文章编号：2096-1618(2023)04-0429-07

一种适用于无线传感器网络的密钥管理策略

华 春，廖小平，侯 翔
(四川文理学院智能制造学院/政务数据安全达州市重点实验室，四川 达州 635000)

摘要：随着信息技术的快速发展，数据安全的重要性愈发凸显，作为数据保护的有效手段，现代数据加密技术在计算机网络中得到了广泛应用，其中密钥分发对密钥保护体系有着举足轻重的作用。在无线传感器网络中，由于节点能量有限，计算能力偏低等诸多限制条件，导致传统的基于非对称密钥的密钥分发策略难以直接应用。设计了一种适用于无线传感器网络的密钥管理策略，借鉴零信任网络思想，采用对称加密技术进行密钥分发，能够减少运算复杂性，降低传感器节点的能量消耗，同时引用了信任系数动态调整机制，可以根据无线传感器网络状况动态调整密钥更新周期，进一步降低能耗，具有一定的应用价值。

关 键 词：无线传感器网络；零信任网络；密钥分发；密钥更新；动态调整
中图分类号：TN918.91 **文献标志码**：A
doi：10.16836/j.cnki.jcuit.2023.04.009

0 引言

无线传感器网络(wireless sensor networks，WSN)是由无线传感器节点组成的分布式传感网络，具有自组织性强、组网方式灵活等特点，应用场景十分丰富。无线传感器网络是一种无基础设施的无线网络，网络节点间以自组织的方式构成网络，以多跳路由方式进行通信，健壮性比较好。无线传感器网络的应用非常广泛，近年随着物联网技术的推广与应用，无线传感器网络作为物联网的一项关键技术受到了广泛的关注与研究[1]。

随着应用的逐渐增多，数据的重要性日渐凸显，无线传感器网络也暴露出一些缺点，如传统的无线传感器网络，由于无线模块能量受限以及计算处理能力偏低等因素，在进行传感数据的采集、传递过程中，对数据的安全保护相对偏弱，很多情况下没有数据安全保护措施(如只有网络接入认证)或者仅使用默认密钥进行简单的数据加密。随着科技的发展和社会的进步，对网络数据安全的需求进一步增强，传统无线传感器网络数据安全需求迫在眉睫。

目前，在传统的计算机网络中，数据安全研究已比较成熟，借助 CA 认证、SSL 证书、RSA/SM2 以及 AES/3DES/SM4 等加密技术，可以对敏感数据进行有效保护。对于无线传感器网络，由于无线传感器节点存在计算能力弱等限制条件，无法直接使用传统计算机网络中的数据安全技术，需要进行相应的修改优化。

针对无线传感器网络节点计算能力弱、电池能量有限等特点，设计了一种适用于无线传感器网络的密钥管理策略，可以为无线传感器网络节点提供密钥产生、分配、更新、数据加密等全方位的安全服务。

1 预备知识

1.1 无线传感器网络

无线传感器网络主要由传感器节点、汇聚节点和管理节点组成。传感器节点是无线传感器网络的主要组成部分，负责传感数据的采集、AD 转换等工作，传感器节点之间可以通过自组织方式构成一张内部通信网络，通过多跳路由方式进行通信，支持平面路由和层次路由两种组织方式。汇聚节点的主要作用：一方面收集传感器节点的采集数据，进行融合汇总后通过外部网络上报到管理节点；另一方面通过外部网络接收管理节点的配置命令，并将配置命令(如传感器节点的上报周期、监测数据的阈值等)下发到传感器节点。管理节点通常处于远端外部网络中，用户可以通过管理节点对传感器节点的采集参数进行设置，还可以接收传感器节点的采集数据并写入后台数据库。无线传感器网络系统模型见图 1。

