

无线传感器网络中的安全威胁分析及对策^{*}

曾志峰¹, 邱慧敏², 朱龙海²

(1. 安氏互联网安全系统(中国)有限公司, 北京 100037; 2. 北京邮电大学 信息安全中心, 北京 100876)

摘要: 首先分析了无线传感器网络的特点、面临的安全威胁、所需要解决的关键安全问题以及安全协议设计原则,在此基础上给出了一种安全解决方案,有效解决了无线传感器网络中通信的机密性、可靠性、完整性与时效性等安全需求。

关键词: 无线传感器网络; 安全; 威胁; 对策

中图法分类号: TP393.08

文献标识码: A

文章编号: 1001-3695(2007)01-0140-04

Risk Analysis and Security Countermeasure about Wireless Sensor Network

ZENG Zhi-feng¹, QIU Hui-min², ZHU Long-hai²

(1. Information Security One Limited, Beijing 100037, China; 2. Information Security Center, Beijing University of Posts & Telecommunications, Beijing 100876, China)

Abstract: This paper analyzes the characteristics, potential security threats, key issues and design goal for achieving the security of wireless sensor network, and then presents integrated approach to securing sensor network, as an conclusion, the security requirement, such as confidentiality, integrity, authentication, freshness, is solved effectively.

Key words: Wireless Sensor Network (WSN); Security; Threats; Countermeasure

无线传感器网络(Wireless Sensor Network, WSN)是一种自组织网络,它通过大量低成本、资源受限的传感节点设备协同工作以实现某一特定任务。由于其具有部署灵活、维护简单等特点而在事件监测、军事监控、气候预测等方面有着广泛的应用前景^[1]。而 WSN 通常部署在无人维护、不可控制的环境中,使其除了具有一般无线网络所面临的信息泄露、信息篡改、重放攻击、拒绝服务等多种威胁外,它还面临传感节点容易被攻击者物理操纵,并获取存储在传感节点中的所有信息,从而控制部分网络的威胁。随着 WSN 应用的普遍化,安全问题也将越来越突出,如何保证传感网络以及所采集数据的机密性、真实性、可靠性,将是 WSN 研究的一个重要课题。

1 传感器网络特点分析

WSN 主要由三个主要部分组成:传感节点(Sensor Node)、基站(Sink)和观察对象。传感节点散布在观察区域内采集与观察对象相关的数据,并将协同处理后的数据传送到 Sink,如图 1 所示。在 WSN 中,每个节点都具有把所采集或收集的信息直接或通过其他节点转发给基站、识别传送给自己的信息包、处理广播信息包的功能。

整个 WSN 的路由是一个树状结构,基站为树的根,并根据路由算法选择某些传感节点作为树的叶节点,也称为簇节点(包括基站),簇内所有其他的普通节点只与簇节点进行通信,簇节点把接收到的传感信息进行处理后,转发给上级簇节点,并最终传送给基站。



图1 无线传感网络体系结构

1.1 传感节点

由于 WSN 是一种大规模的分布式网络,常部署于无人维护、条件恶劣的环境当中,且大多数情况下传感节点都是一次性地使用,这决定了传感节点是价格低廉、资源极度受限的无线通信设备。主要体现在以下几个方面:

(1) 能量有限。能量是限制传感节点能力、寿命的最主要的约束性条件,现有的传感节点都是通过标准的 AAA 或 AA 电池进行供电,并且不能重新充电。因此在进行安全机制设计时,必须充分考虑密码算法、安全协议及密钥存储等对能量消耗的影响。

(2) 计算能力有限。传感节点 CPU 一般只具有 8bits 4MHz~8MHz 的处理能力,因此所选择的密码算法必须适合传感节点处理器的特点,同时密码算法的计算不能为传感信息的传输引入过多的时延,如公钥算法就不宜在传感网络中频繁使用。

(3) 存储能力有限。传感节点一般包括三种形式的存储器,即 RAM、程序存储器和工作存储器。RAM 用于存放工作时的临时数据,一般不超过 2KB;程序存储器用于存储操作系

