# 远程抄表系统组网协议

# 远程抄表系统安全协议

正如前文所描述的，远程抄表子节点模块在主节点的宏观调度下，各自形成一条路径存储在主节点和子节点内存之中。在可用性上已经到达了电网相关标准的要求。但是随着远程抄表相关技术的更新换代，用户的大规模普及，用户用电信息安全的保障是一个重要的话题。本章主要内容则是围绕着本远程抄表系统中可能出现的安全隐患，提出一个切实可行的方案来提升整个系统的安全性能。

## 现有安全措施

进入市场初期的产品在产品功能性上做出了极大的努力，在安全性能上的关注相对而言会被放低。同样的目前现场运行的远程抄表协议中安全方面使用的技术非常少。总结来说目前使用的安全保护技术主要包含如下几点：

1. 帧的完整性：

mac层结尾使用了CRC校验和的方式来保证网络帧内容的完整性。应用层中按照国家电网相关标准要求【】，使用了位叠加的校验方式。

1. 重要数据的机密性：

应用层中的数据是集中器端和电表内部通信的协议，其关键数据使用国家加密算法【】加密保证重要数据的机密性。

1. 防止重放攻击和洪范灾难：

在nwk层中引入AODVjr中的帧序列号机制【】防止帧被攻击者重放，即节点只处理更新的网络帧。mac层中类似的机制也存在，主要为了防止ack未收到情况下连续发包导致目标节点任务量过重。同时所有网络广播帧都拥有一个生命期概念的转发次数域，配合序列号可以起到防止洪范灾难的作用。

在如上三种机制的作用下，网络在现场运行情况基本稳定。但是，这些工作是远远不够的。在现场长时间的运行情况可以很明显的看出来，现有的安全保护措施对于网络安全性的保护还远远不够，更不用说保护的全面性。

## 网络安全隐患

分析上一节中所描述的远程抄表系统的安全防护措施，不难发现：所有的安全防护都是针对于组网完成之后的。根据系统安全性的木桶原理，如果组网阶段安全性很薄弱，那么整个系统的安全性的上限也就是组网阶段的安全性等级。于是对组网期间网络的安全性进行分析并做出相关设计，对于远程抄表系统安全方案设计来说是至关重要的。

假设组网阶段是绝对安全的情况，这样的安全防护也是不够的。很明显的一个方面就是机密性的保护仅仅停留在应用层相关重要数据中。而网络绝对不止有应用层具有重要信息，网络层关系到网络的形成和应用层数据传递的效率，同时还需要对网络进行维护调整以期网络的长时间稳定可靠。由此说明之前的简单设计并不能对网络层面的攻击做出行之有效的保护。

接下来，本节内容将会对组网阶段、正常工作阶段和网络结束阶段的网络安全性能进行分析和设计。

### 组网期间的安全隐患

组网是网络生命期的第一个阶段，这个阶段是不在网子节点，通过和在网节点交互，最终获得所归属网络信息的过程，期间会涉及到大量网络信息的传递。如果这一阶段没有对加入者的身份进行验证的话，会导致大量网络信息泄密，尤其是在网络控制信息被泄露的话，攻击者可以轻易对网络进行操作。另一方面，如果节点加入网络时没有对所加入的网络的主节点进行认证，那么子节点自身也无法确定是否处于安全的环境中。具体来说，存在以下安全隐患。

#### 对网络进行攻击造成混乱

远程抄表系统的网络组建过程中，子节点以长地址作为身份证明，加入到特定的主节点所组织的网络中去。主节点对子节点的过滤也仅仅是长地址匹配这么简单。而凡是具有相关标准知识的人会知道，子节点的长地址来自于子节点所插入的电表地址­【】。电表在表壳或者液晶显示屏中需要标明表号，也就是电表地址【】。这个时候问题出现了，攻击者只需要看到一个表上的表号，然后把自己伪装成这个电表就可以抢先在正常节点之前入网，并且造成网络的混乱。