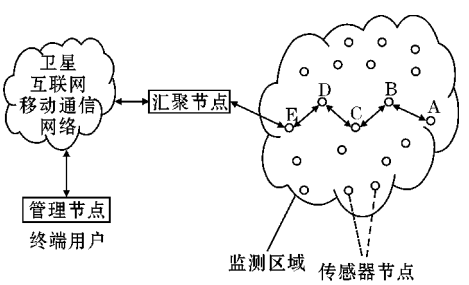

图 1 无线传感器网络系统模型

收稿日期：2022-09-07

无线传感器网络的应用十分广泛,如智能家居、智能电表、智慧农业等。以智能电表为例,电力公司管理人员在远端通过外部网络向智能电表终端配置相应的参数(如电表数据的上报周期、告警阈值等),智能电表终端周期性地采集电表数据(如本月用电度数、计价单位、采集时刻、剩余金额等)并上报电力公司后台数据库。普通用户在手机上安装电力公司 App 并绑定户号,就可以访问电力公司后台数据库获得电表的用电数据信息;同时,普通用户可以通过微信、支付宝、银行转账等方式向电力公司充值,并将充值信息(充值金额、时间等)写入到电力公司后台数据库,电力公司管理节点再将后台数据库最新的充值金额下发到智能电表终端。

1.2 密钥管理

密钥管理涉及密钥的产生、分发、更新等多个环节,通过密钥管理服务(key management service, KMS)[2],用户可以创建和管理密钥[3-5]。密钥管理服务在保护密钥的机密性、完整性和可用性上作用显著[6],是现代信息安全系统中重要一环。

在密钥管理服务中,密钥的分发处于核心位置。密钥分发主要有两种方式。

(1)预置密钥。预置密钥是一种早期的密钥管理方案,具有实现简单的特点。收发双方事先约定加密密钥,在数据通信过程中,发送端使用预置的密钥进行数据加密保护,接收端使用预置的密钥进行数据解密。

(2)密钥交换协议。主要思路是先利用密钥交换协议将收发双方的密钥进行交换,协商好密钥后再利用该密钥保护数据进行消息交互。1976 年,Diffie[7]提出了最早的 Diffie-Hellman 密钥交换算法,后来不同学者提出改进方案,密钥交换算法得到不断发展。Peikert[8]提出一种错误消除算法;Bos 等[9]实现了一种适用于 TLS 协议的密钥交换协议 BCNS15;Alkim 等[10]提出基于 RLWE 的密钥交换协议 NewHope。密钥交换协议具有强大的生命力,绵延不绝。

令人遗憾的是,上述两种方法目前都不能直接适用于传统的无线传感器网络。预置密钥方式的密钥管理,一般采用对称加密技术,优点是保证了运算速度,但最大的问题是不支持密钥自动更新。如果预先设置的密钥在使用过程中长时间不更新,容易被他人暴力破解或者恶意攻击,造成安全性问题;如果采用人工方式对密钥进行手动更新,效率低,并且容易出错,对于较大规模的网络节点来说,费时耗力,难以普及。传统的密钥交换协议,虽然具有一套成熟的密钥交换标准,可以实现密钥自动更新,但密钥交换时需要使用非对称加密手段,实现过程比较复杂,加解密速度慢,对 CPU 计算能力要求高,功耗较大,而无线传感器网络中,传感器节点往往都是采用电池供电,能量受限,CPU 性能较低。

综上所述,在无线传感器网络中,需要对原有的密钥管理方案进行改进。

2 密钥管理策略

2.1 主要思路

设计的适用于无线传感器网络的密钥管理策略结合了零信任网络的思想。零信任的概念在 2010 年由 Forrester 分析师 Kindervag[11]提出,主要思想是认为主机无论处于网络什么位置,都应被视为互联网主机,它们所在的网络,无论是互联网还是内部网络,都必须被视为危险网络[12]。零信任模型提供了用户以任何方式访问任何地方的任何数据的一致性安全策略[13-15],在访问服务和数据时,采取“从不信任并始终验证”原则[16]。

