基于 proverif 的物联网无线传感器节点轻量级认证协议方案设计*

李雁星　陈积常　李建

南宁学院信息工程学院，南宁 530200

摘　要　随着科技的发展，微型传感器已经有了很大的进步，它们不仅能实现多种功能，还能通过无线通信技术互相连接，构成一个由众多传感器节点组成的、覆盖全球的无线传感器网络，从而在各个领域中得到广泛的应用。本设计主要目标是研究无线传感器网络的轻量级认证设计策略，关注安全性和性能问题，提出了一种将防篡改加密算法和自组合交叉位运算相结合的一种创新认证方案，以提高受限设备的解密速度，从而减少资源消耗，本设计中详细介绍了实现认证的具体步骤，包括分析无线传感器网络被攻击的模型、安全防护措施、方案的认证措施及方案的防御方法等，还建立了基于 ProVerif 的无线传感器网络模拟测试平台，最后通过使用 ProVerif 自动化分析工具对该认证方案的算法进行验证，该方案明显降低了计算复杂度并提升了安全性能。

关键字　无线传感器网络，物联网，proverif，安全认证

Design of Lightweight Authentication Protocol for IoT Wireless Sensor Nodes Based on ProVerif

Li Yanxing　ChenJichang　Li Jian

School of Information Engineering
Nanning University, Nanning 530200, China;
Yanxing.li@foxmail.com

Abstract—With the development of technology, microsensors have made great progress. They not only have the ability to perform various functions but also can be interconnected through wireless communication technology, forming a wireless sensor network consisting of numerous sensor nodes that cover the entire globe. As a result, they have found extensive applications in various fields. The main objective of this design is to investigate lightweight authentication design strategies for wireless sensor networks, with a focus on security and performance issues. A novel authentication scheme combining tamper-resistant encryption algorithms and self-compositional bitwise operations is proposed to improve the decryption speed of resource-constrained devices and reduce resource consumption. This design provides a detailed description of the specific steps involved in implementing authentication, including analyzing attack models on wireless sensor networks, security measures, authentication measures, and defense methods. Furthermore, a wireless sensor network simulation and testing platform based on ProVerif is established. Finally, the proposed authentication scheme is validated using the ProVerif automated analysis tool, demonstrating reduced computational complexity and improved security performance.

Keywords—Wireless Sensor Networks, IOT,proverif, Security Authentication

1　引　言

近年来，随着通讯信息技术、传感器技术以及嵌入式计算技术的快速发展，微型传感器网络作为一种新型的网络技术[1]。无线传感器网络同时拥有感知能力、计算能力和通信能力，作为先进的网络技术，它在各个领域中都有着广泛的应用前景。物联网无线传感器网络是由传感器技术、嵌入式计算技术、分布式信息处理技术和通信技术等多种技术综合而成的。这些技术共同作用，使得无线传感器网络能够进行感知、计算和通信，从而实现各种应用场景，如智能家居、智能医疗、智能城市等[2]。

相关研究学者对无线传感器网络的安全性能、增强网络可靠性、优化数据采集和处理等性能的提升做出不少贡献。其中，Shi Haoming 等人在 2023 年提出采用国密技术对 zigbee 无线传感器网络进行加密，提高无线传感器网络的安全性与有效性[3]。Y.Lei 等人为了解决低功耗物联网中数据传输效率低下和安全认证等问题，解决低功耗物联网中数据传输效率低下和安

*基金资助：本文得到南宁学院一流专业培育项目（通信工程）(2020YLZYPY01)资助.

全认证等问题，以提高物联网的性能和可靠性[4]。研究人员提出了一些新的传输协议和加密算法，并在仿真环境下进行了性能评估和比较。此外，S Yu 等人在 2022 年提出了基于区块链和物理不可克隆函数的双向身份认证协议，实现了无线医疗传感器节点之间的基本状态信息双向认证[5]。K.Kalaiselvi 等提出了一种基于椭圆曲线的三方密钥协商协议，使用 160 位密钥长度的算法，并在计算时间、内存空间和带宽方面进行了优化[6]。

针对无线传感器设备的计算能力和存储容量有限，因此需要设计一种新的轻量级认证方案，以减少认证时间和功耗。

2 无线传感器网络安全认证需求分析

2．1 无线传感器网络概述

无线传感器网络是由大量分布式的、自组织的、具有感知、处理和通信能力的微型节点组成的网络。下图所示为无线传感器网络的体系结构，包括传感器节点、传感器区域、任务用户节点、因特网和卫星通信网。因特网和卫星通信网作为传输媒介，将多个节点的信息汇集到汇聚节点，并通过传感器区域的多跳传输模式将信息传递给任务用户节点。无线传感器节点可以通过不同方式传播到监测区域内。在这种以传感网络为中心的体系结构中，节点通过无线连接实现通信，每个节点充当路由器的角色，具有定位、自主动态搜索和回复连接的重要功能，将节点信息初步加工并传递给任务用户。相邻节点通过一对一的方式将信息传送到基站，进而通过用户和节点间的介质将信息传送给任务用户手上。