收稿日期: 2005-08-11; 修返日期: 2005-12-29

基金项目: 国家自然科学基金资助项目(60372094)

统、应用程序以及安全函数等;工作存储器用于存放获取的传感信息,这两种存储器一般也只有几千字节,用于存储安全代码、密钥的空间很少。因此,预先存储大量密钥的安全机制不适用于 WSN,而且还必须选择密钥长度较小的轻型密码算法用于安全通信。

(4)通信范围有限。为了节约信号传输时的能量消耗,传感节点的 RF 模块的传输能量一般在 10mW ~ 100mW 之间,传输范围也局限于 100m ~ 1km 之内,因此并不是所有的传感节点都能与基站直接进行通信,离基站较远的传感节点所发送的信息必须经过中间节点的转发才能到达基站,因而传感信息也面临被篡改、丢弃等多种威胁。

(5)防篡改。传感节点是一种价格低廉、结构松散、开放的网络设备,攻击者一旦获取传感节点就很容易获得和修改存储在传感节点中的密钥信息以及程序代码等^[3]。因而在进行安全结构设计时,必须考虑整个安全结构在部分传感节点被攻击后的容错性能。

1.2 网络特征

(1)自组织网络。大多数传感器网络在进行部署前,其网络拓扑是无法预知的;部署后,整个网络拓扑、传感节点在网络中的角色也是经常变化的,因而不像有线网、大部分无线网络那样对网络设备进行完全配置。对传感节点进行预配置的范围是有限的,很多网络参数、密钥等都是传感节点在部署后进行协商后形成的。

(2)信息包的大小。考虑到传感节点在发送传感信息时的能量消耗以及无线传输时的信号冲突,传感信息包的大小一般只有 30Bytes 左右^[2]。因此,在对信息包进行完整性校验、加密等安全保护时,允许添加的字节数也是有限的。另外,为了减少能量消耗,安全协议也应尽量减少对传感信息包的扩展。

(3)时延。多跳路由由于方式、较低的网络传输速率(一般只有 10kbps)、无线信道阻塞等问题将导致传感信息在传输时会引入较大的时延,因此在保证信息包的时效性、可靠性时,必须考虑通信双方在时间上的同步问题。

(4)路由变换。传感网络的路由算法是根据传感节点能量来进行路由决策的,当充当网关的传感节点能量损耗到预定值时,必须重新进行路由。路由的变化需要节点之间重新进行密钥协商,这将会为整个网络引入额外的能量消耗和网络流量,因此密钥协商协议应尽量减少握手的次数和通信负荷。

(5)信道误码率。传感器网络是通过无线进行通信的,且经常部署于恶劣的环境中,信道的误码率较高,这将会影响信息包的可靠性及完整性认证过程,因此可靠性、完整性认证协议应尽量减少交互的次数和增加的通信负荷。

(6)不可靠的通信。传感网络是面向无连接的包交换网络,由于信道误码率和无线信道冲突,信息包在传输时很可能会丢失,这也决定了应尽量减少或避免安全协议的交互次数。

(7)间歇的连接方式。为了节省能量,传感节点在没有信息传输时通常会处于休眠状态,并按预定的时间间隔唤醒。因此进行密钥协商、密钥同步等安全操作时,必须充分考虑节点间时间的同步问题。

1.3 通信方式

由文献[4]可知,整个传感网络的路由是一个树状结构,

基站为树的根,并根据路由算法选择某些传感节点作为树的叶节点,也称为簇节点(包括基站)。簇内所有其他的普通节点只与簇节点进行通信,簇节点把接收到的传感信息进行处理后,转发给上级簇节点,并最终传送给基站。在 WSN 中,主要有三种通信模式:①单播通信,如节点把读取的传感信息向簇节点进行传送;②全局广播通信,如基站发送给整个网络的请求或控制信息;③局部广播通信,如簇节点发给簇内所有节点的控制信息。