设计的密钥管理策略主要处理思路为:基于零信任网络特点,假设网络是不安全的,无线传感器节点的数据默认都是加密的,在处理转发前,预先配置少量白名单,将加密密钥添加到白名单中,只允许白名单中的密钥对数据进行加解密并转发,同时传感器节点需要定期更新白名单中的密钥,保证高安全性。

具体实现可以分为初始化、密钥分发、密钥更新 3 个阶段,见图 2。

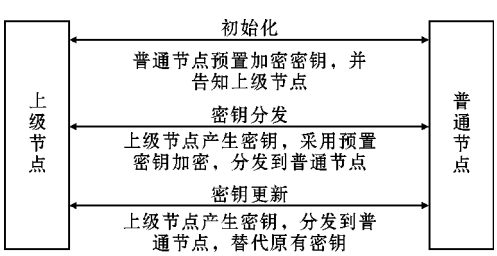

图 2 密钥管理策略 3 个阶段

初始化阶段。无线传感器网络部署完毕后,为无线传感器节点预置密钥,作为上级节点与普通节点之间密钥分发的保护密钥。

密钥分发阶段。普通节点向上级节点申请数据保护密钥,上级节点产生密钥并向普通节点同步数据保护密钥。

密钥更新阶段。为提高安全性,普通节点从上级节点申请的密钥具有一定的时效性,密钥使用一段时间后,普通节点需要重新申请数据保护密钥。

另外,为便于表述,引入两个关键名词:上级节点和普通节点。

上级节点有两种含义:对于平面路由结构的无线传感器网络,上级节点对应汇聚节点;对于分层路由结构的无线传感器网络,上级节点一般表示簇头节点。

普通节点指的是一般的无线传感器节点,主要从事传感数据采集工作。

2.2　初始化阶段

在无线传感器节点部署完毕后,进入到初始化阶段。初始化阶段的主要工作是为每个无线传感器普通节点分配预置密钥,并将密钥同步到上级节点。初始化阶段遵循以下 3 个原则:

(1)每个无线传感器普通节点的预置密钥是不同的,可以将每个无线传感器普通节点 ID 作为预置密钥,也可以产生一段随机数作为预置密钥。

(2)为增加安全性,应同时计算预置密钥对应的数字摘要,使用 SM3 杂凑算法计算无线传感器普通节点 ID 的数字摘要。

(3)保证每个无线传感器普通节点的预置密钥及数字摘要都能同步到上级节点。

说明:此时预置密钥的角色是 KEK(key encryption key),作为密钥分发的保护密钥,不能对采集的数据直接进行加密。

2.3　密钥分发阶段

密钥分发阶段由普通节点发起,主要是将上级节点的数据加密密钥同步到普通节点中,可以细分为 5 个步骤。

步骤 1　无线传感器普通节点向上级节点发出激活消息,激活消息中应携带无线传感器普通节点 ID 对应的摘要信息。

步骤 2　上级节点收到激活消息后,首先判断摘要信息是否匹配。如果不匹配,发送一个拒绝消息或者不应答;如果匹配,进一步判断是否已生成数据加密密钥 Key。如尚未产生加密密钥 Key,则产生一段随机数作为密钥 Key,接下来先计算 Key 的数字摘要 Hash1,再使用预置密钥将密钥 Key 加密,最后将 Key 密文连同数字摘要 Hash1 发送到无线传感器节点。

说明:上级节点的密钥生成有多种方式,除了采用上述方式,还可以采用密钥池的方式,预先生成多个密钥 Key1 ~ Key$n$,生成密钥后,应将密钥、数字摘要、时间戳等信息保存。

步骤 3　无线传感器普通节点收到消息后,先将 Key 密文解密,得到数据加密密钥 Key,再计算 Key 的数字摘要 Hash2,最后比较 Hash1 和 Hash2 是否相同。如果相同,存储 Key 明文及摘要 Hash2;如果不同,跳转到步骤 1 重新请求密钥。

