

KNXnet/IP 协议安全性分析与改进

刘君昌,张曦煌

(江南大学 物联网工程学院,江苏 无锡 214122)

(liujc101@163.com)

摘要:KNXnet/IP 协议作为欧洲安装总线(EIB)协议的扩展应用,提高了 EIB 系统的传输速率并满足了智能管理的需求,但分析表明以 IP 网络作为骨干网的 KNXnet/IP 协议在安全性要求较高的应用领域内面临严重的威胁。在分析现有 IP 网络安全机制及嵌入式系统特点的基础上,提出适用于 EIB 系统的安全加密通信协议,该安全协议以非对称加密算法为基础,使用自定义的密钥交换协议管理密钥集,设备之间使用对称加密算法通信,具有对原协议架构改动较小、提供数据透明传输的特点,协议的原型实现证明了其可行性和安全性。

关键词:KNX/EIB 协议;IP 骨干网;嵌入式网络;密钥集管理;椭圆曲线加密算法

中图分类号:TP393.08 **文献标志码:**A

Security analysis and improvement of KNXnet/IP protocol

LIU Jun-chang, ZHANG Xi-huang

(School of Internet of Things Engineering, Jiangnan University, Wuxi Jiangsu 214122, China)

Abstract: As the extended application of European Installation Bus (EIB) protocol, KNXnet/IP protocol increases the transmission speed of EIB system and fulfills the requirement of intelligent management. But the security of KNXnet/IP protocol is heavily threatened in the security-critical environment. A security protocol was proposed after analyzing the security mechanism of IP network and embedded system. The security protocol used self-defined key sets distribution protocol based on asymmetric cryptography algorithm and used symmetric cryptography algorithm for communication. It provides transparent data transmission and only needs very few changes of the primary architecture. The implementation proves the feasibility and security of the security approach.

Key words: KNX/EIB protocol; IP backbone network; embedded network; key sets management; Elliptic Curve Cryptography (ECC) algorithm

0 引言

欧洲安装总线(European Installation Bus, EIB 也称 KNX/EIB)协议在楼宇及家居自动化中有着非常广泛的应用,它不仅是事实上的欧洲规范,还被美国消费电子制造商协会(Consumer Electronics Manufacturers Association, CEMA)批准为家庭网络 EIA-766 标准^[1]。最初的 EIB 系统设计为孤立的网络,可以在物理层保证系统的安全,因此安全性一直是 EIB 系统的边缘问题,但是随着应用的扩展以及智能网络监控的需要,必须将 EIB 网络接入更加高速的骨干网络。由于 IP 网络具有广泛的应用,并且很多的嵌入式处理器都配备有网络接口,因此 IP 网络作为扩展被选为 EIB 系统的骨干网,但使用 IP 网络同时将 EIB 系统暴露在了整个 IP 网络中,使得对 EIB 系统的访问变得非常容易,并且 IP 协议和其底层的链路层协议没有提供数据通信的安全机制,因此带来极大的安全隐患^[2]。目前广泛使用的安全协议如网络层安全(Internet Protocol Security, IPsec)协议、传输层安全(Transport Layer Security, TLS)协议等由于多播支持及复杂性问题不能直接应用到 EIB 系统中。文献[3]提出了使用 Diffie-Hellman 算法交换密钥并使用高级加密标准(Advanced Encryption Standard, AES)加密数据的方法提供 EIB 设备间的安全通信,但使用 Diffie-Hellman 密钥交换算法无法抵御重放攻击,而且在多播

组中协商出公用的密钥非常困难,耗时很大。本文分析了 KNXnet/IP 协议的安全性,根据其安全性特点提出了四点安全需求,然后分析对比了现有的较符合 KNXnet/IP 协议需求的 IP 网络安全机制,在综合分析它们的特点和不足的基础上提出了基于自定义的密钥交换协议的安全 KNXnet/IP 协议。协议安全层位于 KNXnet/IP 应用层与传输层之间,因此能够提供透明的数据传输,同时对原系统架构改动很小,它将通信过程分为设备认证、密钥集分发和安全通信三个部分,可以支持单播和组播的应用需求。最后对安全协议的安全性进行分析并通过原型实现证明了协议的安全性。

