6LoWPAN 的节点安全机制①

张小娇[1,2], 贾军营[2], 于 波[2], 蒲泓全[1,2]

[1](中国科学院大学, 北京 100049)
[2](中国科学院 沈阳计算技术研究所, 沈阳 110168)

摘 要: 6LoWPAN 一种近距离的新型无线技术, 它在 WSN(Wireless Sensor Network)方面的应用越来越广泛. 但是, 由于无线信道的开放性使得 6LoWPAN 网络很容易遭受到外来的攻击, 因此保证其安全性也日益成为亟待解决的问题. 以 6LoWPAN 协议栈为基础, 提出了 6LoWPAN 安全体系结构, 设计了 MAC 层、网络层的安全机制以及应用层密钥的生成和管理方案.

关键词: 6LoWPAN; 无线传感器网络; 安全体系结构; 密钥管理

Security Mechanism for 6LoWPAN Node

ZHANG Xiao-Jiao[1,2], JIA Jun-Ying[2], YU Bo[2], PU Hong-Quan[1,2]

[1](University of Chinese Academy of Sciences, Beijing 100049, China)
[2](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China)

Abstract: 6LoWPAN is a short-range new wireless technologies, it is widely applied in WSN (Wireless Sensor Network). However, due to the openness of the wireless channel, 6LoWPAN networks are vulnerable to external attacks, thus ensuring their safety is also increasingly becoming a serious problem. In this paper, based on 6LoWPAN protocol stack, we proposed 6LoWPAN security architecture, and we designed the security mechanisms on MAC layer and network layer and the generation and management scheme for the keys on application layer.

Key words: 6LoWPAN; WSN; security architecture; key management

1 引言

6LoWPAN(IPv6 over Low power Wireless Personal Area Network)是基于 IPv6 的低速无线个域网. 随着 WSN 的广泛应用, 它深入到一些传输敏感信息的领域, 对其安全性的考虑越来越重要[1]. 6LoWPAN 网络既面临着常见的安全攻击, 例如窃听、篡改和伪造等, 又面临着一些在传统网络中不曾出现的安全攻击, 如能量耗尽型的 DOS 攻击[2]. 因此, 在节点计算速度、电池能量、通信带宽和存储空间等资源非常有限的情况下, 设计一种简单的安全机制, 为 6LoWPAN 网络提供一个相对安全的工作环境, 是决定 6LoWPAN 网络能否走向实用的关键. 本文对 6LoWPAN 协议栈的 MAC 层、网络层、应用层等的安全性进行了分析, 根据其安全漏洞, 设计了一套带有安全机制的 6LoWPAN 网络.

2 6LoWPAN技术概述

IETF 组织于 2004 年 11 月正式成立了 6LoWPAN 工作组, 着手制定基于 IPv6 的低速无线个域网标准, 旨在将 IPv6 引入以 IEEE802.15.4 为底层标准的无线个域网.

6LoWPAN 技术底层采用 IEEE 802.15.4 规定的 PHY 层和 MAC 层, 网络层采用了 IPv6 协议. 但是, 由于在 IPv6 中, MAC 支持的载荷长度远远大于 6LoWPAN 的底层所能够提供的载荷长度, 为了实现 MAC 层和网络层之间的无缝链接, 6LoWPAN 工作组建议在 MAC 层和网络层中间增加一个网络适配层, 用来完成包头压缩、分片、重组和网状路由转发等工作[3].

6LoWPAN 的层次结构如图 1 所示.

① 收稿时间:2013-11-08;收到修改稿时间:2013-12-23

图 1　6LoWPAN 的层次结构图

3　6LoWPAN安全分析

3.1 MAC层安全分析

6LoWPAN 网络内通信更多的集中在终端节点和数据汇聚点，数据汇聚点对各个终端节点采集到的数据进行数据融合. 因此必须提供终端节点和数据汇聚点间的安全保证. 在 MAC 层可以引入安全机制，实现访问控制，对收发的 MAC 帧进行加密、解密和完整性验证，身份认证，提供点到点的安全通信.

