全方法都基于分层设计的概念。分析了分层安全设计的局限性, 回顾了现存的WSNs的安全设计方案, 提出了一些新的跨层解决办法, 并指出了传感器网络中跨层安全的研究方向。

关键词: 无线传感器网络; 安全; 跨层
中图分类号: TP393; TP311.56　　文献标识码: A　　文章编号: 1000-9787(2007)02-0015-04

Design of cross-layer security for wireless sensor networks*

YANG Guang-song[1], CHEN Chao-yang[1], XIAO Ming-bo[2]
(1. School of Information Engineering, Jimei University, Xiamen 361021, China;
2. Department of Communication Engineering, Xiamen University, Xiamen 361005, China)

Abstract: Wireless sensor networks(WSNs) are developing rapidly, it will be employed in a wide variety of applications ranging from military, industrial and social. Due to their constraints in computation, memory, and power resources, security is a challenge in these networks. Many security methods of WSNs based on the concept of layered-design have the limit. the state of art security design method of WSNs is overviewed, several new cross-layer solve methods are proposed, and the research direction of cross-layer design for the security of WSNs is point out.

Key words: wireless sensor networks(WSNs); security; cross-layer

0 引　言

近年来, 计算机、通信和传感器技术的交叉应用, 产生了无线传感器网络(wireless sensor networsks, WSNs)。WSNs由许多低价、低功耗、多功能、小尺寸的传感节点构成, 以智能的方式完成特定的监测任务, 如, 传感、数据处理、通信等, 比传统的网络有更多的功能[1,2], 因而, 在军事、环境监测、医疗、智能建筑及其他商业领域等多方面得到广泛应用。

WSNs引起了人们越来越多的兴趣, 目前, 对于WSNs的研究主要集中在能量效率[3]、网络协议[4]、分布式数据库等, 但对于安全鲜有涉及[5]。由于WSNs部署在无人值守的外部环境中, 需要保证数据安全和节点容错来防止敌方或者恶意分子对系统的利用和破坏, 并且, 要能够对节点进行认证, 保证从网络中收到正确的信息, 以提高网络的可靠性, 因此, WSNs中安全十分重要。

WSNs中, 各协议层有不同的安全方法, 传统的安全设计主要采用分层的方法, 不能较好地解决WSNs中的安全问题。最近, 跨层的安全方法逐渐成为WSNs中的研究热点, 跨层设计有可能在安全需求及网络性能上有一个良好的折中。

1 WSNs的安全特征

WSNs中安全问题十分重要, 要求各传感节点能被网络认证, 保证来自网络的数据正确性; 网络能避免受到攻击, 并保证数据的安全, 此外, WSNs还有以下的安全需求[6]:

a. 机密性(Confidentiality);
b. 认证(Authentication);
c. 完整性(Integrity);
d. 新颖性(Freshness);
e. 安全分组管理(Secure Group Management);
f. 可用性(Availability)。

WSNs由于其特殊的网络结构, 还存在许多弱点, 使其很容易受到攻击者的破坏。

首先, WSNs工作在无线信道中, 攻击者可轻易在该网

收稿日期: 2006-08-21
* 基金项目: 福建省自然科学基金资助项目(A00440004)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

络的任务域里监听信道; 无线收发器的接收距离短, 容易受到强功率的干扰; 多跳路由使恶意节点容易侵入。无中心、动态拓朴也使其安全操作不易。

其次, WSNs硬件方面的设计限制了实施复杂加密机制的可能性: 有限的不可再生的能源、计算能力较差的 CPU和容量较低的内存和闪存, 不可能在其上实施功能强大的加密算法。

此外, 尽管人们在 AdHoc网络的安全问题作了许多工作[7], 但不能直接应用于 WSNs。与一般的 AdHoc网络相比, WSNs还有自己独特的特点, 使其安全性能进一步受限, 主要表现在[8]:

1)网络规模更加庞大: 与现有的 AdHoc网络相比, WSNs有更多数量的节点, 这样, 导致通信负荷增加, 通信链路增多, 因而, 受攻击的概率增加。而现有的安全方法对节点数量有限制[9], 如果超出这一数量, 则会失效。