1 KNXnet/IP 协议

1.1 KNXnet/IP 协议安全性分析

将 EIB 协议的实现集成到 IP 网络之上叫做 KNXnet/IP 协议,IP 网络作为 EIB 系统的快速骨干网。KNXnet/IP 提供的主要服务为路由和隧道。使用隧道服务,KNXnet/IP 的客户端可以和 KNXnet/IP 的服务器端通过 IP 网络建立点对点的连接;使用路由服务可以连接多个 EIB 子网络。在 KNXnet/IP 的安全规范中,只有一些基本的安全准则,这些准则是基于隔离(如防火墙、EIB 专用网络等)和非标准(如非标准 IP 地址等)的方法^[4],其安全性很大程度依赖于攻击者对 EIB 系统不熟悉,因此这种安全策略是不可靠的。

收稿日期:2011-01-10;修回日期:2011-02-27。

作者简介:刘君昌(1987-),男,山东临沂人,硕士研究生,主要研究方向:嵌入式系统、计算机网络;张曦煌(1962-),男,江苏无锡人,教授,主要研究方向:嵌入式系统、计算机网络。

1.2 协议安全性要求

为 EIB 网络提供安全通信的 IP 骨干网必须满足如下的安全及实际应用需求^[5]:

实体相互认证 为防止攻击者模仿网络中的合法设备,通信对象之间必须先相互认证,只有得到认证的设备才能和其他设备进行通信。

安全通道 为了实现数据在通信对象之间的安全交换,数据交换过程必须在安全的通道中完成,安全通道需使用加密算法来保证数据的完整性、新鲜性和保密性^[6]。

多对多连接 EIB 协议支持的通信方式很多,包括单播、组播和广播,因此安全协议必须能够为多对多的连接方式提供安全通信。

嵌入式设备 EIB 现场设备都是嵌入式设备,资源非常有限,而安全协议和加密算法都是资源密集型的,因此必须根据嵌入式设备的特点设计合适的通信协议。

1.3 IP 骨干网安全机制

IP 网络使用广泛,目前已存在多种网络安全协议,较符合上面提出的安全需求的有 IPsec 协议和 TLS 协议,下面对其分析。

IPsec 是提高 IPv4 安全性的增强版本^[7],它提供实体间相互认证并能保证数据的完整性、新鲜性、保密性。IPsec 定义了不同的加密算法用来加密以及生成数字签名,如使用 DES、三重 DES、AES 等作为加密算法,使用 HMAC-SHA1 计算消息鉴别码(Message Authentication Code, MAC)值等。IPsec 使用网络密钥交换(Internet Key Exchange, IKE)协议^[8]交换密钥,IKE 使用 Diffie-Hellman 算法生成加密及数字签名所需的密钥,同时 IPsec 提供单播和多播服务,原则上可以对 KNXnet/IP 的 IP 骨干网提供保护,但在多播服务中如果有多个发送者,那么用于防止重放攻击的序列号在发送者之间必须做到同步。另外就是密钥的分发,因为 IKE 使用的是 Diffie-Hellman 算法,想要在多播组中生成一个共用的密钥是非常困难的,使用单独的密钥服务器可以解决这个问题,但是其成本太昂贵,而且这容易因为密钥服务器的失效而导致网络瘫痪。

TLS 协议^[9]是用来确保实体之间通信安全的,在协议的初始化握手阶段,实体之间进行相互认证,协商加密算法并交换共享密钥,初始化完成之后实体之间使用获得的密钥建立安全通道。和 IPsec 一样, TLS 在握手交换密钥阶段通常使用非对称加密算法,而在安全通信时使用对称加密算法。TLS 在加密算法选择方面非常灵活,使用椭圆曲线密码算法(Elliptic Curves Cryptography, ECC)的 TLS 协议耗用的资源很少,完全可以在嵌入式设备上实施。但是因为 TLS 是单播协议,没有对多密钥交换的扩展支持,只能对 KNXnet/IP 的隧道服务提供安全保障,而无法对路由功能的多播服务进行保护,因此也无法直接应用于 KNXnet/IP 协议。