#### 对位于节点之后的终端进行攻击

正如之前所说，组网过程中子节点是否加入网络完全由主节点决定。而子节点在远程抄表系统中的身份是一个传递者，子节点对仅仅依据主节点的长地址过滤网络包的做法是太过粗犷的。如果攻击者伪装成主节点，将未入网的子节点加入到自己的网络中，然后就可以对子节点之后的电表发起所有的命令。这样的情况对网络的威胁是非常巨大的。安全的网络如果无法传送的数据本身就是有问题的，那么这个系统的价值就没法得到体现。

基于以上两个方面的考虑，协议在组网阶段需要一个能够完成双向身份认证的一个过程，这个过程可以协助我们对恶意攻击者进行过滤。在尽可能大的程度上保护现场运行节点的安全。

### 正常工作期间的安全隐患

根据章节1.1 所述，正常工作阶段，在完整性和机密性上都有考虑。但是考虑是不全面的。首先完整性保护有两个方面的考虑，一个是信息传输过程中产生错误，一个是攻击者对信息的篡改。CRC校验和的方式仅仅在信息传输过程中的错误有很好的效果，但是对于防止恶意篡改信息这方面是不可靠的。然后是机密性的保护上，缺陷是非常明显的——仅仅在应用层以上数据进行数据机密性保护是远远不够的。网络层中包含有大量网络控制信息，因为网络的日常维护和调整是需要数据的支持的，比如说节点校时时候的时间，从子节点带回来的网络节点间相互之间的强度信息等。应用层机密性保护关系到的是集中器和电表之间的信息的机密，网络层机密性保护关系到的才是网络端的稳定和可用性。我们可以发现当前系统对如下几种攻击方式是存在漏洞的。

#### 篡改数据

现有系统中使用的CRC校验和方式对完整性进行保护，这种方式对于在mac层次上判断数据是否在传输过程中出现自然变异等情况可以比较快速有效的发觉。但是CRC算法无法在防止数据认为篡改这一个层面上进行有效的保护，这是因为CRC算法是公开的，任何人可以可轻松的实现一个相同的算法。恶意篡改数值的攻击者在篡改完信息之后只需要依样对相关数据报打包运算一遍CRC，然后附加在数据的尾部就可以实现对帧内容的改造。以期望达到攻击网络的目的。比如说，在以时间为度量的阶梯计费的电表中，电表自动计算电费，而计算的时钟是内置在电表内部的一个片上系统中。相关的在远程抄表系统中，主站后台为了精确控制各电表的时间，设计了一个校时命令。也就是说时间是可以远程修改的。如果攻击者获取到了相关信息，就可以很轻松的修改电表时间，以期望达到偷电的效果。

#### 网络控制

远程抄表协议的层次划分为四个：驱动层、mac层、网络层和应用层。其中应用层直接使用国家电网相关标准，内部含有加密处理。其他层次中目前没有使用加密或者认证的安全设置。但是实际情况中，远程抄表协议的层次分工指出，网络的管理维护等功能交由网络层实现。网络层实际上是整个网络的核心部分。帧格式中包含有大量的网络层控制命令。其中包括维护、诊断、校时、切换信道组等等。在现有的协议体系中，这些所有的命令是以明文的方式发送的，而且大部分都不需要应用层的协助控制。攻击者只需要获得相应的帧格式信息，按照格式要求填写命令，就可以向外发出网络控制命令。从而将网络纳入攻击者的管理监控域。

#### 操作智能电表

不仅仅是网络控制命令，作为网络层数据帧的应用层控制帧也可以成为攻击者伪造的对象。因为节点无法对网络帧的发起源进行有效的认证，攻击者可以构造一个操作电表的命令，作为网络层数据帧发送给节点。在应用层阶段，根据相关协议，电表无法知道具体的发起者是不是真正的集中器。部分没有使用应用层加密的命令就会直接被电表执行。加之现阶段电表程序难免存在或多或少的缺陷，这样的情况是具有风险的。

显然，在正常工作期间的安全性保护也是非常欠缺的。远程抄表系统需要更加全面的安全设计，至少需要将网络层纳入到安全管控的层面上来，同时需要加强对整个网络包完整性的判定，真正做到防篡改防伪造同时对特定数据进行保护才能够更好的保护远程抄表系统。