3.2 网络层安全分析

6LoWPAN 网络数据融合后，数据汇聚点再通过多跳网络将数据传到远端基站. 在 6LoWPAN 网络中，数据汇聚节点之间主要通信方式是端到端通信. 因此必须在网络层提供一定的安全，以保证端到端安全通信. 在网络层采用高级加密标准(AES)和 CTR 模式加密及 CBC-MAC 验证等对称加密算法对大容量数据进行加密.

3.3 应用层安全分析

MAC 层、网络层虽然提供了安全服务，但是只有上层协议建立了密钥、对密钥进行分配，才能充分利用底层提供的安全服务. 应用层的安全主要集中在为整个 6LoWPAN 网络提供安全支持，即密钥建立、密钥传输和密钥管理等. 而且应用层应该能够控制下层安全服务的某些参数，根据具体需求实现一定程度的灵活性[4].

4　6LoWPAN安全体系结构

不同的应用领域对安全有不同的安全需求:商业领域需要更高的安全强度以保护商业秘密，家居环境安全要求相对比较低，因此必须设计支持多个安全级别的安全机制. 同时根据第三节的安全分析，本文设计了一个支持多个安全级别的安全体系结构，如图 2 所示. 该安全体系结构涵盖了 6LoWPAN 协议栈的 MAC 层、网络层、应用层，不同层次具有不同的安全处理机制，它们各自负责相应层数据帧的安全传输，下层对上层负载，各层间安全信息重用，最终实现端到端和点到点的安全通信.

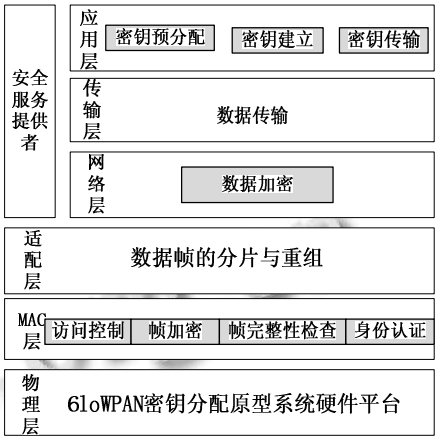

图 2　6LoWPAN 安全体系结构图

如图所示物理层以 6LoWPAN 密钥分配原型系统硬件平台为基础，直接利用无线信道实现 6LoWPAN 网络中的数据传输. MAC 层用于提供节点自身和与其相邻节点之间的数据传输链路，可提供访问控制、数据加密、帧完整性和身份认证等安全服务. 网络层主要负责网络帧的加密传输外，应用层主要做密钥预分配、链路密钥建立、密钥传输等相关工作.

安全服务提供者是 6LoWPAN 安全体系结构的重要组成部分，主要包括 6LoWPAN 密钥分配模型中的安全参数及密码算法库和相关服务接口等.

5　6LoWPAN安全机制设计

5.1 MAC 层安全机制设计

6LoWPAN 底层采用的是 IEEE 802.15.4 规定的 PHY 层和 MAC 层，而 IEEE 802. 15. 4 提供的安全性有限，不能保证终端节点和数据汇聚点间的绝对安全，所以我们对 IEEE802.15.4 提供的安全机制进行了一定程度的改进以增加 MAC 层的安全.

5.1.1 IEEE 802. 15. 4 的安全性分析

lEEE802. 15. 4 在 MAC 层数据传输中提供了三种可供选择的安全模式[5]. 第一种是无安全模式，设备工作在该模式下时，除了对接收的帧的目的地址进行检查外，不做任何其他的安全检查. 如果目的地址是广播地址或本地地址，则将该帧转发给上层，否则被丢弃. 第二种安全模式为 ACL 模式，该模式不提供

加密服务, 只能通过访问控制列表实现访问控制, 确保一个设备只和它希望通信的设备通信. 这种安全模式需要上层采用其它方法保证通信安全. 第三种安全模式在数据传输过程中采用 DES 的对称密码, 对负载数据进行加密.