步骤 4　无线传感器普通节点采集到数据 Data 后,使用数据加密密钥 Key 加密 Data,得到 Data 密文,最后将 Data 密文及摘要 Hash2 发送到上级节点。

步骤 5　上级节点收到数据密文后,解密密文,此时已经完成无线传感器普通节点与上级节点之间的安全通信。最后,上级节点使用类似的方法与其他无线传感器普通节点建立安全通道并转发数据。

2.4　密钥更新阶段

上级节点周期性检查密钥时间戳,一旦发现密钥使用时长超过了更新阈值,会启动密钥更新,密钥更新分为 4 个步骤:

步骤 1　上级节点产生新的密钥 KeyNew,重新计算摘要 Hash1New,并获取新的时间戳。

步骤 2　上级节点使用之前的数据加密密钥 Key 作为 KEK,加密新密钥 KeyNew,并将 KeyNew 密文连带摘要 Hash1New 发送到无线传感器普通节点。

步骤 3　无线传感器普通节点使用之前的数据加密密钥 Key 作为 KEK,解密 KeyNew 密文,得到 KeyNew 明文,计算摘要 Hash2New,并将其与 Hash1New 比较。如果相同,分别用 KeyNew 明文和数字摘要 Hash2New 替代 Key 及数字摘要 Hash2,然后向上级节点发送更新成功报文;如果不同,向上级节点发送更新失败报文。

步骤 4　上级节点收到应答消息后,判断消息类型。如果为更新成功报文,存储 KeyNew、Hash1New 及时间戳;如果为更新失败报文,转入步骤 1 进行密钥更新。

2.5　密钥更新周期设定

密钥更新周期的设定是密钥管理系统中一项重要的工作内容,更新周期的长短对系统会产生直接影响。密钥更新周期值太短,会造成消息交互频繁,浪费传感器节点宝贵的能量;密钥更新周期值太长,会降低无线传感器节点间数据通信的安全性。因此,密钥更新周期的设定需要合理评估,最好能够根据实际情况自适应动态调整。

在固定的密钥更新周期值 P_{def} 之外,引入了一个信任系数 θ,密钥更新周期 P_{new} 为

$$P_{\text{new}} = \theta \times P_{\text{def}}$$

信任系数 θ 的值默认为 1,可以根据无线传感器网络节点实际情况动态调整。

信任系数 θ 增大主要包括 3 个因素:一定时间范围内,无线传感器普通节点与上级节点间交互的消息数量较低,低于设定的阈值,说明数据交互量比较低;一定时间范围内,无线传感器普通节点与上级节点剩余电池能量较低,低于设定的阈值,说明传感器节点的能量充足;一定时间范围内,无线传感器普通节点与上级节点间交互的消息时,错误消息的数量较低,低于设定的阈值,说明网络环境良好,无线信号强度高或者网络未受到干扰。

信任系数 θ 减小主要包括 2 个因素:一定时间范围内,无线传感器普通节点与上级节点间交互的消息数量高于设定阈值,并且剩余电池能量高于阈值;一定时间范围内,无线传感器普通节点与上级节点间交互的消息时,网络环境较差,错误消息的数量高于阈值。如无线传感器普通节点向上级节点发送传感数据,上级节点解密,在进行数字摘要值比较时出错,上级节点认为是一个错误消息,在某个时间段内频繁出现错误消息,表明网络环境差、或者受到恶意攻击干扰,需要缩小密钥更新周期来保证安全性。

3 密钥管理策略举例

3.1 拓扑配置

以 Zigbee 无线传感器网络为例进行说明,采用星型拓扑结构(图 3)。其中上级节点 C 为核心节点,普通节点有 4 个,分别为 E1、E2、E3、E4,密钥管理方案内容主要以上级节点 C 和普通节点 E1 为例进行说明。