### 网络结束阶段的安全隐患

作为节点在网络的生命周期的最后一环，退出网络涉及到的安全隐患相对较少，但是如果不加以好好管理，安全问题同样也会使得整个网络处在一个极度危险的状态。因为节点在退出了网络之后，其节点内部所存储的信息有可能关系到网络的稳定。首先，网络密钥等安全辅助信息如果被攻击者获得，攻击者就能绕过安全验证而直接接入网络；其次，网络的层次和路径信息可以成为攻击者对网络进行破坏的一个重要线索；而且，如果网络信息的残留可能会对该节点加入其他网络产生一定的影响。简单总结也能发现如下两种方式的隐患。

#### 攻击者获取网络安全信息

节点离开了网络，但是没有将网络相关安全信息移除会导致网络被攻击者攻击。如果有攻击者获取到了节点内部存留的安全信息——比如网络密钥、加密算法——的时候，攻击者完全有能力将自身伪装成为网络中的一员与主节点或者和其他网络节点交互。退一步讲，攻击者至少也可以产生一个监控节点，对网络的动态进行数据监控和采集。在大量数据的前提下分析网络情况，制定相关策略来谋取私利。同时也会对其他智能电表用户的信息隐私性产生一定的威胁。结合存在安全信息的网络，如果网络信息是不存在更新机制的，那么这个信息的泄露也就意味着网络信息的完全暴露。

#### 信息残留导致网络混乱

节点退出网络的原因有很多，有节点或者终端故障，有可能是集中器档案错误，也有可能是网络管理的需求。这就意味着存在以下两个情况：

1. 退出网络的节点很有可能会很快被要求加入其他的甚至加入原来的那个网络。而节点地址分配的方式并不是由子节点本身长地址相关信息决定的。也许当节点从网络A移动到网络B时，节点信息需要有更新才能正常通信，原始的信息会增加节点对于新到来的网络帧的过滤。
2. 已经退出网络但是还没有加入新网络需求的节点如果在地理位置上仍然处于原网络的位置时，原有网络的相关帧依然可以被节点监听到。而同样的短地址也许已经被主节点分配给了一个新的节点。这样在网络中就会出现两个具有相同短地址，却有不同长地址的节点。主节点在发送数据的时候这两个节点之间可能会导致网络的混乱出错。

其中第二种情况的存在还不仅仅是当节点使用了相关安全设计之后才存在的。节点退出网络不完全这个问题本身对具有节点入网后分配地址性质的网络都是普遍存在的。对那些节点还需要缓存邻居信息的网络的干扰作用尤为明显。

## 网络安全需求

原有协议在安全层面的设计是远远不够的。对于攻击者而言，这样的网络无论在组网阶段，还是日常工作阶段，甚至是网络解散后阶段都存在很多种方式对网络进行攻击以谋取私利。

而对网络状况进行分析后，不难发现。安全协议应该至少能够满足如下几个方面的功能需求才可以保障基本的远程抄表系统的安全：

1. 在网络的组建阶段，主节点需要一个机制来判断子节点的身份，而不是简单的看返回的地址是否是存在于自身的地址库里；
2. 在网络的组建阶段，子节点也需要一个机制来识别主节点，不能轻易地加入到一个无法识别的网络中；
3. 在正常工作阶段，主节点与子节点之间需要一个机制来让双方来认证对方，以防止攻击者的伪装攻击对网络造成伤害，防止攻击者对网络数据包的篡改；
4. 在正常工作阶段，秘密性保护应该延伸到网络层这个层次，对相关的管理命令内容需要保护，不能再以完全明文而且不加验证就转发和操作的这个模式来工作了；
5. 在正常工作阶段，网络节点的安全信息是需要一个安全机制来更新的，不能是一成不变的；
6. 在网络退出阶段，节点相关信息需要一次完整的清除以保证安全信息的秘密性；
7. 在网络退出之后，需要一个机制来保证退出之后的节点内部信息在主节点和子节点之间是一致的。