2 改进的 KNXnet/IP 安全协议

以上的分析表明每种安全机制都有它们的优点以及现实应用中的不足,没有一种协议的直接应用能够满足 EIB 系统的安全要求。对 TLS 协议的分析表明它基本符合系统的安全需求,但其对多播不提供原生态的支持,而基于 IPsec 协议的 GDOI 协议是一个组安全管理协议,支持多播密钥管理。因此,在综合分析现有协议的基础上提出了一种满足 EIB 网络特点要求的安全协议,该协议安全层位于 KNXnet/IP 协议

应用层与传输层之间,这样的最大优点就是提供透明的数据传输,不会对原有 KNXnet/IP 网络产生任何影响。

为了能够和其他的设备安全地进行通信,每个设备需要和其他设备之间建立一个安全的通信通道,数据在通信通道中传输时采用加密算法进行加密。对于加密算法,可供选择的有对称加密算法和非对称加密算法,由于每次数据的收发都需要加密和解密,而非对称加密算法的时间以及空间复杂度太高,不适用于此处的通信要求。另外相比于非对称加密算法,使用对称加密的通信对象之间只需要分享单个的密钥集,一个消息在组内只需要发送一次,因此这里选择的是对称加密算法。由于对称加密算法通信的双方需要持有相同的密钥,因此如何协商以及获得密钥是要重点解决的问题。提出的安全协议将安全通信分为设备认证、密钥集分发和加密通信三个阶段,在设备认证阶段,设备从认证中心获得有效证书及认证中心的公钥,这些用来保证将密钥集分发给合法的设备而避免攻击者得到密钥集;在密钥集分发阶段,设备间协商获得安全通信所需要的密钥集,并在第三阶段的通信中使用该密钥集加密数据,完成安全通信。

2.1 设备认证

设备认证的过程如图 1 所示,其中 Device A 表示将要加入网络的设备,CA 表示担任认证中心(Certificate Authority, CA)角色的管理工具(Management Tool, MT), P_A 表示设备 A 的公钥, P_M 表示 MT 的公钥, $Addr_A$ 表示设备 A 的地址, $Cert_A$ 表示设备 A 的证书。在此阶段内,设备从 CA 处获得数字证书,由于数字签名及数字证书需要用到非对称加密算法,非对称加密算法复杂度高,对嵌入式设备的速度及存储都是一个挑战,而椭圆曲线密码(Elliptic Curve Cryptography, ECC)算法^[10]的出现,使得非对称加密算法能够应用在嵌入式设备上,相比与广泛使用的 RSA, ECC 提供更小的密钥长度、更快的计算速度、更小的空间占用等,并且使用 ECC 不再需要单独的密钥服务器^[11],这里选择的 ECC 密钥长度为 256 位。

首先每个设备生成一个 ECC 密钥对(公钥/私钥),然后设备的公钥通过一条在物理上安全的通道发送给 CA,这是由于设备认证阶段是用来初始化安全口令的,不可能使用加密技术来建立一条安全的通道,因此采用设备与 MT 直接通过串口点对点相连的方式来完成,此时设备的私有密钥依然保持其安全性。接着 CA 生成包含设备公钥及其 IP 地址签名的证书,此证书连同 CA 本身的公钥一同发送给设备,依靠此证书设备即可在密钥分发阶段证明自己的身份,使用 CA 的公钥设备也可以在后续的通信过程中确认其他设备的合法性。

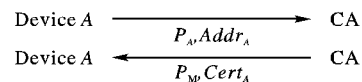


图 1 设备认证过程

2.2 密钥集分发

设备认证及初始化配置完成后,设备拥有三个口令:自身生成的密钥对、CA 的公钥以及从 CA 获得的证书,使用这些口令设备即可开始第二阶段的密钥集分发过程。在此过程中非常重要的一个角色称之为密钥服务器(Key Server, KS), KS 在网络中不是一成不变的,多播组中每个设备都有可能成为 KS,这样可以避免因单服务器失效而引起的网络瘫痪。单播与多播的密钥集分发过程有较大差别,分别讨论。