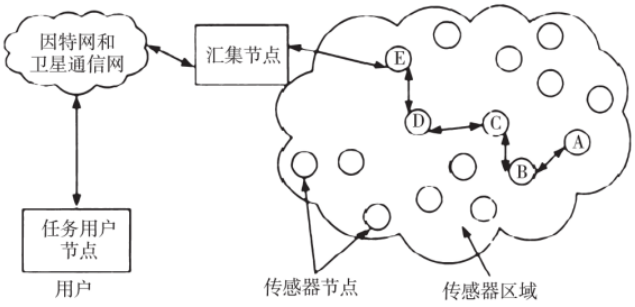

图 1 无线传感器网络体系结构

2．2 无线传感器网络安全认证需求分析

无线传感器网络中的传感器节点通常部署在无控制的环境中，如野外、工业区域等。这种开放的环境容易受到物理攻击、窃听和干扰，从而威胁到数据的安全性和可靠性[1]。

传感器节点通常具有有限的计算能力、存储容量和能量供应。这导致传感器节点难以实施复杂的安全机制，使得攻击者有机会利用资源有限性进行攻击，如拒绝服务攻击、能量耗尽攻击等。

无线传感网依赖无线传输来进行数据通信，而无线信号容易受到窃听和篡改。攻击者可以截获传输的数据，窃取敏感信息，或者篡改数据造成误导和破坏。

无线传感网中的数据通常是敏感的，如环境监测、军事侦察等。未经加密或不恰当的加密机制可能导致数据泄露和篡改，危及系统的完整性和保密性[7]。

在无线传感网中，节点的身份验证是一个重要的安全问题。攻击者可能伪造节点身份，进入系统并执行恶意操作，如数据注入、网络入侵等。

为了应对这些安全威胁，需要采取一系列安全措施，针对以上问题，本文设计一种基于 proverif 形式化安全分析的轻量级认证方案设计。

3 轻量级认证方案设计

本方案采用汇聚结构的网络模型，由若干个感知节点和汇聚节点组成。感知节点采集数据后传输到相应的集中点即汇聚节点，加密的无线通信网络传输相应收集的数据到管控中心进行认证，以确保感知节点数据的安全性。为验证无线传感器轻量级认证方案的安全性和可用性，本设计对其进行了详细的安全性分析，考虑了部署在公开环境中可能遭受的窃取攻击、假冒、重放攻击等攻击类型，并评估了该方案的安全性强度和抵御攻击的能力。下图所示展示了本方案的网络模型。

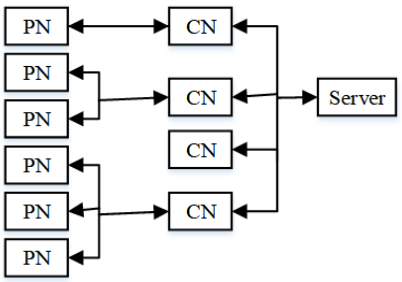

图 2 无线传感器网络通信的网络模型

在无线传感器网络的验证中，被划分成两个部分进行，前者是对感知节点进行初始化，后者是对无线传感器网络进行轻量级的双向验证。

3．1 感知节点初始化

初始化感知节点的主要工作是在被部署的环境里面查看对应身份消息有没有被未知人员攻击而被修改，还能提高节点的安全性能，如果对应身份消息安全则检测部位可以设置为安全状态 0，该初始化感知节点会继续检测环境内别的检测部位安全性。

服务器、感知节点和汇聚节点是无线传感器网络模型里面的通信节点，感知节点与服务器通信时需要进行验证，而汇聚节点则是相当于路由器功能一样具有处理能力和资源数据，服务器和感知节点通信必须先把汇集到汇聚节点，相当于传输介质，众多感知节点会对服务器进行验证访问，但必须经过汇聚节点，汇聚节点这时候发挥自己的处理能力，防止服务器被多次访问系统反应不过来。服务器相当于消息管控中心。