2)节点在目标区域密集分布: 传感节点更容易出错, 这些节点主要使用广播通信, 而 AdHoc网络倾向于点对点通信, 因而, 其安全负荷较大。

3)节点更容易失效: WSNs能量受限, 微处理器处理能力较低、收发距离短, 这些决定了对 WSNs安全协议设计要相对简单。攻击者正是利用这一点, 通过操纵数据或协议报文, 或者连续向某一邻居发送路由或数据请求报文, 使该邻居不停的分配资源以维持一个新的连接, 在更大范围内对 WSNs进行破坏或使全网瘫痪。

4)节点没有全网统一的身份认证: 不良节点很容易冒充进入, 因而, 增加了危险性。使用一个公共密钥简单地对链路层加密和验证, 可以防止多数外部人员对 WSNs路由选择协议的攻击。但在内部人员出现的场合或在被损害的节点处, 链路层安全机制使用一个公共密钥是完全无效的。需要提供更复杂的防御机制。

2 分层安全方法的局限性

WSNs中分布着大量网络节点, 设计时要求低价和低功率, 因而其网络资源有限, 如, 缓存、计算能力有限, 且要求用更有效的方法来节省功率。由于数量大, 且有分布特征, 要求其协议和算法可升级。最近, 提出了许多安全算法[10~12], 这些解决方案针对某一层的攻击而言, 不能有效解决 WSNs的安全问题。主要表现在以下方面:

1)导致冗余的安全提供

通常, 在 WSNs网络协议栈中的每一层, 有可能提供不同的安全服务。当 WSNs受到同一种攻击时, 原始数据从最高一层开始, 进行逐层处理。部分数据分组会在通过不同层时, 进行不同的安全操作, 导致提供多余的安全服务。

WSNs也受到多种攻击时, 对抗这些攻击的每种安全机制都要消耗资源 (如, 电池、缓存、链路带宽等), 如果在每个节点的每一层都提供大量的安全服务, 将会造成系统资源的浪费, 从而减少整个网络的生存期[11]。如果不从系统的观点看, 而针对某一层开发的单独的安全协议, 将产生冗余的安全服务, 消耗不必要的网络资源。无组织的安全设计在消耗网络资源的同时, 会无意识地导致 DOS攻击。

2)缺乏安全的自适应性

WSNs要求适应环境、流量等外界变化, 要求有自适应的安全技术。在 WSNs的安全机制中, 分层设计缺乏自适应性。这是由于安全攻击来自不同层和不同协议, 抗攻击机制依赖于多层或者跨层的解决。通常, 链路层更关注于加密、两级认证、数据更新的安全, 而不考虑物理层的安全问题。但如果物理层不安全的话, 会使整个网络都不安全。不难理解, 多层或者跨层的方法能得到较好的安全性能。而且, 由于能适应网络拓朴、流量等外界变化, 通过自适应地改变安全服务, 还可以获得更多的安全保证。

3)功率有效性问题

能量有效性是 WSNs中考虑的一个重要问题之一。空闲侦听、重传导致的冲突、控制负荷、不必要的高传送功率都会造成功率消耗。因此, 有不同的方法可以降低功耗[13]。文献 [14]提出的方法在保证网络连接性的情况下, 能增加空间重用, 限制发送功率。根据不同的应用, 各协议层有不同的功率控制手段: 在网络层, 功率识别的路由协议[15]被证明能节省功率; 在 MAC层, 文献 [16]提出在不必要时 (如退避阶段) 关掉发射机, 或者使其处于睡眠状态, 通过减轻空闲侦听功率或者降低总的冲突数来节省功率。应用层采用的一些方法[17]也能减少功耗。总之, 功率有效性设计不能完全在网络协议栈中某一层得到完全解决[18], 所以, 安全协议而导致的功率消耗也需要用跨层的方法加以解决。

3 WSNs中跨层的安全解决方案

WSNs安全协议设计的主要考虑因素应该是公钥加密算法和安全协议通信引起的额外能耗。文献 [19]提出了 WSNs中安全设计问题的 4个指导原则:

1)网络安全取决于所有协议层的安全;

2)在大型分布网络中, 安全测量应该服从于动态可重构, 并能进行分布式管理;

3)在给定网络的某一时刻, 由于安全测量而导致的代价, 不应该超出那一时刻由于安全风险而产生的代价;

4)如果不能保证某一节点的物理安全, 安全测量应该能够恢复物理层受到的损害。

第一项原则强调了跨层设计的概念。WSNs由于易受攻击, 所以, 安全问题非常重要。然而, 越高的安全机制越容易消耗更高的网络资源, 从而又会导致 DOS攻击。例如: 能量是物理层参数, 安全是应用层服务, 因此, 安全设计

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

应该用跨层的方法来考虑。

在 WSNs的安全机制中, 研究的侧重点各不相同, 物理层主要通过考虑安全编码来增加机密性; 链路层和网络层的机密性考虑的是数据帧和路由信息的加密技术; 而应用层则着重于密钥的管理和交换, 为下层的加解密提供安全支持。不同层的安全和网络性能不同, 用跨层设计可以平衡这 2个因素。对 WSNs中的安全问题, 有必要结合各层的特点进行考虑。

例如: 在保持安全的前提下, 当以能量消耗作为约束条件时, 在物理层, 可以根据干扰信号自动调整发射功率, 避免拥塞攻击并降低能耗; 在 MAC层, 可以限制数据分组的重传次数, 既能避免耗尽攻击, 又能节省功率; 在网络层, 可以采用多径路由, 既能避免路由黑洞, 又能减少拥塞而造成的能耗。上述措施的联合使用, 将对 WSNs安全性的提高有很大的益处。

3.1　基于需求级别和服务类型的跨层方法

WSNs中, 不同的应用环境有不同的安全需求。即使对于相同的应用, 不同的任务也有不同的安全考虑。文献[20]在 WSNs中把数据类型进行分类, 每一类数据定义相应的安全机制。根据这个分类, 鉴别可能的通信安全威胁。由于每种机制有不同的安全需求, 针对不同的需求, 进行有效的资源管理。

文献[21]提出了一个称为 SecureSense的安全框架, 在 WSNs中提供能量有效的安全通信。根据观察到的外部环境、内部制约和运用需求, 综合考虑安全服务的运行时间, SecureSense可保证节点能最优地分配资源到相应的安全服务中。

由于所有类型的信息含有或多或少的保密信息, 其保密程度与安全负荷成正比, 而安全负荷与能量需求成正比。相应于不同安全方案的数据类型位于不同的协议栈, 可以用跨层的方法来安排安全机制。主要目的是在满足安全需求的前提下, 尽量减少能量消耗。

3.2　跨层的侵入检测

侵入检测主要在 MAC层协议进行, 也可在加密协议中考虑。现在提出的侵入检测方案仅是基于分层的考虑, 对于来自不同层的攻击, 其有效性非常有限。因此, 使用有一个检测安全的工具, 它具有跨层的检测框架, 能够合并不同协议层的操作方案, 尽管文献[22]提出了一个初步的框架, 但没有真正地用跨层结构考虑侵入检测。

现存的分层协议不能很好地执行侵入检测。例如: 研究者研究侵入检测问题时, 往往会忽略物理层的攻击, 但这种类型的攻击很严重, 难于检测。如果物理信道被恶意用户有意干扰, 基于 MAC或者路由协议的安全机制将不能发现这种问题, 因此, 有必要用跨层的观点来进行侵入检测。

3.3　功率有效的跨层设计

如前所述, 能量预留是 WSNs中一个重要的设计目标。在每一个设计阶段, 需要考虑功率消耗, 通过跨层设计, 在能量消耗、网络性能、复杂度方面进行折中, 在提供安全服务时, 跨层方法可以保存在满足安全要求的同时, 节省能量, 以最大化整个网络的生存期。

例如: 在 WSNs中, 载波检测易受 DoS攻击, 恶意节点可以在 MAC层反复地请求接入信道。不仅能够阻止其他节点连接目的节点, 而且, 由于频繁请求消耗其电能。根据与其他层交换日所得的信息, 可以认识恶意节点, 然后, 进行隔离或者限制。