## 远程抄表系统安全系统设计

在章节1.3 中，针对本远程抄表系统的安全方面提出的七项安全需求。以网络节点所处在的网络生命期为线索，我们大体可以将本远程抄表系统的安全方案划分为三大部分：双向身份认证以及密钥协商更新、工作阶段网络命令加密以及发起者认证、退网安全信息处理。本章节接下来会以此为线索对这三大部分进行描述。

### 工作阶段网络安全性保障

从网络的生命期来看，本章节应该放在第二阶段描述。但是网络系统安全设计的一个重要的原则是使网络在通常情况下能够更安全的运行。而组网阶段的双向身份认证和密钥协商的目的是为了让正常通信阶段更加安全。期间的很多安全认证和协商的内容和本章节的内容息息相关。所以本章节特提前于组网部分描述。

作为对网络安全的设计，本章节将对正常工作状态下的网络模型进行描述，然后增加相关的安全设计，来保证网络的安全可靠。

#### 正常情况下网络的工作模型

正如前文所言，远程抄表系统模型中拥有控制中心（主站），网络集中器（主节点）和设备模块（子节点）这三大核心部分。其中主站与主节点之间通过GPRS方式联通，不再本远程抄表系统课题范围之内，可以认为是安全的通道。而所有的主节点到子节点，以及子节点与子节点之间的通信通道可是不安全的。攻击者可以在开放的无线环境下做所有的事情。本论文参与的安全设计区间就在于主节点和子节点共同存在的开放式无线环境中，即下图中的不安全区域内。正常情况下，网络的所有数据包都将在此不安全区域内传递。下一节将对本网络作出合理的安全假设。



#### 安全假设

1. 信任中心与主节点之间的通信是安全的。不在本系统的考虑范围；
2. 主节点与子节点之间的通信信道是开放的，不安全的区域；
3. 子节点与子节点之间的通信信道也是开放的，不安全的区域；
4. 攻击者可以获得主节点及子节点的长地址等信息，了解各电表节点所在位置；
5. 攻击者拥有本网络所有网络帧的格式信息，可以对抓取到的网络包进行分析计算；
6. 网络的数据存在两种，点对点和广播，均发生在不安全区域。

基于如上的安全假设，网络的具体研究集中在不安全的区域，也就是说主节点与子节之间以及子节点与子节点之间的通信。如何针对1.3 所提出的安全需求来设计，提升网络安全性能是本章节所需重点研究的课题，也是本设计的核心目标所在。

#### 网络层数据安全设计

为了保护网络层数据的完整性和机密性，我们需要在网络层之外增加一个安全层次或者扩展网络包格式，来达到目的。其中ember公司针对zigbee协议所设计的安全模式是使用在网络层之外添加一个附加头和附加尾的形式【】，类似于添加了一个安全层次。这么做的好处在于安全层次扩展可以获得更灵活的设计，而不用担心原有网络层设计为安全留下的信息位是否够。可是不利的地方在于这么做会修改原有节点对网络包的解析顺序，解析模式的改变意味着大量的节点升级改动。而当前无线远程抄表系统的国家标准中，使用的是在网络层预留安全比特位信息的方式来操作的。这么做是为了使协议拥有更好的未来扩展性。但是缺点恰恰在添加安全层次方式所拥有的优点之上，由于原有保留位的不够，会很大程度影响安全设计的施展。从本质说来，这两种方式的核心是一致的。都是以附加信息的方式操作。同时考虑到微功率无线抄表标准，作为一个刚刚新生的标准，加之相关设计的欠缺，为了保障安全设计的尽可能全面，本文使用的是附加头的方式作安全系统的设计。

#### 安全层具体设计

接下来的部分将对这个新加的安全层次进行描述。下图为原有协议系统的网络层次构造图，里面包含了负责驱动单片机和射频芯片的驱动层，处理退避机制和保障节点单跳传输的mac层，负责网络组建、网络路由和网络控制的网络层，以及位于最上层的可以对接各种其他标准协议的应用层。

|  |
| --- |
| 应用层：用户数据 |
| 网络层：路由，维护 |
| Mac层：退避，单跳 |
| 驱动层：驱动设备 |

本安全系统的设计中，在应用层和网络层之间添加了一个用以支持安全机制的安全层。

|  |
| --- |
| 应用层：用户数据 |
| 安全层：支持安全机制 |
| 网络层：路由，维护 |
| Mac层：退避，单跳 |
| 驱动层：驱动设备 |