第三种安全模式虽然它可以用来保护数据和防止攻击者冒充合法节点, 但是它却存在着明显的缺陷, 包括:

1、进行安全通信前必须以安全的方式进行密钥交换. 但是网络不是绝对安全的, 在某 些情况下实现是非常困难的. 不能防止攻击者在双方交换密钥时通过窃听来获取对称密钥. 因此无法保证数据的安全性, 不过可以采用公钥加密的方式来解决这一问题.

2、不能保证数据的保证数据的完整性. 可以采用数据签名的方法来保证数据的完整性.

3、规模复杂. 对于对称密钥每两个人通信的密钥, 必须不同意另外两个人通信的密钥, 否则, 安全性就会受到威胁. 这样如果网络有 n 个节点就需要 $n^2/2$ 个不同的密钥.

通过上面的分析可以知道, 可以使用公钥加密的方法来替代 DES 加密, 来解决以上缺陷. WSN 节点的内存和计算能力都非常有限, 因此 RSA 等密钥过长, 空间和时间复杂度大的公钥不适用, 经过与其他公钥加密体制比较, 选取椭圆曲线公钥算法 ECC. ECC 公钥算法优点, 包括以下几点:

1、安全性能更高.

2、计算量小, 处理速度快.

3、存储空间占用小.

4、带宽要求低.

5.1.2 改进后的 IEEE802.15.4

改进后的 802. 15. 4 采用 ECC 公钥算法增强其 MAC 层安全性能, 网络内所有节点都有自己的密钥对, 各个节点的公钥可以采用离线预设置的办法使其它节点获得,在此基础上利用 ECC 来对源和目的节点等信息进行数字签名和加密. 图 3 和图 4 是该协议的 MAC 帧格式, 由帧头、负载和帧尾三部分组成.

<table>
<tr><td rowspan="2">帧控制信息</td><td rowspan="2">帧序列号</td><td>目的设备 PAN 标识符</td><td>目的地址</td><td>源设备 PAN 标识符</td><td>源设备地址</td><td rowspan="2">帧数据单元</td><td rowspan="2">FCS 校验码</td></tr>
<tr><td colspan="4">地址信息</td></tr>
<tr><td colspan="6">帧头</td><td>MAC 负载</td><td>MFR 帧尾</td></tr>
</table>

图 3 IEEE802.15.4 协议 MAC 帧格式

<table>
<tr><td rowspan="2">帧控制信息</td><td rowspan="2">帧序列号</td><td>目的设备 PAN 标识符</td><td>目的地址</td><td>源设备 PAN 标识符</td><td>源设备地址</td><td rowspan="2">ECC 签名</td><td rowspan="2">帧数据单元</td><td rowspan="2">FCS 校验码</td></tr>
<tr><td colspan="4">地址信息</td></tr>
<tr><td colspan="6">帧头</td><td>签名</td><td>MAC 负载</td><td>MFR 帧尾</td></tr>
</table>

图 4 改进后的 IEEE802.15.4 协议 MAC 帧格式

5.1.3 该协议的流程

1)密钥初始化.

假设一组椭圆曲线的参数为(p, a, b, G, n, h). 其中 p, a, b 用来确定一条椭圆曲线, G 为基点, n 为点 G 的阶, h 是椭圆曲线上总个数 m 与 n 相除的整数部分. 密钥对生成过程如下:

(1) 选择一个随机数 d, 1<d<n-1.

(2) 计算 Q, Q = dG.

(3) 那么公钥为 Q, 私钥为整数 d.

(4) 各个节点可以采用离线预设置的办法获得其它节点的公钥, 公钥预存储在各个传感节点中, 私钥存储在自己的内存中.

2)数据的加密、解密过程.

