文章编号:1002-4026(2011)04-0036-05

基于两种加密机制的 ZigBee 网络密钥管理方案

潘金秋,赵华伟,徐如志,黄太波
(山东财政学院计算机信息工程学院,山东 济南 250014)

摘要:网络的安全性问题是制约 ZigBee 无线传感网络飞速发展的主要原因。密钥管理是保证网络安全性的基础,本文利用多边形顶点和边及对角线数目的关系,对网络大小和多边形顶点数目的关系进行统计分析,提出一种密钥管理方案,安全性能较高,对存储和计算的要求较低,节省了保证网络所需要的资源,对进一步研究 ZigBee 网络安全具有理论指导意义。

关键词:ZigBee 网络;加密算法;密钥管理
中图分类号:TP393.084 **文献标识码**:A

A two encryption mechanisms based key management scheme of ZigBee wireless sensor networks

PAN Jin-qiu, ZHAO Hua-wei, XU Ru-zhi, HUANG Tai-bo
(School of Computer & Information Engineering, Shandong University of Finance, Jinan 250014, China)

Abstract: The main negatives of a ZigBee wireless sensor network are limited computing ability, storage capacity and self resources. Network security is one of the main restrictions to its rapid development. It is therefore quite significant to guarantee its security. Key management is the basis for such security. This paper statistically analyzes the relationship between network size and the number of polygon vertices with the relationship among vertices, sides and diagonals of a polygon and then presents a novel key management scheme. This scheme has higher security but lower storage and computing capability requirements, so it reduces the requirement for network resources and can guide further research on network security.

Key words: ZigBee wireless sensor networks; encryption algorithm; key management

近些年来,物联网的发展越来越受到重视,无线通信、集成电路、传感器等技术飞速发展、融合,已经可以生产出成本低廉、通信能力良好、数据计算和信息搜集能力较高的无线通信节点[1-3]。人们已经能够实时的监控外部环境,达到了大范围、自动化地数据采集。无线传感网络利用节点内置各式各样的传感器,进行环境的监控和信息的采集,并通过无线通信的方式,将获取到的信息传给终端用户,将物理世界、人类社会、计算机三者有机的结合起来。但是,和有线网络相比,无线传感网络中的数据更容易被窃听,攻击者可以实时地监听信道,向信道注射比特流等,对网络进行干扰和攻击。所以,如何保证数据的安全机密性是无线传感网络通信的关键问题。密钥管理是保密通信的基础,而无线传感网络节点自身的计算能力和存储空间非常

收稿日期:2011-04-08
基金项目:国家自然科学基金(NO.60873041)
作者简介:潘金秋(1986-),男,硕士研究生,研究方向为信息安全。Email:panjinqiu_007@163.com

有限,不适应计算存储要求高的密钥管理方案,因此,需要进行更加有效的安全防范,本文提出了 ZigBee 网络中一种基于 ECC 和 AES 混合加密算法的轻量级的密钥管理方案,利用该方案可以在保证网络安全通信的前提下,弥补 ZigBee 网络节点计算和存储能力有限的缺陷。

1　ZigBee 无线网络面临的安全威胁

ZigBee 无线传感网络可能存在多种形式的安全威胁[4],节点被恶意损害所造成的破坏对网络影响不会太大,但是如果是由于计算能力、存储能力、资源受限等方面的原因所造成的安全问题,很可能被攻击者操纵、窃取,控制数据带来巨大的损失,ZigBee 无线传感网络主要有以下被攻击方式:

(1)信息窃听

由于无线传感网络部署的特点,攻击者可以通过节点间的传输而获得敏感或者私有的信息。例如,在医院病人手腕上佩戴的脉搏传感器节点,部署在室外的无线接收器可以接收到发送的信息,获得病人的脉搏跳动次数,获取病人的身体健康状况信息,对病人的隐私构成威胁。

(2)拒绝服务攻击(DoS)