新增的安全层在帧格式中的表现为一个安全附加头和安全附加尾。附加头和附加尾之间的部分为网络层帧的数据载荷或者命令载荷部分。以下为增加安全层次之后的网络层帧模式。

网络层：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字节：8 | 1 | 变长 | 2或0 | 变长 |
| NWK包头 | 安全附加头 | 安全层载荷 | 安全附加尾 | 路由域 |

安全附加头设计的原则在于提醒收到相关网络帧的节点在处理相关命令的时候，节点可以通过安全附加头内部的信息，获得安全层载荷所使用的加密模式，以及安全附加尾的工作模式。下面将对新增的三个域进行分别描述。

1. 安全附加头

下图为安全附加头的帧格式设计。目前安全附加头预留一个字节

|  |  |  |
| --- | --- | --- |
| 比特：2 | 4 | 2 |
| 安全模式 | 帧计数 | 预留 |
| 安全头 | | |

各比特域的说明如下：

安全模式：两个比特标明安全层载荷的加密模式，具体见下表。需要特殊说明的是，如果同时拥有加密和添加附加尾的操作时，所有的操作模式应该是先加密后添加附加尾。

|  |  |
| --- | --- |
| 安全模式域值（二进制） | 对应设计 |
| 00 | 不加密，无安全附加尾 |
| 01 | 网络密钥加密，具有安全附加尾 |
| 10 | 点对点密钥加密，具有安全附加尾 |
| 11 | 不加密，具有安全附加尾 |

帧计数：类似于网络层帧序列号用途，发起者从0开始循环递增，子节点不处理同一节点的同一帧计数的帧，但是不影响转发。用以防止同一命令多次操作。

1. 安全附加尾

安全附加尾的格式实际上是一个带密钥的哈希函数HMAC的计算结果。用以保护网络帧的完整性，不仅仅防止数据自然变形，同时也可以附带认证功能。

#### 安全层的使用

在1.4.1.4的安全附加头中涉及到了两个网络密钥：网络密钥和点对点密钥。这两个密钥的产生源都是主节点。具体生成算法不在本安全系统设计的范畴之内，可以根据实际情况使用特定的算法。而在这两个密钥的使用上应该注意按照以下方式实行。网络密钥：这个密钥主要用以主节点和所有节点同时通信，即广播帧。密钥的设计是为了方式网外节点获得网络内部信息。这个密钥在组网协商的时候主节点通过临时密钥加密发送给对应子节点。在加密的时候，加密方式为对称加密。点对点密钥：这个密钥用以加密主节点和子节点之间的点对点通信，比如设置参数等命令中。目的是防止网络内其他节点获得特定节点的信息。在加密使用的时候，加密方式同网络密钥，也是对称加密。在发起者发送数据帧的时候有特定加密需求的时候会使用特定的密钥搭配特定的加密算法进行加密传输。

在1.4.1.4中还涉及到一个HMAC算法生成的附加安全尾域，这个域虽然设计为安全层的附加部分，但是实际上与加密算法是相对独立的两个部分。总体来说，安全层使用的具体流程如下：

1. 网络帧的发起者在获得了命令发送对象时，确定使用的密钥是网络密钥还是点对点密钥，同时确定是否使用附加安全尾。根据策略填充安全附加头的安全模式域，同时根据存储的安全帧计数加一，填充入附加头中。
2. 如果使用加密方式，则使用特定密钥和加密算法加密数据，填充入安全层载荷，否则直接填充数据域安全层载荷位置。
3. 如果需要使用安全附加尾，则使用选择的密钥作为HMAC的一个输入，同时将关键数据作为HMAC的另一个输入。输出结果作为安全附加尾的形式添加在关键数据之后。在没有使用加密算法的时候，HMAC使用的密钥为网络密钥。