加密过程: 当节点 A 发送信息 M 给节点 B 时, 执行如下操作:

(1) 查找 B 的公钥 Q;

(2) 将数据 M 表示成一个域元素 m∈Fq ;

(3) 在区间[1, n-1]内选取一个随机整数 k;

(4) 计算(x1,y1)=kP ;

(5) 计算(x2,y2)=kQ, 如果 x2 =0, 回到(3);

(6) 计算 c=m*x2 ;

(7) 传送加密数据(x1,y1,c) 给 B.

解密过程: 当节点 B 解密从节点 A 收到的密文(x1,y1,c) 时, 执行如下操作:

(1) 使用它的私钥 d, 计算点(x2,y2)=d(x1,y1) ;

(2) 通过计算 m=c*x2-1,恢复出数据 m.

3)数字签名的生成和验证

数字签名的生成: 当节点 A 给节点 B 签名信息 M 时, 执行如下步骤:

(1) 将信息 M 表示成二进制串;

(2) 使用一个 hash 函数计算 hash 值 e=H(M),此处采用安全散列算法 SHA-1;

(3) 在区间[1, n-1]内随机选取一个整数 k;

(4) 计算(x1,y1)=kP ;

(5) 计算 r=(x1+e) mod q;

(6) 利用私钥 d 计算 s=(k-dr)mod n;

(7) A 传送给 B 信息 M 和签名(r,s).

数字签名的验证: 当节点 B 验证 A 对信息 M 的签名(r,s)时, 执行如下步骤:

(1) 查找 A 的公钥 Q;

(2) 计算点(x1,y1) =sP+qR;

(3) 计算 hash 值 e=H(M);

(4) 计算 r=(x1+e) mod q;

(5) 接受 A 对信息 M 的签名当且仅当 r=r[6].

改进后的协议增加了数据的完整性、身份的真实性和抗否认等三种安全服务, 具有更高的安全性. 比起 RSA 算法, ECC 具有更短的密钥和相同的安全级别, 因此改进后的协议具有更好的网络性能.

5.2 网络层安全机制设计

由于 IPSec 太复杂, 开销太大, 并不适用于 6LoWPAN 网络, 需要重新设计一种网络层安全机制. 使其提供的安全服务和 IPSec 一致, 本文仿照 AH 和 ESP 的方法, 在 IPv6 包头后面引入一个扩展安全报头.

IPv6 数据包在传输过程中, 包头中的有些字段可能发生变化, 例如跳数限制字段, 所以不能对原始包进行认证, 必须把变化字段变成固定值, 例如可以把跳数限制字段设置成 0, 然后对整个 IPv6 包头进行认证. 接收到 IPv6 包后, 也把变化字段变成固定值, 然后按照发送方的安全模式进行认证. 而且 IPv6 数据包在传输过程中需要中间节点处理, 所以 IPv6 包头和扩展报头不能加密, 只对 IPv6 负载加密.

5.2.1 IPv6 数安全格式设计据包

扩展安全报头的内容包括下一包头字段、采用的安全级别、密钥类型、帧计数器和密钥序列号.

安全扩展报头:

下一个包头	安全控制	
帧计数器		密钥序列号

下一个报头占一个字节, 标识 IPv6 上层协议; 安全控制占一个字节, 标识安全级别(3 比特)和密钥类型(2 比特); 帧计数器是标记安全处理后发送的数据帧. 密钥序列号是标识采用的网络密钥.

安全处理后的 IPv6 包格式如图 5 所示:

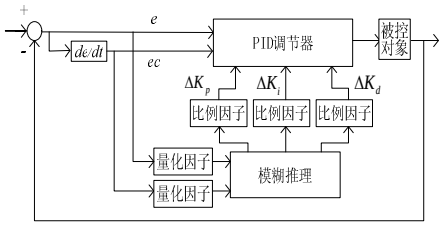

图 5 安全处理后的 IPv6 包格式

5.2.2 网络层数据包安全模式处理流程

在网络层收到未经过安全处理的 IPv6 包后, 根据是否添加安全性, 将进行安全处理或者直接发送出去, 具体安全处理流程[4]如下:

(1)根据源 IPv6 地址和目的 IPv6 地址查找链路密钥 , 如果找不到则缓存该数据包, 并触发 Link key 建立协议, 如果密钥建立失败, 则采用缺省的安全材料.