3．2　轻量级双向验证方案设计

本方案运用到的符号和符号描述：

表 1　方案字符说明表

符号	描述
PN	感知节点
CN	汇聚节点
Server	服务器
M	明文
K	会话密钥
H（）	防篡改加密函数
C	加密密文
c	防篡改加密密文 和会话密钥 K 的拼接密文
C_L、C_L, C_R、C_R	C、D 通信数据的左右部分
P	身份信息篡改位
Sac（X）	自组和交叉位运算
R	随机数
Rot（）	位移运算

下面是无线传感器节点方案，认证过程是双向的，分为三个部分：

(1) 防篡改加密

有范围的数据信息必须控制在在 3 个字节以内。设 M1M2M3 为一个明文信息序列，其中 M 为 3 个字节且其长度为一个字节，然后随机密钥生成器会自动生成会话密钥为 K。

以下就是防篡改加密的过程：

随机密钥生成器会自动生成会话密钥为 K。

明文 M 的信息被获取。

密文 C 是 M 和防篡改加密算法 H（）的算数融合，即：

$$C=HK（M⊕K） \quad （1）$$

会话密钥 K 和防篡改加密密文 C 拼接成为新的加密密文 c，即：

$$c=K+C \quad （2）$$

这里的密钥 K 是在初始化阶段由服务器 Server 与节点共同协商生成的。密钥 K 与密文 C 进行异或运算。以上算法流程如下图 3 所示。

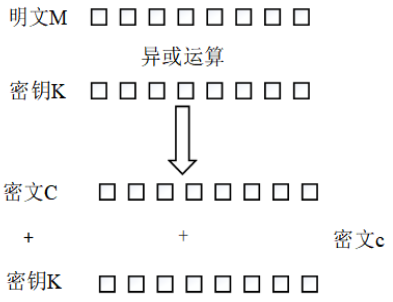

图 3　异或运算流程图

(2) 自组合交叉位运算（二次加密）

在该步骤中，进行第二次加密以防止攻击者监听密文传输。假设有三个 X 位的二进制组 A、B、Z，其中 $A=a_1a_2...a_x$，$B=b_1b_2...b_x$，$Z=z_1z_2...z_x$，a_i、b_i、$z_i∈\{0,1\}$，i=1，2，...，X。首先，对 A 和 B 进行异或运算得到 Z，然后进行自组合交叉位运算 Sac(Z)，将 Z 的高位和低位交叉组合形成新的 L 位数组 W，即 $Sac(Z) = z_1z_x/2+1z_2z_x/2+2...z_x/2z_x$[7]。

具体步骤如下：

感知节点发送认证请求命令 Request，自动随机生成 R1 并将计算出的加密数据 A、B、C_L 一起打包发送至汇聚节点，伴随的是等待汇聚节点的验证以及回复。

汇聚节点收到 Server 发送的数据信息后，将储存在汇聚节点的 MID、S 以及收到的数据信息 A、B 进行异或运算和自组合交叉位运算，得到加密数据 C 和 c。然后验证信息 C_L，如果 C_L=C_L′，说明协议合法，验证成功继续进行下一步计算。计算得到 D_L、E，并将其返回给 Server。如果 C_L≠C_L′，说明数据信息被攻击者篡改，协议终止。

实现公式如下：

$$A=S\_L⊕c \quad （3）$$

$$B=S\_R⊕C \quad （4）$$

$$（C\_L，C\_L）=Rot（c\_L⊕S）Sac（C⊕S） \quad （5）$$

$$（D\_L，C\_L）=Rot（c\_R⊕S）Sac（c⊕S） \quad （6）$$

$$S=Sac(c⊕S)Rot(c2⊕S) \quad （7）$$

自组合交叉位运算过程如图 4 所示。

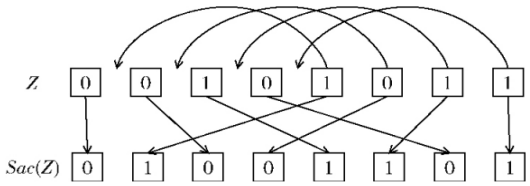

图 4 自组合交叉运算

(3) 解密

最先进行解密的是防篡改加密密文，其次进行自组合交叉位运算加密的解密过程。如果想了解信息数据是否被改动，则需要将现有的数据和经过解密的密文（即明文）进行比对。一旦发现信息数据被改动，该信息位置会被设置为 1 并且必须抛弃该信息数据，随之的是数据信息传输被终止。信息传输被终止就会重新检测初始化信道，相当于有 1 出现，初始化信道就会被启动。