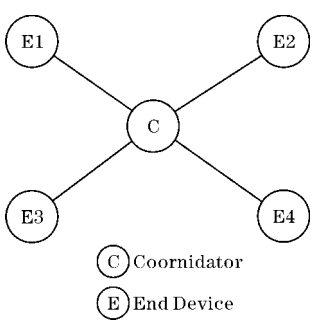

图 3 Zigbee 星型拓扑

3.2 密钥分发

每个 Zigbee 节点都有一个 64 位的全球唯一地址,在初始化阶段,可以将此地址作为预置密钥,并计算其摘要信息 Hash,然后将预置密钥及摘要信息 Hash 添加到上级节点 C 的白名单中,同时记录时间戳 T。

上级节点 C 的处理过程:先把普通节点 E1 的 64 位地址作为预置密钥 Key1,再对 Key1 进行数字摘要计算,得到摘要 Hash1,接着记录当前的时间戳 T1 和密钥 Key1 生命周期 P1,最后将{Key1,Hash1,T1,P1}添加到上级节点 C 的存储区中。

普通节点 E1 的密钥分发包括 6 个步骤。

步骤 1 普通节点 E1 与上级节点 C 关联成功后,以自身的节点 ID(对应于上级节点的 Key1)作为 Key1′,并计算摘要 Hash1′。

步骤 2 普通节点 E1 向上级节点 C 发起消息 Req1,请求获取普通节点 E1 与 C 节点之间通信的加密密钥 Kenc1。

步骤 3 上级节点 C 收到 Req1 之后,产生一个随机密钥 Kenc1 并记录时间戳 Tenc1 及生命周期 Penc1,连同 Key1 的摘要 Hash1 组合成一串数据 Data,然后用 Key1 对数据 Data 进行对称加密,得到 Data 的密文并将其放入应答消息 Rsp1,最后将 Rsp1 发送到普通节点 E1。

步骤 4 普通节点 E1 收到上级节点 C 的应答消息 Rsp1 后,以 Key1′作为解密密钥,对 Data 的密文进行解密,得到 Data 明文。然后提取{Kenc1,Hash1,Tenc1,Penc1}信息,并将 Hash1 与节点自身的 Hash1′做比较,如果相同,表明解密成功,将{ Kenc1,Henc1,Tenc1,Penc1}保存到普通节点 E1,然后转入步骤 5;如果不同,转入步骤 2。

步骤 5 普通节点 E1 向上级节点 C 发送应答消息 Rsp2,表明密钥获取成功。

步骤 6 上级节点 C 收到 Rsp2 后,计算 Kenc1 的摘要 Henc1,保存{Kenc1,Henc1,Tenc1,Penc1}信息。

说明:在初始阶段,使用普通节点 ID 作为 KEK,后续密钥更新时直接采用上一次的密钥 Key 作为 KEK 即可。

3.3 数据交互

密钥分发完毕后,可以进行数据交互,普通节点 E1 的数据交互分为 5 个步骤。

步骤 1 普通节点 E1 采集了一定数据 Data,达到了上报条件,计算 Data 的摘要 Hdata′。

步骤 2 普通节点 E1 将上报数据 Data、摘要 Hdata′等信息进行组合,得到 Data′。将通过密钥分发获得的 Kenc1 作为加密密钥,对 Data′进行加密,得到 Data′密文。

步骤 3 普通节点 E1 将 Data′密文封装到消息 M1 中,并发送到上级节点 C。

步骤 4 上级节点 C 收到 M1 后,使用 Kenc1 解密 Data′密文,得到 Data′,并从中提取 Data,解析获得 Hdata′。

步骤 5 上级节点对提取到的 Data 进行摘要运

算,得到 Hdata,将 Hdata 与 Hdata′进行比对。如果相同,表明解密成功。

3.4　密钥更新

密钥更新分为被动触发和主动触发两种方式。被动触发,上级节点 C 作为触发节点,如果普通节点 E1 的密钥需要更新,由上级节点 C 负责通知普通节点 E1 进行密钥更新。主动触发,普通节点直接作为触发节点,如果普通节点 E1 的密钥需要更新,由普通节点 E1 负责触发密钥更新。需要注意的是,对于主动触发方式,需要在普通节点与上级节点 C 之间事先启用时间同步功能。