拒绝服务攻击主要用来破坏网络的使用,比如试图中断,颠覆和毁坏传感网络,使整个传感网络无法正常对外提供服务,向目标节点发送大量的无用信息,目标节点就会消耗大量的能量去处理这些无用信息,因此没有更多的资源去处理正确的信息,导致网络无法正常提供服务。

(3)私有性安全问题

传感器网络的主要目的是用于收集信息,攻击者可以通过窃听、加入伪造的非法节点等方式获取这些敏感信息,如果攻击者知道怎样从多路信息中获取有效信息的相关算法,那么攻击者就可以通过大量获取的信息导出有效信息。一般传感器中的私有性问题,并不是通过传感器节点去获取不大可能收集到的信息,而是攻击者通过远程操作,从而获得大量的信息,并根据特定算法分析出其中的私有性问题。因此攻击者并不需要物理接触传感节点,是一种低风险、匿名的获得私有信息方式。

2　密钥管理方案

2.1　目前的密钥管理方案

在目前的密钥管理方案[6]中,最简单的一种方案是让 ZigBee 网络的所有节点共享一个会话密钥,所有的节点用会话密钥协商生成新的通信密钥,这种方法很简单,对存储的要求很低,但是安全性能非常低,因为如果一个节点被捕获,整个网络的安全就会受到威胁;另外一种方案是让 ZigBee 网络中的每个节点存储 M－1个密钥(M 是 ZigBee 网络中节点的个数),这样节点就可以与网络中其他 M－1 个节点进行安全通信,任何一个节点被捕获,都不会影响网络中其他节点的安全通信,但是这对节点的存储能力要求太高,该方案难以应用;多数密钥管理方案都是对节点的存储能力和计算能力有着一定的限制要求,而节点的存储能力较低成为提升安全性能的瓶颈。

总体而言,现存的提出密钥更新的密钥管理方案中,几乎都是使用各个节点不同的密钥对新密钥进行加密,然后发送给各个节点,这无疑增加了节点的负担,而且以往的加密多数采用对称加密算法,对身份隐私进行验证[7]。

2.2　新的密钥管理方案

ZigBee 网络由几个部分组成,最基本的组成部分是节点,节点既可以是 Coord 节点(协调器全功能设备),也可以 RFD 节点(精简功能设备),如果两个或者更多的节点在一个通信空间的范围内,并且处于同一信道通信,那么这些设备就组成了 ZigBee 网络,网络中必须含有一个 Coord 节点作为协调器。Coord 节点是一种特殊的节点,它可以作为发起设备、终端设备或者作为路由设备,而 RFD 节点只能作为终端节点。

本文提出的新的密钥管理方案,考虑将更多的计算和存储放在中心节点上进行,这样对于节点数目庞大

的 ZigBee 网络而言,终端节点的存储要求就得到了很大程度的降低,我们假设中心节点的计算能力和存储能力足够强大,中心节点使用少量密钥就可以实现密钥的更新分发,并保证节点之间的安全通信,并采用了 ECC 非对称加密算法来进行身份的验证。

2.2.1 新的密钥管理方案基本原理

新的密钥管理方案是利用数学中一个多边形任意两个顶点连接可以变成对角线或者多边形的边的知识,一条多边形的边或者对角线可以作为一个密钥,便可以得到多个密钥,使用这样的方式来实现密钥管理。用 n 表示网络中节点的个数,q 表示多边形的顶点数目,那么我们就可以得到这个多边形边和对角线数据之和为$(q*q-q)/2$,即网络划分成的每一个小的部分最多能够拥有的节点个数。