对于单播服务,通信双方分别为客户端和服务端,此时服

务器被选作 KS。密钥集的请求与分发过程如图 2 所示,图中箭头上是发送消息的名称,下方是该消息中包含的内容,圆圈内是对消息签名使用的密钥,椭圆圈内是对消息加密使用的密钥。为了获得密钥集,客户端首先向服务器发送一个 Hello 消息,此消息包含客户端的临时变量 N_1 及其自身证书,且消息经过客户端的私有密钥签名。服务器收到 Hello 消息后确认消息的签名及证书的合法性,如果签名及证书均合法,服务器会立即响应一个经服务器签名的 KS_avail 消息,此消息包含 Hello 消息中的 N_1 及新的变量 N_2, N_1 用来证明 KS_avail 消息是合法的服务器响应,从而避免攻击者的重放攻击。客户端收到 KS_avail 消息后同样通过服务器的签名、证书以及临时变量 N_1 判断消息的合法性。如果证明收到的消息为合法的服务器的响应,客户端可以发送消息请求密钥集,请求密钥集的消息称为 Key_req 消息,同样为了避免重放攻击,它包含服务器应答消息中的 N_2 ,还包含新生成的 N_3 临时变量。服务器收到消息后检查消息的合法性,如果合法,则将包含密钥集 (KS_C) 及 N_3 的 Key_resp 消息发送给客户端,Key_resp 是经 KS 私钥签名并使用客户端公钥加密的,这样可以确保只有请求此密钥的设备才可以成功解析出密钥集,客户端在收到此消息并确认其合法性后保存密钥集,密钥集在下一阶段的安全通信中使用。至此,单播服务的密钥分发过程完成。

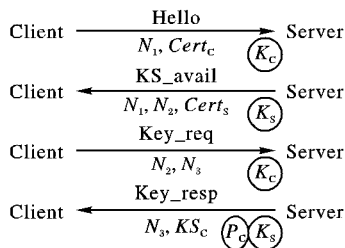


图 2 单播服务的密钥集获取过程

对于多播服务,情况较复杂,多播组中的密钥服务器不再是预定义的,每个多播组中有一个负责密钥集分发的密钥服务器。一个设备要加入多播组时,它同样向多播组发送一个 Hello 消息,此时取决于多播组的状态分为以下三种情况。

1) 如图 3,如在 t_{70} 时间内,设备 A 没有收到其他 IP 设备的回应,那么设备 A 就认为自己是此多播组内第一个激活的设备并开始担任 KS 的角色,为了宣布它本身的 KS 身份并避免此多播组内的其他设备继续成为 KS,设备 A 发送一个 KS_beg 消息,消息发送完毕后设备 A 生成此多播组的密钥集,生成密钥集所需要的时间为 t_{GK} ,生成密钥集结束后,设备 A 发送 KS_establ 消息。如果有 2 个设备在时间 t_{70} 内同时成为了 KS,那么具有较低 IP 地址的一个会最终被选为 KS,一个设备确认其 KS 的角色后其他的设备都要取消其正在成为 KS 的过程。另外, t_{70} 需要大于 t_{GK} ,这样第二个设备将会在它发出 KS_beg 消息前收到一个 KS_establ 消息,以防止密钥集生成过程中产生冲突。

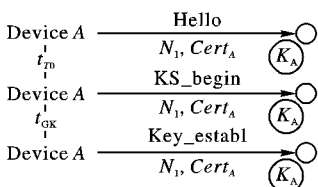


图 3 单设备密钥集获取过程

2) 如果此时组内已有一个设备担任了 KS 角色,在设备 A

发送 Hello 消息后 KS 会应答设备 A 发出的 Hello 消息,接下来的步骤和单播服务的密钥集分发过程相同,如图 2 所示,不再赘述。

3) 如图 4,如果组内已有一个 KS,但因为某种原因(如 KS 已经崩溃了)没有对新设备的密钥集请求做出回应,那么新加入的设备会尝试成为组内新的 KS,它会发送一个 KS_begin 消息,组内的其他成员收到此消息后响应 KS_establ 消息以告知新设备组内已存在一个密钥集,此回应消息包含 KS_begin 消息中的 N_1 和新的 N_2 ,新设备会从众多的响应消息中选择一个进行授权并发送 Key_req 消息请求密钥集,此时组内被选中的设备将密钥集经过签名和加密后发送给设备 A,设备 A 收到密钥集后将密钥集保存并取代之前 KS 的角色成为组内新的 KS,它通过广播 KS_establ 消息通知其他设备,这样新的 KS 就可以对以后加入该组的设备分发密钥集。