(2)根据得到的安全材料设置安全扩展报头, 并对 IPv6 包头进行如下修改: 下一个报头标识为安全扩展报头, 负载长度更新为加上安全扩展报头后的长度.

(3)设置安全级别、密钥类型、帧计数器和密钥序列号等安全处理参数.

(4)开始硬件安全处理.

(5)把硬件处理后的密文读到缓存中. 此时网络层处理完毕, 数据包将被传送到 MAC 层进行进一步处理.

5.3 应用层安全机制设计

根据前面的安全分析, 本文在应用层提供了密钥分配协议. 根据 6LoWPAN 网络的特点, 本文设计了如图 6 所示的密钥分配模型, 用于指导密钥分配方案的设计, 以保证网络中各类密钥分配的安全性[7].

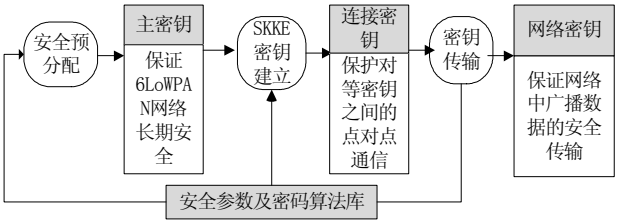

图 6　密钥分配模型

如图 4 所示, 在该分配模型中, 安全参数和密码算法库为密钥分配提供必需的安全参数和密钥算法. 主密钥用于保护链接密钥和网络密钥的安全建立和传输, 是节点之间安全通信和网络长期安全的基础. 链接密钥主要用于保护两个对等实体之间的点对点通

信, 同时也可应用于网络密钥的传输服务. 网络密钥主要用于保护网络中所有节点广播数据的安全传输, 在链接密钥安全建立的基础上, 网络密钥可以通过安全的密钥传输服务获得. 由于密钥传输服务的执行过程相当简单且均是在已有共享密钥保护的情况下通过对称密钥加密算法完成, 所以网络密钥的建立不作为本文的研究重点, 本文主要对主密钥的分配和链接密钥的建立进行设计.

5.3.1 主密钥分配

本文主密钥分配方案是根据不同节点深度设计的, 主要包括密钥参数预分配和主密钥协商两个阶段[7,8].

5.3.1.1 密钥参数预分配

本文主要基于基本的 Blom 密钥对预分配模型来进行密钥参数的预分配, 原理是利用在有限域上形成密钥对生成矩阵来定义所有相邻节点之间的共享密钥对.

在密钥参数预分配阶段, 由离线服务器为节点预置从一个或多个密钥空间中抽取出的密钥参数, 具体过程如下:

生成一个$(\lambda+1)\times N$ 的公开矩阵 G 和 ω 个$(\lambda+1)\times(\lambda+1)$的对称私密矩阵 $D_1,D_2,\ldots\ldots D_{w,}$ 每一对(D,G)称为一个密钥空间. 离线服务器分别计算 $Ai=(Di\cdot G)^T$,每个节点根据其深度随机选择 τ 个密钥空间.

5.3.1.2 主密钥协商

节点在完成密钥参数的预分配后, 可以与邻居节点进行主密钥协商. 节点加入网络后, 首先确定自身是否于邻居节点拥有相同的密钥参数空间. 为此, 节点广播包含节点号、节点深度、安全系数和密钥参数的等参数的数据包, 收到此广播数据包得相邻节点根据如下图所示的流程完成与其之间主密钥对的协商, 具体过程如下图 7 所示:

5.3.2 链接密钥的建立

由于常规网络上的密钥建立机制并不适合 6LoWPAN 的特性, 而且针对无线传感器网络提出的密钥管理机制在扩展性和可行性上也有欠缺. 针对以上问题, 本文提出基于对称密钥的密钥建立协议 SKKE(Symmetric Key Key Establishment)的设计方案[9].