如表 1 所示,$n=10$,$q=5$,T 表示节点拥有此边,F 表示该节点不拥有此边,每个节点拥有的边数是 1,即每个节点拥有多边形的一条边。

表 1 密钥分发方案

Table 1 Key distribution scheme

	节点 1	节点 2	节点 3	节点 4	节点 5	节点 6	节点 7	节点 8	节点 9	节点 10	顶点标志
边一	T	F	F	F	F	F	F	F	F	F	1
边二	F	T	F	F	F	F	F	F	F	F	2
边三	F	F	T	F	F	F	F	F	F	F	3
边四	F	F	F	T	F	F	F	F	F	F	4
边五	F	F	F	F	T	F	F	F	F	F	5
边六	F	F	F	F	F	T	F	F	F	F	6
边七	F	F	F	F	F	F	T	F	F	F	7
边八	F	F	F	F	F	F	F	T	F	F	8
边九	F	F	F	F	F	F	F	F	T	F	9
边十	F	F	F	F	F	F	F	F	F	T	10

2.2.2 网络形成时的密钥分发

在公钥密码体制中,ECC 加密体制资源消耗相对较低,而且密钥的长度较短,符合 ZigBee 网络节点存储能力和计算能力较差的现实条件。

形成网络时 Coord 节点将密钥分发到各个 RFD 节点中去,密钥由 Coord 节点产生,多边形的每个顶点有一个密钥,每条边或者对角线对应的密钥通过连接的两个顶点的密钥异或运算得到,首先使用 ECC 加密算法将 Coord 节点的公钥发送给各个 RFD 节点,各个节点将自己的公钥发送给 Coord 节点(只是在密钥分发的时候使用 ECC 公钥加密方式,实现身份认证和安全发送密钥,以减少资源的消耗),然后将每条边对应的密钥使用各个 RFD 节点的公钥加密后发送给各个 RFD 节点。其次整个 ZigBee 网络通信过程中,每一个 Coord 节点组建的网络部分会有一个自己的公共密钥进行通信,如果每个组内的两个节点需要私密通信,需要在这两个节点之间建立一个独立会话密钥。

以 $n=10$,$q=5$ 为例,进行详细的阐述介绍。Coord 节点作为协调器节点,计算能力和存储能力较为完备,首先 Coord 节点将自己的公钥发送给网络中的各个 RFD 节点,由 Coord 节点产生密钥一、密钥二、密钥三、密钥四、密钥五,分别分配给顶点一、顶点二、顶点三、顶点四、顶点五,并产生组内通信的公共密钥(公共密钥利用顶点的密钥通过异或运算产生,即密钥一⊕密钥二⊕密钥三⊕密钥四⊕密钥五(注:⊕表示异或运算)),Coord 节点按照图 1 所示方案将顶点密钥和组内通信的公共密钥分发给各个 RFD 节点,发送前使用 Coord 节点的私钥对各个边密钥和密钥标志进行加密,各个 RFD 节点收到各自加密后的边密钥时,用 Coord 节点的公钥进行解密,获得各自的边密钥,组内的节点进行通信时使用公共密钥,如果组内两个节点需要私密通信,可以在两个节点间建立一个临时的独立会话密钥。

独立会话密钥的建立过程如下:以节点 1 和节点 5 为例,(1)节点 1 向 Coord 节点发出通信请求,要求和节点 5 进行私密会话;(2)Coord 节点为节点 1 和节点 5 生成一个独立会话密钥(若两个节点拥有的边密钥

代表的边是相连的,直接使用相连边的三个顶点密钥异或得到;若不相连,则利用两条边对应的四个顶点密钥异或得到);(3)Coord 节点得到节点 1 和 Coord 的独立会话密钥 key(Coord,1),利用 AES 加密算法使用边密钥将节点 1 和节点 5 的独立会话密钥加密后发送给节点 1;(4)Coord 节点将节点 1 和节点 5 的独立会话密钥使用边密钥通过 AES 加密算法加密后送给节点 5;(5)节点 1 和节点 5 使用各自的边密钥,解密得到节点 1 和节点 5 的独立会话密钥。整个过程如图 1 所示。