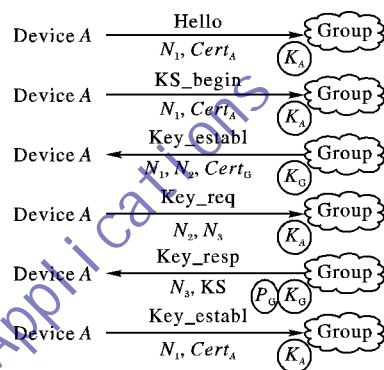


图 4 KS 无响应时获取密钥集过程

2.3 加密通信

密钥集分发完成后,便可在通信对象之间建立安全通道,密钥集内包含三个安全口令:安全密钥 SK_C 用来加密和解密数据、密钥 SK_{MAC} 用来进行 MAC 计算、当前的有效计数器 C 。通信的数据格式使用基于 TLS1.2 应用协议的帧格式,如图 5 所示。此数据帧中的数据分为加密部分和非加密部分,非加密部分包括 Ethernet 头、IP 头、TCP/UDP 头以及 Ethernet 尾,这些是 TCP/IP 协议规定格式,无需加密。加密部分则包括初始化向量 IV、KNXnet/IP 数据帧、MAC、Padding、Padding length 以及加密部分的总长度 Length。加密部分又分为两种情况:其中计算 MAC 值的部分可以保证数据的完整性;进行加密计算的部分则可以保证数据的保密性。另外 IV 的使用可以保证数据的新鲜性,避免重放攻击。

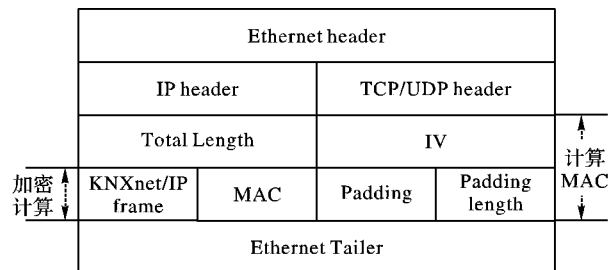


图 5 安全协议帧格式

计算 MAC 值使用的是散列消息鉴别码 (Hash Message Authentication Code, HMAC), 基于密钥的 Hash 算法认证协议。HMAC 实现鉴别的原理是:用公开函数和密钥产生一个固定长度的值作为认证标识,用这个标识鉴别消息的完整性。数据发送方使用密钥生成一个固定大小的数据块 MAC,并将其加入到消息中,接收方利用与发送方共享的密钥进行鉴别认证。MAC 的计算表示如下:

$MAC = HMAC (SK_{MAC}, C \parallel Length \parallel IV \parallel User\ data \parallel$
 $Padding \parallel Padding\ length)$

其中, SK_{MAC} 即是从密钥集中获得的密钥, 第二个参数如图 5 中数据帧格式所示。

使用 HMAC 算法需要一个散列函数, 这里选择的是 SHA_256, 其计算方法如下:

$HMAC(SK_{MAC}, text) = SHA_256((SK_{MAC} \text{ XOR } opad) \parallel$
 $SHA_256((SK_{MAC} \text{ XOR } ipad) \parallel text))$

其中, $ipad = 36h$, $opad = 5Ch$, 密钥 SK_{MAC} 和 $ipad$ 异或操作后和 $text$ 连在一起, 再经过 SHA_256 函数后连接到 SK_{MAC} 与 $opad$ 异或后结果的后面, 最后再经过一次 SHA_256 函数计算即可得到结果。

对于加密计算的数据部分, 使用密码段链接 (Cipher Block Chaining, CBC) 模式的 AES_128, 加密的过程如下:

$CIPHERTEXT = AES_128_CBC (SK_C, IV, User\ data \parallel$
 $MAC \parallel Padding \parallel Padding\ length)$

AES_128_CBC 加密过程有三个参数作为输入: 共享密钥 SK_C , 明文 ($User\ data \parallel MAC \parallel Padding \parallel Padding\ length$) 和 IV , 为避免 CBC 模式下的攻击, 初始化向量 IV 使用随机数。