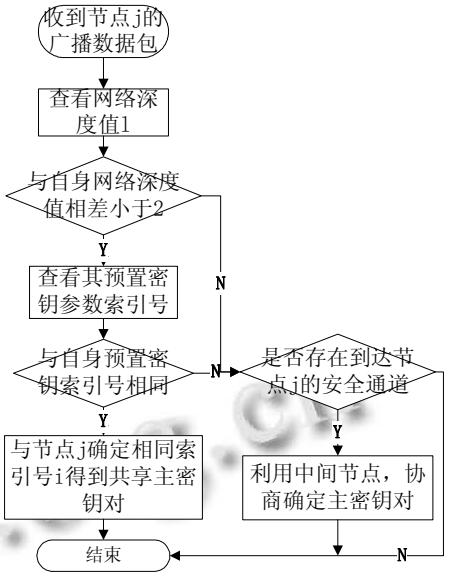

图 7 主密钥协商

5.3.2.1 SKKE 协议主要设计思想

SKKE 以共享主密钥为基础, 在要通行的节点之间建立共享密钥. 主要包括以下四个步骤:

(1)交互双方共享的主密钥;

(2)互相交换各自的随机数据, 分别为 QEU 和 QEV;

(3)双方根据这两个随机数用密钥导出函数 SKG 生成一个共享密钥 Key, 再用这个 Key 和双方已经共享的主密钥使用 KDF 推导出密钥数据 KKeyData, 将 KKeyData 的左边作为用于确认密钥的 MAC key, 剩下的作为用于加密的密钥 KeyData.

(4)双方都使用 MAC key 对事先约定好的数据计算 MacTag 值, 接收到对方发来的 MacTag 值后, 同时自己也用 MAC key 计算该 MacTag 值, 通过比较这两个 MacTag 来确定对方所拥有的 MAC key 自己导出的是同样地, 从而推导出的 KeyData 也是相同的[9].

5.3.2.2 SKKE 帧格式

密钥建立过程要使用 SKKE 帧, 该帧的格式如图 8 所示:

帧控制	命令标识符	初始地址	响应地址	数据
帧头	负载			

图 8 SKKE 命令帧格式

命令标示符域: 表示 SKKE 帧的类型, 主要有 SKKE-1、SKKE-2、SKKE-3、SKKE-4 四种类型.

初始地址域: 表示 SKKE 发起者的 64 位扩展地址.

响应地址域: 表示 SKKE 响应者的 64 位扩展地址.

数据域的内容是由命令标示符决定的, 如果是 SKKE-1 帧, 数据域的内容是 SKKE 的发起者产生的 QEU, 如果是 SKKE-2 帧, 数据域的内容是 SKKE 的响应者产生的 QEV,如果是 SKKE-3 帧, 数据域的内容是 SKKE 的发起者产生的 $MacTag_2$, 如果是 SKKE-4 帧, 数据域的内容是 SKKE 的响应者产生的 $MacTag_1$[11].

5.3.2.2 应用层链接密钥建立流程

应用层链路密钥建立协议主要由 SKKE 发起者处理和 SKKE 接受者处理两个过程完成.

SKKE 发起者处理处理流程如下:

(1)首先判断是不是 SKKE-1, 是则转(2), 否则转(3).

(2)查找当前可用的安全资料, 如果找到, 则转(3), 否则返回错误 ERRO, 结束.

(3)检查当前 SKKE 状态, 如果状态错误, 则返回错误 ERRO, 如果是发送 SKKE-1, 转(4), 接收到 SKKE-2, 转(5), 接收到 SKKE-4, 转(6).

(4)生成 QEU, 设置 SKKE 状态和 SKKE-1 头部, 将 QEU 放入 SKKE 的数据字段, 发送 SKKE-1, 转(8).