这么做的方式的核心思想是，加强版的CRC校验，作为安全签名【】来进行发起源的安全认证。签名的使用仅仅针对所有的特定关键数据进行签名。为了保障网络的安全【】，本远程抄表安全系统均采用先加密后添加附加头的方式。

### 双向身份认证以及密钥协商

在了解了正常模式下的安全系统设计之后，下面需要解决的问题是点对点密钥的获得方式和节点入网时双向身份认证问题。相对应的，本节中所需要解决的是安全需求中的1）2）两项需求内容。文章接下来的段落将会对相关方向的研究进行简单的分析总结，并提出一个合理的安全设计。

#### 方案分析

远程抄表系统中的节点分为两大类：功能较为强大的主节点和功能很弱的子节点，其中子节点在运算和存储等各项资源都十分有限。同时由于远程抄表系统的传输速率较慢，大量的信息交互会导致组网认证时间的延长。双向身份认证和密钥协商协议在安全性保障的同时，应该秉着子节点越简单越好的和网络交互越少越好的原则设计。

RFID双向认证系统是在资源更为简单的软硬件环境下工作的，很多情况下安全的保障来源于一个标签和主节点之间的共享安全秘密的安全【】和一系列的共享秘密的同步更新。本远程抄表系统的安全设计可以借鉴此相关思路来尽可能的减少子节点开销。而远程抄表系统安全系统在设计的同时也要意识到单纯以共享安全秘密的方式来保障安全是不足够的。远程抄表系统所使用的节点在计算能力和存储能力上都要强于RFID标签，而且远程抄表系统的网络结构要复杂于RFID的网络结构，所以相关的算法可以不用拘泥于RFID使用的简单方式，而是可以使用更高级的一些方式。与远程抄表系统节点能力类似，但是网络结构却不同的网络主要是AD-Hoc自组织网络。目前对于此类网络的认证和密钥协商机制的研究主要分为了两大类，一类是基于公钥体系的安全设计【】，另一类是使用传统密钥体系，在预共享信息的帮助下进行交互协商【】。

公钥方式目前公认比较安全的有RSA和ECC两大类型，其中后者因为计算复杂度大大低于前者而成为了目前研究的热门。基于公钥的安全体系的优点在于，公钥体系在密钥的存储上可以以身份信息——例如长地址或者长地址的变形——作为公钥，而按照一定方式协商形成私钥。所以很多时候并不需要存储大量的密钥信息。而且公私钥对一旦形成，基于私钥的签名和基于公钥的加密都可以很自然而然地实施了，不再需要进一步单独的对于身份认证的协商。但是此类网络的缺点也同样明显。哪怕ECC方式的计算复杂度已经降低了很多，在计算能力薄弱的节点上要运行起相关的程序，仍然是一个十分艰难的任务。而且公钥方式普遍在密钥长度不够的情况下，安全性能会大打折扣。在八位的单片机上如果不是使用硬件来实现的话，运行效果将十分有限。传统的对称加密体系下的双向认证和密钥协商则处在公钥方式的两个极端的一个折中位置。他的安全性能不如公钥方式好，协商复杂度比公钥方式高，但是在节点上易于实现，简单部署。在能力薄弱的节点上应该来说是一种更加合适的方式。

通过以上方案分析，整理和综合考虑当前远程抄表系统的特点，本章节将从安全条件、安全流程和安全验证这几个方面阐述用于远程抄表系统的安全设计。

#### 安全条件

为了达到双向身份认证，我们需要一个共享的秘密值，主节点和子节点之间的认证将依赖于这一个共享的秘密。以下为具体需要增加的安全条件。

1. 主节点与子节点之间共享一个秘密值S和子节点的长地址IDsub；
2. 主节点存储有一个（ID，S，H(ID)）的三元组表格，其中Sn为主节点与子节点之间的秘密值(随机获得)，ID为子节点长地址。
3. 需要新增一个广播网络密钥Knet；
4. 一个用以鉴定身份的带密钥的哈希函数HMAC(key，M)，其中key为密钥，M为待加密文本；
5. 一个点对点密钥生成函数Gen(ID，ran)，其中ID为对应节点长地址，ran为特定长度的随机值，此函数仅主节点内部存储；
6. 一个对称加密算法SF(key，M)，其中key为密钥，M为待加密文本；
7. 一个随机值生成器，生成长度为l的串；
8. + ：此符号在本文章作为亦或的意义。