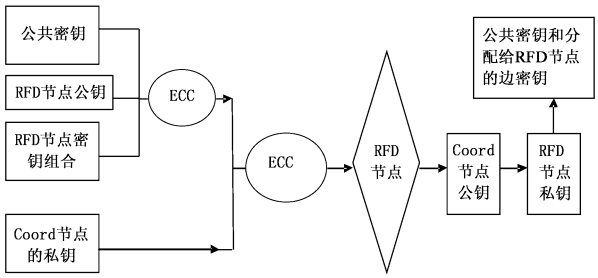

图 1　开始时的密钥分发过程

Fig. 1　The beginning of the key distribution process

2.2.3　节点加入时的密钥更新

RFD 节点的加入要分为两种情况:一种是节点加入前网络中的节点数目小于$(q*q-q)/2$;另一种是节点加入前网络中的节点数目等于$(q*q-q)/2$。首先考虑第一种情况,节点加入前网络中的节点数目小于$(q*q-q)/2$,说明在此时还可以继续有节点的加入,此时问题变的较为简单,Coord 节点只需要查找多边形中闲置的边或者对角线对应的密钥分配给新加入的 RFD 节点就可以了,并将 Coord 节点的公钥发送给新加入的 RFD 节点,用 Coord 节点的私钥加密后,将新分配的边密钥和公共密钥使用 Coord 节点私钥加密后发送给新加入的 RFD 节点;另外一种情况是节点加入前网络中的节点数目等于$(q*q-q)/2$,此时网络中的节点数目达到上限,不能允许新 RFD 节点的加入,此时需要 Coord 节点更新 q 的值,增大网络中可以容纳的节点数目,形成新的更多的边密钥,然后发送 Coord 节点的公钥,Coord 节点首先使用各个 RFD 节点公钥加密边密钥和公共密钥,再用 Coord 节点的私钥加密后,发送给相应的各个节点。流程图如图 2 所示。

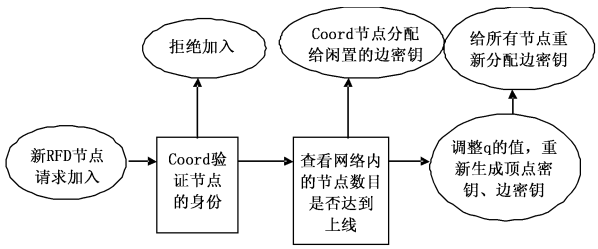

图 2　新节点加入时的密钥更新

Fig. 2　Key update when new nodes joining

2.2.4　节点退出时的密钥更新

若网络中的某个节点退出网络时,需要对整个网络中的共享密钥和这个节点拥有的边密钥进行更新,以保证整个网络的安全性。当某个节点退出网络,Coord 需要产生整个网络中新的共享密钥,同时产生这个退出节点拥有的密钥来替代原来的密钥,以图 1 为例,对节点退出网络时密钥的更新进行介绍:当节点 2 退出网络时,Coord 节点需要产生新的共享密钥以及和这个边密钥对应边的两个顶点密钥,并更新和这两个顶点密钥对应顶点相连的边密钥,Coord 节点使用各个 RFD 节点的公钥加密共享密钥(除去退出节点拥有边密钥对应边得顶点,剩余顶点做异或运算,产生新的共享密钥)后,使用 Coord 节点私钥加密后发送给剩余的节点,这样就完成了组密钥的更新,同时,将新的边密钥以及密钥标志使用共享密钥用 AES 算法加密后发送给曾经拥有通过边二连接的两个顶点形成的其他边密钥的节点,按照密钥标志对新边密钥进行更新,具体过程如图 3 所示。