(5)生成 MacKey 和 KeyData, 计算 MacTag2, 设置 SKKE-3 头部, 将 MacTag2 放入 SKKE 的数据字段, 发送 SKKE-3, 转(8).

(6)生成 MacKey 和 KeyData, 计算 MacTag1, 与接收到 SKKE-4 的数据字段中的 MacTag1 进行比较, 如果不相同则, 转(7), 否则转(8).

(7)返回错误.

(8)成功返回.

SKKE 接受者处理流程如下:

(1)接收到的 SKKE-1, 则转(2), 接收到 SKKE-3, 转(3).

(2)查找到当前可用的 AclEntry, 如果找到, 则转(3), 否则返回错误 ERRO, 结束 .

(3)检查当前 SKKE 状态, 如果状态错误, 则返回错误 ERRO, 如果接收到的 SKKE-1, 转(4), 接收到 SKKE-3, 转(5).

(4)生成随机数 QEV, 设置最新 SKKE 状态, 和 SKKE-2 头部, 将 QEV 放入 SKKE 的数据字段, 发送 SKKE-2, 转(7).

(5)生成 MacKey 和 KeyData, 计算 MacTag2, 与接收到 SKKE-3 的数据字段中的 MacTag2 进行比较, 如果不相同转(6), 否则转(7).

(6)返回错误.

(7)成功返回[9,10].

综上所述, 本文可以得出在 6LoWPAN 网络中的密钥分配是如下过程: 首先, 依据密钥参数预分配方案设计为每个 6LoWPAN 节点预置密钥参数. 新加入 6LoWPAN 网络的节点与网络中的可信节点进行主密钥协商, 完成主密钥预分配.

在主密钥预分配完成后, 节点可利用 SKKE 协议建立链接密钥, 利用安全传输密钥命令传输网络密钥. 至此, 6LoWPAN 密钥分配完成, 新加入节点可以与网络中的节点安全通信.

6 结语

6LoWPAN 技术有着广阔的应用前景, 但是要使 6LoWPAN 得到更加快速的发展和应用, 就需要解决 6LoWPAN 网络的安全问题. 本文以 6LoWPAN 协议栈为基础, 提出了 6LoWPAN 安全体系结构, 设计了 MAC 层、网络层的安全机制以及应用层的密钥生成和管理方案, 为 6LoWAPN 网络通信提供了安全保证, 从通信协议底层保证了信息安全, 但是这是远远不够的, 还需要进一步的研究.

参考文献

1 刘外喜,唐冬,胡晓,郑晖.6LoWPAN 网络安全问题的分析.电信科学,2010,4:66–70.

2 朱政坚,谭庆平,朱培栋.无线传感器网络安全研究综述.计算机工程与科学,2008,30(4):101–105.

3 吴俊.6LoWPAN 技术分析.铁道通信信号,2006,42(12):38–40.

4 王志克.6LoWPAN 协议栈及安全机制研究与实现[硕士学位论文].北京:北京交通大学,2006.

5 杨剑,杨铭熙,李腊元.增强安全性的 IEEE802.15.4 协议研究.计算机技术与发展,2007,17(12):136–139.

6 江志祥,蔺志青.椭圆曲线密码体制.北京:北京邮电大学,2011.

7 杨同豪.Zigbee 密钥分配方案的设计与实现[硕士学位论文].郑州:解放军信息工程大学,2012.

8 王鹿媛.无线传感情网络的密钥预分配方案研究.南京:南京理工大学,2013.

9 鲁慧.6LoWPAN 分析与设计[硕士学位论文].上海:华东师范大学,2007.

10 周公博,韩振铎,胡宁宁.ZigBee 标准的密钥协商机制分析.电子技术应用,2007,(10):158–160.

11 张旖旎.ZigBee 协议的安全层研究与实现[硕士学位论文].沈阳:沈阳工业大学,2008.