不同的通信模式具有不同的通信特点,所传递的信息也不一样,所以具有不同的安全需求。但不管哪种通信模式,传感节点都是通过 RF 模块以广播的方式对信息进行传送,在信号广播范围内的所有节点都能接收到该广播信息,这是一个共性问题。安全设计必须根据不同通信模式的特点,提出不同的有针对性的安全解决方案。

1.4 部署环境

WSN 一般规模比较大,从几百个节点到成千甚至上万个节点不等,同时常部署在无人维护、开放的、广阔的环境当中,使攻击者能很方便地对其传送的传感信息进行窃听、插入、重放以及对传感节点进行物理操纵。与其他的无线网络、有线网络相比,针对 WSN 的攻击种类更多,且比较容易实施。因此所设计的安全协议必须具有相当的容错能力,即使在部分节点被攻击者捕获后,整个安全协议也必须具有相当的安全等级。

2 威胁分析

任何安全协议的设计都是基于对网络可能的安全威胁充分分析基础上的,本节将根据 WSN 的特点,对 WSN 所面临的潜在安全威胁进行分类与描述。

(1)传感节点的物理操纵。传感节点是一种没有防篡改能力的物理设备,同时为了提高传感节点的灵活性,各传感节点都有一个编程接口(JTAG 接口),以便对传感节点重新编程。当攻击者获取传感节点后,就很容易地对传感节点内存储的内容进行读取、修改,并把修改或伪造的节点重新部署到 WSN 中。一旦攻击者控制了 WSN 中部分的传感节点,就可以发起很多种攻击,如伪造虚假传感信息、丢弃所要转发的传感信息、分析传感信息中的敏感数据、对转发信息进行篡改、假冒合法节点、伪造拥有多个合法身份的节点等。

(2)传感信息的窃听。由于 WSN 的特点,攻击者可以很容易地对单个甚至多个通信链路间传输的信息进行窃听,并从多个传感信息中分析出敏感数据。同时,通过传感信息包的窃听,还可以对 WSN 中的网络流量进行分析,从而分析出传感节点的位置、作用等。

(3)拒绝服务攻击。它主要用于破坏 WSN 的正常功能,其攻击形式主要有以下几种:①在网络中发送大量的无用信息以产生链路阻塞,从而干扰网络协议和传感信息的正常传送;②向传感节点发送大量有用或无用的传感信息,从而快速消耗节点的能量和资源;③发布虚假路由,引起网络路由循环等。

(4)重放攻击。攻击者截获在 WSN 中传播的传感信息、控制信息、路由信息等,并假冒成合法节点对截获信息进行重放,从而造成网络混乱、传感节点错误决策等。

(5)完整性攻击。它一般包括对传感信息的修改、插入,

但由于传感网络的广播性质,在攻击者对传感信息进行截取并修改重发之前,广播范围内的节点都已接收到了原始的广播信息。对广播信息进行修改攻击在 WSN 中很难实施,因此 WSN 中的完整性攻击一般指信息插入攻击。

3 安全需求和设计原则

3.1 安全需求

(1) 传感信息的机密性。它可通过对传感信息内容进行加密实现,以防止信息泄露给非法节点或外部攻击者。

(2) 传感信息的完整性。它保证了信息在传输过程中没有被非法篡改,信息的完整性可通过计算信息的摘要等来实现。

(3) 传感信息的可靠性。它保证了信息来自合法的传感节点。可靠性可通过数字签名、通过共享的唯一性密钥对信息加密、通过共享的唯一性密钥计算信息的摘要、单向密钥链等实现,对于不同的通信模式应选择不同的方式来实现信息可靠性。