3.4.1　被动触发

被动触发密钥更新分为 6 个步骤。

步骤 1　上级节点 C 发现普通节点 E1 的加密密钥 Kenc1 满足触发条件。Kenc1 从产生至今,生命周期完成已超出设定阈值(比如 90%),达到密钥更新条件,触发密钥更新。

步骤 2　上级节点 C 产生新的加密密钥 Kenc1New,计算其数字摘要 Henc1New,记录其时间戳 Tenc1New 和生命周期 Penc1New,并将{Kenc1New, Henc1New, Tenc1New,Penc1New}组成数据串 DataNew。

步骤 3　上级节点 C 使用之前的加密密钥 Kenc1 对 DataNew 加密,得到 DataNew 密文,将其组合成一条密钥更新消息 M1,然后发送到普通节点 E1。

步骤 4　普通节点 E1 收到消息后,提取 DataNew 密文并用 Kenc1 解密,得到 DataNew。

步骤 5　普通节点 E1 解析 DataNew,提取{Kenc1New, Henc1New,Tenc1New, Penc1New},对 Kenc1new 做摘要,先得到 Henc1new′,接着再将 Henc1new′与 Henc1new 进行比较。如果相同,用{Kenc1New, Henc1New, Tenc1New, Penc1New}替换{ Kenc1, Henc1,Tenc1,Penc1}并保存,最后向上级节点 C 发送密钥更新成功消息;如果不同,直接向上级节点 C 发送密钥更新失败消息。

步骤 6　上级节点 C 收到普通节点 E1 的消息后,进行判断。如果密钥更新成功,用{Kenc1New,Henc1New,Tenc1New,Penc1New}替换{ Kenc1,Henc1,Tenc1,Penc1}并保存;如果密钥更新失败,随机延时一段时间后,重新启动密钥更新流程。

3.4.2　主动触发

主动触发分为 7 个步骤。

步骤 1　普通节点 E1 发现其加密密钥 Kenc1,从生成至今,生命周期完成超出预设阈值(比如 90%),满足密钥更新条件。

步骤 2　普通节点 E1 构建一条密钥更新请求消息 Req,发送到上级节点 C。

步骤 3　上级节点 C 产生新的加密密钥 Kenc1New,计算其数字摘要 Henc1New,记录其时间戳 Tenc1New 和生命周期 Penc1New,并将{Kenc1New, Henc1New, Tenc1New,Penc1New}组成数据串 DataNew。

步骤 4　上级节点 C 使用之前的加密密钥 Kenc1 对 DataNew 加密,得到 DataNew 密文,将其组合成一条密钥更新消息 M1,然后发送到普通节点 E1。

步骤 5　普通节点 E1 收到消息后,提取 DataNew 密文并用 Kenc1 解密,得到 DataNew。

步骤 6　普通节点 E1 解析 DataNew,提取{Kenc1New, Henc1New,Tenc1New, Penc1New},对 Kenc1new 做摘要,先得到 Henc1new′,接着再将 Henc1new′与 Henc1new 进行比较。如果相同,用{Kenc1New, Henc1New, Tenc1New, Penc1New}替换{ Kenc1, Henc1,Tenc1,Penc1}并保存,最后向上级节点 C 发送密钥更新成功消息;如果不同,直接向上级节点 C 发送密钥更新失败消息。

步骤 7　上级节点 C 收到普通节点 E1 的消息后,进行判断。如果密钥更新成功,用{Kenc1New, Henc1New,Tenc1New,Penc1New}替换{ Kenc1,Henc1,Tenc1,Penc1}并保存;如果密钥更新失败,随机延时一段时间后,重新启动密钥更新流程。