#### 安全流程

在以上的安全假设前提下，拟设计修改过的组网过程如下：

1. 长地址为IDsub1的未入网子节点上电，读取到长地址之后，向外发出信标请求帧期望得到已入网节点的回应；
2. 附近的在网节点收到IDsub1的信标请求回复信标，表明附近存在可用网络，信标中附带网络相关信息，如主节点长地址，网络号PanID等；
3. 子节点IDsub1在收集一定时间信标之后，从众多回复信标的在网节点中选择一个最优父节点IDsub2。向IDsub2发起入网请求，请求中附带子节点IDsub1。
4. 指定父节点IDsub2收到了入网请求时生成一个长度为l的随机值r1，发送给子节点IDsub1。
5. 子节点IDsub1在回应父节点IDsub2之前，首先生成一个长度为l的随机值r2。此随机值将作为IDsub1与主节点会话的临时密钥。

同时计算如下四个值：

H1 = HMAC(IDsub2，IDsub1)

H2 = HMAC(S，IDsub1)

M1 = S + r2

M2 = HMAC(S，r1 + r2)；

发送给指定父节点IDsub2。

1. 父节点IDsub2收到H1,H2, M1, M2之后，计算HMAC(IDsub2，IDsub1)，并入H1比较，如果两者相等，则使用自身与主节点的点对点密钥，采用对称加密算法将H2, M1, M2, r1传送给主节点，否则拒绝节点入网，终止过程。
2. 主节点收到IDsub2传送来的信息后，以H2为索引，在自身存储的三元组表的第三列元素中检索。如果找到对应的三元组，则继续计算一下两个值：

r3 = M1+S

M3 = HMAC(S，r1 + r3)，

如果M3与收到的M2相等则认为验证通过，允许入网，否则认为验证未通过不允许入网，终止过程。

1. 主节点将网络信息（包括主节点长地址、信道组号等）、Gen(IDsub1，r3)、Knet以及S+(r3>>l/2)通过对称加密算法使用r3作为密钥加密打包发给末端节点IDsub1。
2. 末端节点IDsub1收到信息之后计算S+(r2>>l/2)，判断与收到的S+(r3>>l/2)的值是否相等，如果相等则认为对主节点认证完成，接受入网配置。使用Knet为网络密钥，Gen(IDsub1，r3)为点对点密钥，与主节点进行交互。如果两者值不相等，则认为主节点认证不通过，拒绝接受入网，丢弃配置包内容。

下图为以上过程对应的流程图：

#### 安全分析

按照前一节中的安全设计，主节点与子节点以主节点与子节点之间共享的安全秘密作为安全的基线，可以完成一个双向的认证过程。这样极大的加强了子节点接入网络和主节点允许子节点接入网络时，对对方的认证。确保网络和加入的网络是正确的而且安全的。

由于子节点的计算资源的有限，所以所有的密钥生成，交由主节点完成。在入网时分配密钥时就使用了加密算法。而且密钥是子节点自主随机生成的。这样也能一定程度避免与共享密钥泄密的危险【】。

在不安全区域内传递的数据包括申请入网者长地址、一个协助认证的随机数r1，三个与安全秘密S息息相关的计算值H2，M1，M2，一个对用以辅助父节点对申请者验证的H1。还有两个使用攻击者未知密钥加密的网络帧。很显然，整个系统在S未知的情况下，攻击者是无法获得主节点与申请者之间的临时密钥r2的。更无法获得使用r2进行加密的网络信息。

而且本协议设计所使用的交互包只是在原有组网流程中多了一个单跳的入网申请的交互过程，涉及到的数据包传送仅仅为两个包。可以认为这样的设计对整个网络系统的开销增加是非常有限的。却在安全性上有了极大的提升。