(4) 传感信息的时效性。通过保证信息的时效性,可有效地防止重放攻击。时效性可通过时间戳、随机数、序列号等实现。

3.2 设计原则

(1) 能量有效性。由于传感节点只具有有限的能量,因此所设计的安全机制必须是能量有效的,特别是不能引入过多的信息传输以及计算复杂的密码算法。

(2) 尽量避免使用交互式的安全协议。一方面是无线传感器网络大部分的能量消耗在信号的接收和发射上,因此使用交互式协议将会增加传感器网络的能量消耗和通信负荷;另一方面,传感器网络中容易发生信号丢失,从而导致传感节点由于等待下一条信号而造成系统资源的浪费。

(3) 避免信息的分段传输。由于安全而增加的安全负荷应尽量地小,否则必须对信息包进行分段传输。由于无线环境中包的丢失率很高,为了保证传输信息的可靠性,传感网络必须进行信息包的重传和缓冲,这将会增加传感网络协议设计的困难和复杂性,同时会加大网络的通信负荷、传感节点的能量消耗和过多的 RAM 空间消耗。

(4) 支持传感信息的网内处理。为了增加网络寿命,减少传感节点的能量消耗,簇节点一般会对从簇内其他节点传送的传感信息进行网内处理,如对簇节点对传感信息进行合并、簇内普通节点对传感信息的被动监视等,因此在 WSN 中不宜实现端到端加密。

(5) 较高的容错性能。由于传感节点很容易被攻击者物理操纵,即使提高了节点本身的安全性能,也存在节点内信息被读取、修改的可能性。因此所设计的安全机制必须保证在部分节点被破坏后也能达到一定的安全性能。

4 安全解决方案

4.1 密钥协商

本文引入两种密钥来保证 WSN 中信息传输的安全:

(1) Pairwise Key。它是传感节点之间或传感节点与基站

之间临时建立起来的配对密钥,主要用于在簇内安全地分发 Cluster Key 或保证节点之间传感信息传输的安全。

(2) Cluster Key。它是簇节点和簇内所有普通节点所共享的密钥,用于保证簇内局部广播通信和簇内传感信息的安全传送。采用 Cluster Key 对传感信息加密是为了支持传感信息的网内处理,从而节省能量消耗,本文也采用 Cluster Key 对传感信息加密。

下面将阐述 Pairwise Key, Cluster Key 的产生及相应密钥的更新过程。

(1) Pairwise Key 协商

本文利用 Blundo-et-al 方法^[3]来产生 Pairwise Key。当 WSN 部署后,各传感节点不需要进行任何交互就可以计算出相互之间的 Pairwise Key,具体如下:

在 WSN 部署前,随机地产生一个 t 次多项式 $f(x, y) = \sum_{i,j=0}^t a_{i,j} x^i y^j$ ($a_{i,j} = a_{j,i}$)。根据每个节点唯一的 ID, 计算 $g_{ID}(x) = f(x, ID)$, 然后把多项式 $g_{ID}(x)$ 的系数存储在各传感节点中, 这样, 当网络部署后, 只要传感节点知道互相之间的节点 ID_x , ID_y , 就根据 $f(ID_x, ID_y) = f(ID_y, ID_x)$ 计算 Pairwise Key, 该算法在攻击者捕获 t 个节点前是无条件安全的。

(2) Cluster Key 协商

簇节点 u 随机地产生一个 Cluster Key $k_{u,c}$, 并用与簇内普通节点 $v_1, v_2, \dots, v_m$ 共享的 Pairwise Key k_{u,v_i} 加密, 随后把加密后的 $k_{u,c}$ 发送给 $v_i, 1 \leq v_i \leq m$ 。

$$u \rightarrow v_i : (k_{u,c})_{k_{u,v_i}}, \text{timestamp}$$

节点 v_i 收到该信息后, 首先验证时间戳的有效性, 如果有效则对加密的 $k_{u,c}$ 解密, 并把 $k_{u,c}$ 存储于传感节点中。当间隔一定的时间, 或簇内某个节点发生异常而撤销后, 必须对 $k_{u,c}$ 进行更新, 更新的步骤与上述方法类似。