2.4 证书吊销及密钥集更新

当由于某种原因 (证书过期、密钥泄露等) 设备对通信网络构成威胁时, 需要立即把它从整个通信网络中排除, 这包括设备证书的吊销以及密钥集的更新; 另外为了减少密钥集的使用次数从而减少密钥集泄露的风险, 也需要周期性的更新密钥集。设备证书的吊销需要一张由 CA 维护的证书吊销列表 (Certificate Revocation List, CRL), CRL 是一个被签署的列表, 它指定了一套 CA 认为无效的证书。当一个设备被认为无效后, CA 将其证书序号添加进 CRL, 然后通过发送 $cert_revoke$ 消息通知网络内所有设备, 此消息经过 CA 的私钥签名。设备收到此消息后首先通过 CA 公钥判定消息合法性, 然后将 CRL 存储用来在以后的通信中判定其他设备的有效性。设备被排除后密钥集可能泄露, 因此网络内的各通信组需要更新密钥集, 其过程如图 6 所示。

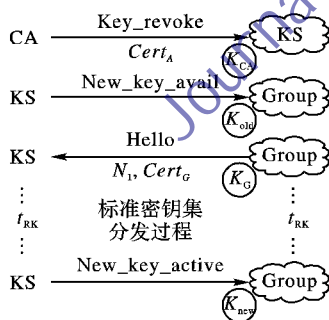


图6 密钥集更新过程

首先由 CA 发送 Key_revoke 消息给网络内的所有 KS, KS 在收到消息后重新生成密钥并通过旧有密钥加密一条 New_key_avail 消息通知通信组内的设备, 组内的其他设备收到此消息后则按正常的密钥集获取步骤重新获取密钥集, 在一段可配置的时间 t_{RK} 后, 各通信组的 KS 发送一条 New_key_active 消息以通知组内所有设备开始使用新的密钥集。另外当密钥集的生命周期结束时同样需要更新密钥集, 各通信组内的 KS 计算密钥集的生命周期结束时间, 密钥集生命周期结束时 KS 同样生成新的密钥集, 和上面提到的密钥分发方法不同的是通信组内的设备不需要重新请求密钥集, 而是由 KS 直接发送一条经旧有密钥加密的 New_keyset 消息, 此消息

内包含新的密钥集, 设备收到消息后获取新密钥集并保存, 同样在一段时间 t_{RK} 后 KS 发送 New_key_active 消息, 之后所有组内设备开始使用新密钥集加密通信。

3 改进协议的安全性分析及实现

在设备认证阶段 CA 颁发证书给设备, 这是协议的初始阶段, 通过在物理层上的安全通道可以保证只有合法设备才能获得证书, 为后续的密钥集分发提供设备合法性保证。

第二阶段的密钥集分发在设备认证完成的基础上进行, 在密钥集分发之前设备已拥有 CA 颁发的设备证书、自身生成的密钥对以及 CA 的公钥。设备在获取密钥集阶段发送自身的证书, KS 通过证书判定设备的合法性, 同时设备发送的消息经过私钥加密, 非法的 KS 没有设备的公钥, 因此无法冒充合法 KS 对设备作出回应。KS 向新加入的设备发送密钥集时同样发送 KS 的证书以及使用私钥加密消息, 可以防止非法设备获得密钥集。另外设备在发送消息时都附带临时变量 N , 设备在收到的消息中确认 N 的合法性, 如果收到的 N 与之前发送的 N 相同, 则证明此消息为合法的设备发来的消息, 否则就可能是非法设备截获的之前的消息现在重放来对设备进行攻击。

密钥集分发协议确保设备收到合法安全的密钥集, 密钥集包括了计算 MAC 的密钥, 使用 HMAC 算法计算 MAC 可以保证数据的完整性, 而使用 CBC 模式的 AES_128 加密算法能够保证消息的保密性, 计数器 C 用来保证消息的新鲜性, 满足 2.2 节中提出的协议安全需求。