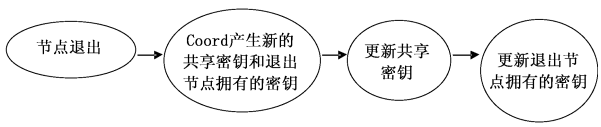

图 3　RFD 节点退出时密钥更新

Fig. 3　Key update when RFD nodes exiting

2.2.5　新的密钥管理方案分析

ZigBee 网络需要满足的安全性基本要求是保密性、可行性、安全性,最为重要的是,要考虑到 ZigBee 网络中节点的计算能力和存储能力有限的现实情况,所以在 ZigBee 网络的密钥管理方案设计中,计算量小,安全性能高,消耗资源少是首先需要考虑到的问题,由于 ZigBee 网络经常会有节点的加入和退出,所以需要考虑好密钥管理方案中密钥更新的问题。在本方案中,节点被捕获以后会进行密钥的更新,以前的密钥会被弃

用,而且开始组建网络的时候使用 ECC 非对称加密的方式分发密钥,保证密钥来源的安全性,增加了对 Coord节点的识别,有效地防止了伪造 Coord 的攻击,节点的退出和新节点的加入都会导致密钥的更新分配,保证了网络的向前、向后私密性。

通过上面的分析我们可以得出,使用新的密钥方案在保证同样安全性的前提下,很大程度上降低了对节点存储能力的要求,每个节点只需要存储数量很少的密钥,就可以实现网络的安全性;每个节点只需要更新较少数量的密钥,就可以完成网络中密钥的更新操作。

使用 MATLAB 对节点数目和密钥数目之间的关系进行分析后绘制出的曲线见图 4。可以看出,在新的密钥管理方案中,仅仅需要数目较少的密钥就可以组建节点数目较大的网络,满足以上公式的 q 和 n 可以做到最大化地减少节点对存储空间的要求,网络的安全性也同样得到保证,而且网络的扩展性良好。

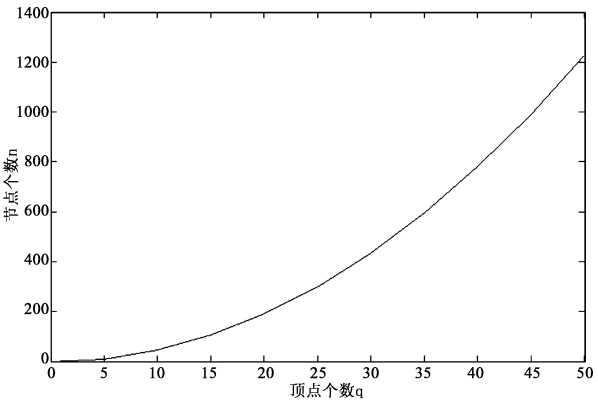

图 4 多边形顶点和节点数目关系曲线

Fig. 4 The relationship between the number of polygon vertex and the number of nodes

3 结论

ZigBee 无线传感网络有别于有线网络,在计算能力、存储空间、能源消耗等方面和有线网络相比存在着很大的不足,而且安全性更容易受到外来的威胁,本文设计的这种基于 ECC 和 AES 混合加密算法的轻量级的密钥管理方案,可以使 ZigBee 无限传感网络的安全性有所提高,同时可以减少计算量,节约资源的消耗,降低对存储空间的要求,提高了网络的健壮性。

参考文献:

[1]李晓延. 浅谈无线传感器网络[J]. 今日电子,2006(9):57 - 59.

[2]孙利民,李建中,陈渝,等. 无线传感器网络[M]. 北京:清华大学出版社,2005.

[3]AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, CAYIRCI E. A survey on sensor networks[J]. IEEE Communications Magazine,2002,40(8):102 - 114.

[4]陈海光. 无线传感器网络中若干安全问题研究[D]. 上海:复旦大学,2008.

[5]黄鑫阳,杨明. 无线传感网络密钥管理研究综述[J]. 计算机应用研究,2007,24(3):10 - 15.

[6]赵宝康. 无线传感器网络隐私保护关键技术研究[D]. 长沙:国防科学技术大学,2009.