(3) Pairwise Key 更新

为了适合 WSN 的动态网络拓扑, 必须对传感节点中的 Pairwise Key 进行更新。

$$u \rightarrow * : u, \text{timestamp}$$

$$v_i \rightarrow u : v_i, \text{MAC}(k_{u,v_i}, \text{timestamp} \parallel v)$$

$$k_{u,v_i} = \text{Pseudo}_{k_{u,v_i}}(u)$$

簇节点首先向簇内所有节点发送包括 ID 和时间戳的 Pairwise Key 更新请求, 当节点接收到该信息后, 向簇节点返回一个用 Pairwise Key 加密后的 MAC 码, 簇节点收到各节点返回的应答信号后, 就用随机数函数产生一个和 v_i 共享的新 Pairwise Key k_{u,v_i} , 各节点也根据同样的随机数函数产生 k_{u,v_i} 。

4.2 节点间的安全通信

根据传感节点的特性, 本文选择对称的分组密码算法实现单播通信的机密性, 常用的分组密码包括 AES, DES, RC5, Serpent, Skipjack 等, 但经过对以上算法的细致分析, 发现并不是都适合于传感节点的特性。如 AES 至少需要 800Bytes 的查询表和不少于 128bits 的密钥长度; DES 需要一个大小分别为 512 的 SBox、256 的置换表; RC5 虽然效率很高, 但是其算法执行过程中需要的各种临时密钥, 需要在算法执行前进行预计算, 从而消耗额外的内存空间, 如 RC5-32/12/8 至少需要 112Bytes 的临时密钥存储; 另外 RC5 算法需要进行 32bits 的环形移位

操作,这对于8bits的传感节点而言是一个非常复杂的计算;Serpent虽然只需要简单的逻辑操作,但是其程序代码空间很大。基于此本文选用Skipjack密码算法。

本文选用CTR模式的加密方法:

(1)因为该模式的加解密过程是完全一样的,可以节省代码空间,如图2所示;

(2)因为CTR加密方法具有流密码性质,明文和密文具有一样的长度;

(3)因为对于每次加密操作,由于计数器的不同,即使是相同的明文,其密文也是不同的,对于不知道加密密钥的攻击者来说,利用CTR模式加密的密文是一种无关的、随机化的信息;

(4)递增的计数器既保证了传感信息具有弱的时效性,又可抵抗重放攻击。

另外,为了减少能量消耗和暴露出当前计数器的值,本文把计数器的值存储在相互通信的节点之内,并不随着加密信息一起传输,当发生计数器之间的不同步时,由簇节点发送本身存储的计数器的值,以维持传感节点间计数器之间的同步。

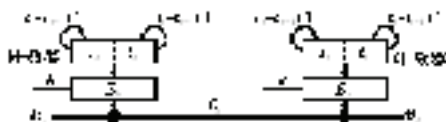


图2 CTR模式加解密框图

为了节省代码存储空间,本文利用同样的加密算法,通过CBC-MAC方式来保证传感信息的完整性。MAC的大小为4Bytes,从下文的分析看,4Bytes的MAC完全可以满足传感网络的安全需求。另外,为了保证传感信息的时效性,在每个传感信息中都加入了1Byte的时间戳。整个过程可表示为

$$v_i \rightarrow u: \{M | \text{timestamp}\}_{k_{ctr}}, \text{CBC-MAC}(k_{mac}, \{M | \text{timestamp}\}_{k_{ctr}})$$

上式中, k_{ctr} 即为Cluster Key, k_{mac} 是以 k_{ctr} 为种子,由随机函数 $\text{Pseudo}_{k_{ctr}}(u)$ 导出的完整性密钥。

5 总结

本文所提出的安全措施,可有效地防止目前传感网络中出现的大多数安全威胁,保证了传感信息的机密性与节点间的相

互认证,同时还有效地减小了当传感节点被捕获后对整个网络安全的影响。具体如下:

(1)通过加密、时间戳、信息摘要有效地保证了节点间通信的完整性、机密性和时效性,同时通过加密、CBC-MAC的计算也保证了节点与节点之间的相互认证,因为只有合法的节点才可能知道相互之间的通信密钥。除此之外,CTR方式的加密和时间戳还可以有效地抵抗重放攻击。

(2)通过实现节点与节点之间的相互认证,有效地防止了非法节点加入WSN,从而增加了进行DoS攻击的难度。

(3)提供了有效的密钥更新方案,增加了攻击者通过大量观察传感信息获知Cluster Key等通信密钥的难度。

安全是传感网络设计中的重要问题,本文首先分析了传感网络的特点和面临的威胁,并在此基础上提出了安全的无线传感器网络所要解决的关键问题和设计原则,并有针对性地给出了安全的解决方案,有效解决了无线传感器网络中通信的机密性、可靠性、完整性及时效性等安全需求。

参考文献:

- [1] D W Carman, P S Kruus, B J Matt. Constraints and Approaches for Distributed Sensor Network Security [EB/OL]. <http://download.nai.com/products/media/nai/zip/nailabs-report-00-010-final.zip>, 2000-09-01.
- [2] Perring A, Szewczyk R, Tygar J D, et al. SPINS: Security Protocols for Sensor Networks [C]. Rome: the 7th Annual ACM International Conference on Mobile Computing and Networks, 2001. 521-534.
- [3] Blom R. An Optimal Class of Symmetric Key Generation System [C]. Advances in Cryptology-Eurocrypt, Springer LNCS 209, 1984. 335-338.
- [4] Priit Caru. Practical Comparison of Fast Public-Key Cryptosystems [EB/OL]. <http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers/loikkanen-kahe.pdf>, 2000-07.
- [5] Colleen Marie O'Rourke. Efficient NTRU Implementation [EB/OL]. <http://www.emsec.ee.ucla.edu/pdf/corourke.pdf>, 2002-04.

作者简介:

曾志峰,男,博士,研究方向为网络安全、安全服务;邱慧敏,男,博士研究生,研究方向为密码学、电子商务、网络安全等;朱龙海,男,博士研究生,研究方向为密码学、电子商务、网络安全等。

(上接第68页)

- [10] Jurgen Bohn, Friedemann Mattern. Super-Distributed RFID Tag Infrastructures [C]. EUSAI 2004, Springer, LNCS 3295, 2004.
- [11] Valerie Issarny. Developing Ambient Intelligence Systems: A Solution Based on Web Services [C]. Automated Software Engineering, Springer, 2005. 101-137.
- [12] Tom Broens, Stanislav Pokraev. Context-Aware Ontology-based Service Discovery [C]. EUSAI 2004, Springer, LNCS 3295, 2004. 72-83.
- [13] Paolo Remagnino. Ambient Intelligence: A New Multidisciplinary Paradigm [J]. IEEE Trans. on System, Man and Cybernetic- Part A, 2005, 35(1): 1-6.
- [14] SOAP Toolkit 3.0 [EB/OL]. <http://msdn.microsoft.com/webservices/downloads/default.aspx>, 2005.

- [15] Microsoft UDDI SDK 2.0 [EB/OL]. <http://msdn.microsoft.com/webservices/downloads/default.aspx>, 2005.
- [16] WSDL Specification [EB/OL]. <http://www.w3.org/TR/wsdl>, 2005.
- [17] UDDI Specification [EB/OL]. <http://www.uddi.org/>, 2005.
- [18] 李大成,陈莘萌. UDDI技术及应用概览 [J]. 计算机工程, 2002, 28(12): 3-5, 8.
- [19] 任捷,吴明晖,应晶. Web Services技术在异构系统集成中的应用研究 [J]. 计算机应用, 2004, 24(1): 95-98.

作者简介:

凌庆华(1980-),男,湖南人,硕士研究生,主要研究方向为网络通信、网络服务;程伟明(1954-),男,江苏溧阳人,研究员,主要研究方向为IP网络技术、移动通信网络和多媒体传输技术。