为了验证提出的改进安全协议, 实现了设备硬件及软件原型。硬件方面, 其控制器芯片选用的是 LM3S8962, 它是基于 ARM Cortex-M3 内核的微控制器, 包括 256 KB 单周期 Flash 以及 64 KB SRAM, 最高工作频率可达 50 MHz, 处理器还包含 UART 模块以及以太网控制模块。处理器的一端通过以太网芯片接入 IP 网络, 另一端通过 UART 端口连接 TP-UART^[12] 以访问 EIB 网络。设备的软件模型如图 7 所示, 安全协议层位于 TCP/IP 协议与 KNXnet/IP 应用层之间, 其中使用开源的 LWIP (Light Weight IP) 协议栈作为 TCP/IP 栈, 它具有很小的体积并提供所有需要的功能。对于加密算法的实现, 使用的是 Multiprecision Integer and Rational Arithmetic C Library (MIRACL) 库, 它提供二进制及素域内的 AES, RSA, Diffie-Hellman, ECC 等加密算法以及众多哈希功能。另外, KNXnet/IP 协议栈应用程序层对基本的 KNXnet/IP 路由及隧道功能提供支持; EIB 协议栈实现设备与 EIB 系统的交互; TP-Uart Driver 与 Ethernet Driver 分别提供与 TP-Uart 芯片及以太网控制器的驱动。

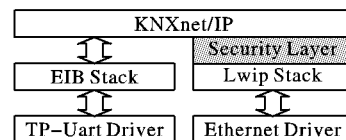


图7 协议实现软件模型

实验显示, 整个软件模块需要的 Flash 存储空间为 146 KB, RAM 执行空间为 58 KB, 因此现有硬件资源可以满足改进协议需求。时间方面, 在设备认证及密钥集分发阶段使用 ECC 算法, 这包括数字签名的生成、识别以及数据的加密、解密, 处理数据长度约为 140 B, 经实验测得的耗时数据为: 签名生成时间 136 ms, 签名识别时间 243 ms, 数据加密时间 384 ms, 数据解密时间 137 ms。因为设备认证及密钥集分发

只在安全协议的初始阶段进行,设备获得密钥集后不再需要使用 ECC 算法,因此测试的结果表明 ECC 算法可以满足安全协议在时间实时性上的需求。EIB 标准数据帧的长度最小为 9 B,最大为 23 B,扩展数据帧的最大长度为 263 B,因此安全协议中数据帧的加密部分最大长度为 296 B。EIB 总线的传输速率因使用物理介质的不同而异,其中使用最广泛的是 TP1 双绞线,EIB 标准规定的传输速度为 9 600 bps,传输一个长度为 263 B 的扩展数据帧需要约 219 ms,而在加密通信阶段使用对称加密算法,经实验测得加密速度可达 204.96 kbps,解密速度可达 174.15 kbps,完全满足安全协议应用需求。

设备正常工作时所处的网络环境模型如图 8 所示,网络中包含数个接入 IP 骨干网络的小型 EIB 网络,三个原型设备作为 KNXnet/IP 服务器,每个服务器连接一个或多个 KNX 子网,一台运行 KNXnet/IP 客户端程序的 PC 作为客户端,另外一台工作与混杂模式的 PC 可以监听网络上的所有数据包。在非安全模式下,KNXnet/IP 的数据帧可以很容易被截获,因为其通信内容全部为明文传输,因此很容易分析出报文内容,经修改后发送给目标设备进行攻击,而使用改进的安全协议后,攻击者由于没有 CA 颁发的证书,因此无法完成密钥集分发过程获得密钥集,即使截获设备间的通信数据也无法解析出数据内容,KNXnet/IP 设备就能确保安全性。

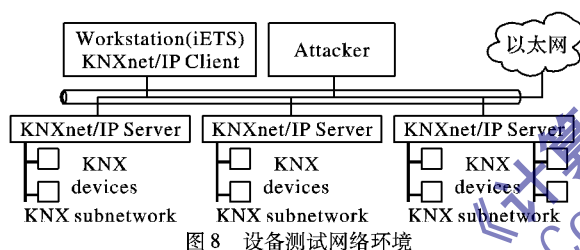


图 8 设备测试网络环境

4 结语

改进的安全协议是在综合分析当前 IP 网络安全机制的基础之上提出的,使用了设备数字签名、密钥集管理等方法,其中自定义的密钥集交换协议既满足安全性需求又能使安全协议符合嵌入式设备资源有限的特性。分析表明安全协议能够保证通信数据的完整性、新鲜性、保密性,设备原型的实现

进一步证明安全协议可以在嵌入式设备上实施,能够满足空间和时间的需求。改进的安全协议弥补了 KNXnet/IP 协议安全性不足的缺点,使得将 KNX 系统可以应用在对安全性要求较高的领域。