在网络层, 利用其他层的信息选择合适的路径。例如: 根据电池的利用信息, 可以选择电池能量多的路径, 以保证有更多的用于安全的计算负载。根据认证信息, 选择路径绕开恶意节点, 结合地理位置信息也可以有助于抵抗诸如 Sinkhole的攻击。

WSNs中最安全和最省能量的节点是不活动的节点, 如睡眠状态。设计中, 也可以根据跨层信息, 尽量使节点处于睡眠模式, 达到节能的目的。

3.4　跨层的密钥管理

由于 WSNs节点有限的容量, 应该考虑存贮空间, 减少计算的复杂度, 并且, 减少密钥管理的通信负荷。

为了得到高的安全性, 加密算法是必不可少的防御措施之一。但传感节点有限的资源使得公钥加密体制对 WSNs而言是不现实的, 因而, 对 WSNs而言, 合适的对称加密体制是必然的选择。对传感器而言可选的是对称的加密机制, 密钥被窃将导致整个网络瘫痪, 因此, 密钥要进行及时的更新和管理。

现存有不同的密钥管理方案, 如基本随机密钥方案 (basicrandom key scheme)[23]和基于多项式登记的密钥方案 (polynomial poll based key scheme)[24]。它们对抗攻击的复杂性、可测量性以及有效性都不同。可以设计自适应密钥管理方案, 考虑安全级别、拥塞、剩余能量。一个重要目标是通过多层的约束条件导出优化的目标。密钥管理基于这种优化算法的约束目标, 反过来又需要各层不同的协作, 以达到优化性能。

3.5　跨层设计检测自私节点

在 WSNs中, 网络连接性主要依靠各节点的协作。如果其中一个节点故意停止中继分组, 网络将不能正常通信。这种节点称为自私节点, 为了避免这种情况发生, 需要 2种解决方法。其一是执行通信协议, 鼓励节点承担中继任务; 其二是在通信协议中检测自私节点, 警告并处罚它们, 并让它们返回协作模式。所有的解决方案都需要使用跨层的方法, 因为自私行为可以在各层出现, 特别是 MAC层和路由层。仅考虑一层的行为并不能有效避免自私行为, 所以, 需要在多层进行跨层的考虑。例如: 在 MAC层和网络层进行跨层考虑时, 一部分安全机制放在节点的网络层, 通过其后续节点监视其中继分组。另一个安全机制放在 MAC层, 负责添加跳与跳之间的信息, 如 ACK信息, 并进行中继。这

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

种跳间信息被高层的安全机制应用,以发现自私节点。当自私节点被检测时,通常,由 MAC层的安全构件采取措施,这种方法可以快速检测自私节点,比网络层要快。与普通的单层方法相比,减少了通信的负荷,对于防止自私节点十分有效。

4 结束语

可以预见,在不久的将来,WSNs将在军事、工业、商业得到广泛的应用。对 WSNs进行自组织,最大化操作时间,在可能存在的安全攻击下,保持高级别的可用性是非常重要的。

但是,WSNs在安全提供方面面临挑战,传统网络中的安全技术不能在传感网中直接应用。这是由于 WSNs中有限的资源,如,计算容量、功率提供、记忆等造成的,节点密集分布,使安全性更加困难。

由于 WSNs中有限的资源,将来的努力方向是对于安全、弱点、网络性能等进行综合考虑,许多问题需要进一步的研究。其一是在满足最小功耗的前提下对安全级别和网络性能进行折中;其二是提出跨层的交互方案,用于检测攻击和提供入侵抵抗能力,提高网络的抗毁性;其三通过跨层调度分配功率和密钥,优化网络的性能。最后,寻找解决物理层安全缺陷的方法也是一个待研究的方向。

参考文献:

[1] Akyildiz I F, Weilian Su, Sankarasubramaniam Y, et al. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.

[2] Pottie G J, Kaiser W J. Embedding the internet: wireless integrated network sensors[J]. Communications of ACM, 2000, 43(5): 51-58.