3.5　密钥管理策略

无线传感器网络密钥管理策略,具有以下 3 个优点。

(1)适应能力强。密钥管理策略可以应用于小型的平面路由无线传感器网络,也可以适用于大型的层次路由无线传感器网络。平面路由结构可以直接使用密钥管理策略,见图 4。层次路由结构,簇头节点有两种身份。在一个簇内部,簇头节点以上级节点身份与成员节点(普通节点)进行交互;在一个簇外部,簇头节点以普通节点身份与汇聚节点(上级节点)进行交互,见图 5。

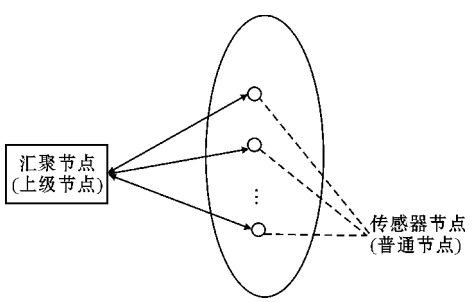

图 4　平面路由结构

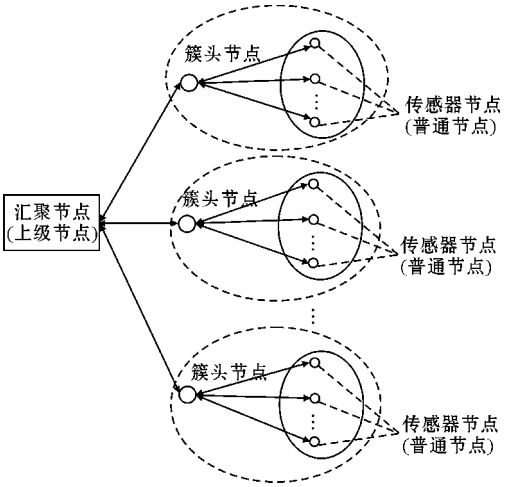

图 5 层次路由结构

(2)安全性强。基于零信任网络策略,无线传感器节点采集数据在传递前先进行对称加密以及加密密钥定期更新等措施,提高了安全性。

(3)处理速度快、节能。密钥交换采用对称密钥,加解密速度快,对 CPU 的要求低,节约能量;同时,密钥更新时引入信任系数 可以动态调整更新周期,尽可能降低消息交互频率,进一步降低节点能量消耗。以 TI 公司 CC2530 芯片为例,CC2530 芯片已硬件支持 128bit 的 AES 加密算法,Z-stack 协议栈也封装了 AES 加密接口。使用 3 个 CC2530 网络节点搭建一个实验网,采用以 AES-128 为基准的密钥管理策略后,节点的运算速度没有受到明显影响,收发时延基本稳定在 15 ~ 30 ms。

4 结束语

随着无线传感器网络节点数量的增多和数据量的增大,信息安全的重要性愈发凸显,迫切需要一种数据安全保护方案。设计的无线传感器网络密钥管理策略,在基于零信任网络的白名单机制基础上,使用对称加密技术保护密钥及数据。另外,引入了信任系数动态调整机制,能够根据无线传感器网络特点优化密钥更新周期,在保证密钥分发及数据传输的安全性的同时,兼顾无线传感器节点数据处理及节能的要求。该策略应用场景比较广泛,如智能电表系统、智能交通系统、智能家居系统等,具有良好的推广价值。

致谢:感谢政务数据安全达州市重点实验室 2022 年度开发基金项目(ZSAQ202212、ZSAQ202203)对本文的资助

参考文献:

[1] Wu Dapeng, Liu Zhenli, Yang Zhigang, et al. Survivability-Enhanced Virtual Network Embedding Strategy in Virtualized Wireless Sensor Networks [J]. Sensors, 2020, 21(1): 218-237.

[2] Reiter M K, Franklin M K, Lacy J B, et al. The Omega Key Management Service [J]. Journal of Computer Security, 1996, 4(4): 267-287.

[3] Challaly, Seba H. Group Key Management Protocols: A Novel Taxonomy [J]. International Journal of Information Technology, 2005, 2(1): 105-118.