### 网络密钥的更新和退出网络

网络的组建起来之后，可能因为安全原因，也可能由于设备的原因，网络管理者需要更换网络的密钥或者直接将网络取消。一个完整的远程抄表系统应该能够预料到这两种情况的发生，而做出相关的设计。相对于入网协商和正常工作情况下的安全方式的使用，网络密钥更新和退出网络，可以认为是网络的两个特定的功能。在默认前两个生命周期是安全的情况下，这两个功能是作为网络层的两个特殊命令设计的。他们属于安全层需要使用加密同时添加附加安全尾签名认证的范畴。

#### 密钥更新

当网络由于某种原因需要更换网络密钥的时候，远程抄表系统还应该拥有一种机制可以完成远程密钥调整。而根据实际情况，这个功能还可以分为两种情况：全网络的更新和点对点的更新。

当使用全网络更新功能是，网络层应该使用广播命令帧的格式发送，同时安全附加头中应该设置使用广播密钥同时具有附加安全尾的模式。关键数据应该是使用广播密钥加密后的原密钥和新密钥。在子节点收到了命令之后先判断安全帧计数和附加尾的HMAC，如果新帧不同于上次处理的特定帧而且认证通过的时候，比较现存有的两个密钥是否和网络帧中的原密钥相同。相同则修改现有密钥为新密钥。否则不处理此帧，但是不影响网络层转发。为了保证全网的成功率，主节点需要对此帧分批次多次发送，但是每次发送的安全帧计数不变。而后如果某些节点抄表不回或者返回解密数据无意义时，需要点对点对此节点进行更新密钥。当使用的是点对点密钥更新功能时。主节点使用的应该是点对点密钥，其他处理过程类似全网修改的广播阶段，子节点安全层处理不区分广播和点对点方式。唯一区别是点对点需要子节点回复确认命令。

#### 退出网络

退出网络存在三种方式，一种是子节点主动退出，一种是主节点点名退出，另一种是主节点发起的全网解散命令。下面将对这三种情况分别进行描述。

主节点点名退出：主节点对特定节点发出点对点命令，安全层使用点对点密钥加附加尾的模式。主节点需要子节点回应确认消息。在没有收到确认信息的前提下，主节点可以多次发送。子节点回复确认信息之后，清空所有网络信息。

主节点全网解散：主节点使用广播目标地址。安全层使用广播密钥加附加尾的模式。主节点多轮发送此命令，来保证到达的尽可能彻底。另一边子节点不回复确认信息。但是子节点在解散网络命令中指定时间内不清空网络信息，没收到一个新的退网帧则重置这个时间计时。直到这个计时超时，才清空网络信息。

子节点申请退网，此种情况目前不存在与本网络系统中。但是预留的设计为子节点发送申请之后，主节点走点名退出的同样流程。相当于给主节点增加了一个让特定子节点退网的命令渠道。

需要指出的是，由于全网解散可能无法使每个节点接到特定帧。子节点内部存在一个长时间计时。在每次子节点收到了所在网络的命令的时候，这个计时重置。而当这个计时时间超时的时候自动清空所有网络。防止遗留节点对网络进行干扰。

## 本章总结

本远程抄表系统的设计考虑了原有远程抄表系统中，对网络层信息保护不力的情况。增加了对网络层信息安全的保护，系统对网络的保护更加全面，也对整个系统的关键信息的机密性提供了更好的保障。同时采用了新的入网流程，在流程中增加了一个双方身份认证的安全过程。增加了攻击者通过假借网络公开信息对网络节点以及位于节点之后的电网终端进行攻击的难度，更好的保护了系统节点和终端。而在数据的完整性上，不单单保护了空中传输包的异变，也对恶意修改信息提出了相应的保护措施：使用HMAC技术，对网络包进行逐帧的签名，使得节点在处理相关命令时都可以完成对主节点的身份认证。最终，远程抄表系统还添加了特殊的网络命令及其操作流程。使得网络更新密钥和节点退出网络成为了可能，更加方便控制中心管理控制整个网络。相对于原有系统而言，本安全系统在网络安全的保护上更为全面具体。同时也不会加入太多大量的计算和包交互过程，具有比较强的实用价值。