参考文献:

- [1] SEIP G. The future of the EIB system[J]. EIB Proceedings, 2000, 35(3): 9-13.
- [2] TREYTL A, SAUTER T, SCHWAIGER C. Security measures for industrial fieldbus systems-state of the art and solutions for IP-based approaches[C]// Proceedings of the 5th IEEE International Workshop on Factory Communication Systems. Piscataway: IEEE, 2004: 201-209.
- [3] SALVATORE C, GIOVANNI C. Implementing encryption and authentication in KNX using Diffie-Hellman and AES algorithms[C]// Proceedings of the 35th IEEE Annual Conference on Industrial Electronics. New York: IEEE, 2009: 2459-2464.
- [4] KNX Association. The overview over the KNXnet/IP specifications[S], 2009.
- [5] GRANZER W, LECHNER D, PRAUS F, et al. Securing IP backbones in building automation networks[C]// Proceedings of the 7th IEEE International Conference on Industrial Informatics. New York: IEEE, 2009: 410-415.
- [6] GRANZER W, REINISCH C, KASTNER W. Key set management in networked building automation systems using multiple key servers[C]// Proceedings of the 7th IEEE International Workshop on Factory Communication Systems. New York: IEEE, 2008: 205-214.
- [7] KENT S, SEO K. RFC 4301, Security Architecture for the Internet Protocol[S], 2005.
- [8] HARKINS D, CARREL D. RFC 2409, The Internet Key Exchange (IKE)[S], 1998.
- [9] DIERKS T, RESCORLA E. RFC 5246, The Transport Layer Security (TLS) protocol version 1.2[S], 2008.
- [10] HANKERSON D, VANSTONE S, MENEZES A. Guide to elliptic curve cryptography[M]. Berlin: Springer, 2004.
- [11] CILARDO A, COPPOLINO L, MAZZOCCA N, ROMANO L. Elliptic curve cryptography engineering[J]. Proceedings of the IEEE, 2006, 94(2): 395-406.
- [12] SIEMENS. Technical Data EIB-TP-UART-IC[R], 2001.

(上接第 1911 页)

道,配合动态化的密码流分组算法,扰乱了混沌系统原有特性,也使针对密码流分组特征的攻击更加艰难。改进后的算法在巩固提高明文敏感性措施的可靠性上达到了预期效果,并很好地解决了在加密解密者之间共享信息的问题。

参考文献:

- [1] YANG TAO, YANG LINBAO, YANG CHUNMEI. Breaking chaotic switching using generalized synchronization: examples[J]. IEEE Transactions on Circuits Systems, 1998, 45(10): 1062-1067.
- [2] 肖迪,赵秋乐.一种基于 Logistic 混沌序列的图像置乱算法的安全分析[J].计算机应用,2010,30(7):1815-1817.
- [3] 刘婷,闵乐泉.对一种混沌图像密码的选择明文攻击[J].武汉大学学报:信息科学版,2010,35(5):546-549.
- [4] 张涛.一个混沌分组密码算法的分析[J].计算机应用研究,2010,27(6):2294-2296.
- [5] 汪海明,李明,金晨辉.对 XW 混沌密码算法的分割攻击[J].计

算机应用研究,2010,27(7):2625-2628.

- [6] 陈艳丰,李义方.交替分段相互置乱的双混沌序列图像加密算法[J].华南理工大学学报:自然科学版,2010,38(5):27-33.
- [7] HENON M. A two dimensional mapping with a strange attractor[J]. Communications in Mathematical Physics, 1976, 50(1): 69-77.
- [8] 袁宁,宣蕾.超混沌序列密码受参数变化影响的实验研究[J].计算机研究与发展,2008,45(s1):351-356.
- [9] YONG R, ANOOP G, ALEX A. Automatically extracting highlights for TV-baseball programs[C]// Proceedings of ACM Multimedia. New York: ACM, 2000: 105-115.
- [10] 陈关荣,汪小帆.动力系统的混沌化——理论、方法与应用[M].上海:上海交通大学出版社,2006.
- [11] WANG XIAOYUN, YU HONGB. How to break MD5 and other Hash functions[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 3494. Berlin: Springer-Verlag, 2005: 19-35.