[3] Rabaey J, Ammer J, Silva J L da, et al. PicoRadio: Ad Hoc wireless networking of ubiquitous low-energy sensor/monitor nodes[R]. Workshop on VLSI, 2000: 9-12.

[4] Estrin D, Govindan R, Heidemann J. Embedding the internet: introduction[J]. Communications of ACM, 2000, 43(5): 38-41.

[5] Perrig A, Szewczyk R, Wen V, et al. SPINS: security protocols for sensor networks[C]// Rome: MOBICOM 2001, 2001: 2-3.

[6] Carman D W, Kruus P S, Matt B J. Constraints and approaches for distributed sensor network security[R]. Cryptographic Technologies Group, Trusted Information Systems, NAI Labs, 2000: 27-28.

[7] Zhou L, Haas Z J. Securing ad-hoc networks[J]. IEEE Network, 1999, 13(6): 24-30.

[8] Akyildiz I F, Weilian Su, Sankarasubramaniam Y, et al. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.

[9] Ye F, Luo H, Lu S, et al. Statistical en-route filtering of injected false data in sensor networks[C]// INFOCOM, 2004: 2446-2457.

[10] Perrig A, Szewczyk R, Wen V, et al. SPINS: security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521-534.

[11] Chris Karlof, Naveen Sastry, David Wagner, et al. A link layer security architecture for wireless sensor networks[C]// ACM Sensys, 2004: 78-87.

[12] Wood A D, Stankovic J A. Denial of service in sensor networks[J]. IEEE Computer, 2002, 35(10): 54-62.

[13] Ye W, Heidemann J, Estrin D. An energy-efficient MAC protocol for wireless sensor networks[C]// Proceedings of the IEEE Infocom, USC/Information Sciences Institute. New York, USA: IEEE, 2002: 1567-1576.

[14] Wattenhofer R, Li L, Bahl P, et al. Distributed topology control for power efficient operation in multihop wireless ad hoc networks[C]// Proc of INFOCOM, 2001: 22-26.

[15] Aslam J, Li Q, Rus D. Three power-aware routing algorithms for sensor networks[J]. Wireless Communications and Mobile Computing, 2003, 2(3): 187-208.

[16] Woo A, Culler D E. A transmission control scheme for media access in sensor networks[C]// Proc ACM MOBICOM, 2001: 221-235.

[17] Madden S R, Franklin M J, Hellerstein J M, et al. TAG: a tiny aggregation service for ad-hoc sensor networks[C]// Proc of OSDI, 2002: 131-146.

[18] Min R, Bhardwaj M, Ickes N, et al. The hardware and the network: Total-system strategies for power aware wireless microsensors[C]// Proc of the IEEE CAS Workshop on Wireless Communications and Networking, USA: Pasadena, CA, 2002: 36-12.

[19] Jones K, Wadaa A, Oladu S, et al. Towards a new paradigm for securing wireless sensor networks[C]// Proceedings of the 2003 Workshop on New Security Paradigms, 2003: 115-121.

[20] Sasha Slijepcevic, Miodrag Potkonjak. On communication security in wireless Ad Hoc sensor networks[C]// USA: (WETICE) IEEE Pittsburgh Pennsylvania, 2002: 139-144.

[21] Qi Xue, Ganz A. Runtime security composition for sensor networks(SecureSense)[C]// Vehicular Technology Conference, 2003 VTC 2003-Fall 2003 IEEE 58th, 2003: 2976-2980.

[22] Zhang Y, Lee W. Intrusion detection in wireless Ad-Hoc networks[C]// ACM MOBICOM, 2000: 545-556.

[23] Eschenauer L, Gligor V D. A Key-Management scheme for sensor networks[C]// The 9th ACM Conference on Computer and Communication Security, 2002: 41-47.

[24] Du W, Deng J, Han Y S, et al. A pairwise key predistribution scheme for wireless sensor network[C]// ACM CCS, 2003: 42-51.

作者简介:

杨光松(1968-),男,贵州丹寨人,讲师,博士,主要研究方向为无线传感器网络。

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net