[4] Ready L B, Oden R, Chadwick H S, et al. Development of An Anesthesiology-based Postoperative Pain Management Service [J]. The Journal of the American Society of Anesthesiologists, 1988, 68(1): 100-106.

[5] Tian Biming, Han Song, Liu Liu, et al. Towards Enhanced Key Management in Multi-phase ZigBee Network Architecture [J]. Computer Communications, 2012, 35(5): 579-588.

[6] Chandramouli R, Iorga M, Chokhani S. Cryptographic Key Management Issues and Challenges in Cloud Services [J]. Secure Cloud Computing, 2014: 1-30.

[7] Diffie W. New Direction in Cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[8] Peikert C. Lattice Cryptography for the Internet [C]. Springer. International Workshop on Post-Quantum Cryptography. October 1-3, 2014. Waterloo, ON, Canada. Berlin: Springer, 2014: 197-219.

[9] Bos J W, Costello C, Naehrig M, et al. Post-quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem [C]. IEEE. 2015 IEEE Symposium on Security and Privacy. May 21, 2015, San Jose, California. New Jersey: IEEE, 2015: 553-570.

[10] Alkim E, Ducas L, Poppelmann T, et al. Post-quantum Key Exchange-A New Hope [C]. USENIX. USENIX Security Symposium, August 10-12, 2016, Austin, TX, Berkeley: USENIX, 2016: 327-343.

[11] Kindervag John. Forrester Build Security into Your Network's DNA: The Zero Trust Network Architecture [EB/OL]. https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA., 2010-11-10.

[12] Nist. Zero Trust Architecture[EB/OL]. https://csrc. nist. gov/publications/detail/sp/800-207/archive,2019-9-23.

[13] Rizvi S,Ryoo J,Liu Y,et al. A Centralized Trust Model Approach for Cloud Computing[C]. IEEE. 23rd IEEE Wireless and Optical Communication Conference,May 9-10,2014,Newark,New Jersey,USA. NJ:IEEE,2014:1-6.

[14] Decusatis C,Liengtiraphan P,Sager A,et al. Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication[C]. IEEE. 2016 IEEE International Conference on Smart Cloud, November 18-20, 2016,New York,USA. NJ:IEEE,2016:5-10.

[15] Eidle D,Ni S,Decusatis C,et al. Autonomic Security for Zero Trust Networks[C]. IEEE. 8rd IEEE Annual Ubiquitous Computing,Electronics and Mobile Communication Conference, October 19-21,2017,New York,USA. NJ:IEEE,2017:288-293.

[16] Samaniego M,Deters R. Zero-Trust Hierarchical Management in IoT[C]. IEEE. 2018 IEEE International Congress on Internet of Things,July 2-7,2018, San Francisco, CA, USA. NJ: IEEE, 2018:88-95.

A Key Management Strategy for Wireless Sensor Networks

HUA Chun, LIAO Xiaoping, HOU Xiang

(College of Intelligent Manufacturing,Dazhou Key Laboratory of government data security,Sichuan Institute of Arts and Science,Dazhou 635000,China)

Abstract:With the rapid development of information technology, the importance of data security is becoming more and more prominent. As an effective means of data protection, modern data encryption technology has been widely used in computer networks, among which key distribution plays an important role in key protection system. In wireless sensor networks, the traditional key distribution strategy based on asymmetric key is difficult to be applied directly due to many restrictions, such as limited node energy and low computing ability. This paper proposes a key management strategy suitable for wireless sensor networks. Learning from the idea of zero trust network and using symmetric encryption technology for key distribution, it can reduce the computational complexity and reduce the energy consumption of sensor nodes. At the same time, a dynamic adjustment mechanism of trust coefficient is proposed in this paper, which can dynamically adjust the key update cycle according to the status of wireless sensor networks and further reduce the energy consumption, it is of certain application value to data security.

Keywords:WSN;zero trust network;key distribution;key update;dynamic adjustment