如表所示，就是本文方案的认证过程，箭头指向都是服务器、感知节点和汇聚节点三个节点间的通信即身份信息认证之间的算法与流程。以下是认证方案的流程步骤：

（1） 感知节点的进程中，会自动生成时间戳和请求，分别是 T1、Request。服务器自动生成随机数 R，和服务器协商会话密钥 K，汇聚节点会接收到来自感知节点的 MID 和来自服务器的 R、密匙 K。

（2） 汇聚节点验证 Request 的合法性，须将 T1 和 K 进行一次异或运算。

（3）服务器收到汇聚节点传送时间戳 T1、Request 和 MID 的同时会再次验证 Request 的合法性和时间戳 T1 的计算。服务器将响应的 Request 信息即为 Request1 信息和 MID1 发送至汇聚节点。

表 2 轻量级验证流程

PN→ (M,MID)	←CN→ (MID)	←Server (K)
①生成Request和时间戳T1，MID →		①生成随机数R和密钥K ←
	②S=T1⊕R，Request，MID →	
		③服务器认证Request、T1，保存MID ←
⑤验证Request=Request′ MID′=MID 验证成功将进行N加密运算，否则终止会话。 C=HK (M⊕K) ，c=K+C →	④验证MID=MID′ ,会响应 Request′ ←	
	⑥A=S_L⊕c B=S_R⊕C (C_L, C_L) =Rot (c_L⊕S) Sac (C⊕S) (D_L, C_L) =Rot (c_R⊕S) Sac (c⊕S) S=Sac(c⊕S)Rot(c2⊕S) →	解密Cc会得到验证解密M′=M，M′=M用来验证时间戳T1，时间戳T1如果验证成功，则数据信息没有被改动，反之将抛弃数据信息，存储MID，数据信息传输结束，认证完成。

（4）MID 已经在汇聚节点中保存，验证 MID1=MID 和 Request1 就方便多了，只需要在内存中对比差异进行验证，对比结果相同就可以执行后面的验证操作，则感知节点接收到 MID 和 Request1，反之认证操作会被终止。

（5）感知节点接收到 MID 和 Request1 前会对它们进行验证，成功则进行加密运算。加密运算是 M 与 K 进行一次异或得到 C，再拼接密文 C 和会话 K 得到 c，然后汇聚节点将会收到来自感知节点的加密密文 c。

（6）Cc 是加密密文 c 取反得到的，将 Cc 传输到服务器就可以解出密文 C 和 M。服务器又会通过前面解出来的 C 和 M 进而解出 m，协商会话密钥 K 和密文 C 结合计算解出 m。

4 协议安全分析

4．1 基于 PROVERIF 的形式化安全分析

使用 windows10 电脑终端，在 proverif 形式化分析工具中编辑代码，定义了 even PNACServer（感知节点对服务器已经成功验证）、even ServerAcPN（服务器成功验证感知节点对应身份信息)和 even End(服务器对感知节点对应身份信息验证已结束）。另外还要查询攻击者是否获取到 Request 和 MID 这两个的数据信息。在环境部署实施中，由于 CN 是汇聚节点且不

进行数据信息运算处理，我们在网络环境中取消了 CN 的存在，使其仅起到汇聚数据的作用。

```
(* 事件 *)
event PNAcServer().
event ServerAcPN().
event End().
(* 查询 *)
query attacker(MID).
query attacker(Request).
query inj-event(End()) ==> inj-event(ServerAcPN()).
```

在 ProVerif 模拟平台执行代码后，电脑终端展示了进程 PN-CN 和 Server 的运行情况，表明并且代码没有出现报错。

```
-- Query not attacker(MID[])
Completing...
200 rules inserted. The rule base contains 198 rules. 30 rules in the queue.
400 rules inserted. The rule base contains 354 rules. 12 rules in the queue.
Starting query not attacker(MID[])
RESULT not attacker(MID[]) is true.
-- Query not attacker(Request[])
Completing...
200 rules inserted. The rule base contains 198 rules. 30 rules in the queue.
400 rules inserted. The rule base contains 354 rules. 12 rules in the queue.
Starting query not attacker(Request[])
RESULT not attacker(Request[]) is true.
-- Query inj-event(PNAcServer) ==> inj-event(ServerAcPN)
Completing...
200 rules inserted. The rule base contains 199 rules. 31 rules in the queue.
400 rules inserted. The rule base contains 359 rules. 24 rules in the queue.
Starting query inj-event(PNAcServer) ==> inj-event(ServerAcPN)
RESULT inj-event(PNAcServer) ==> inj-event(ServerAcPN) is true.
-- Query inj-event(End) ==> inj-event(ServerAcPN)
Completing...
200 rules inserted. The rule base contains 199 rules. 31 rules in the queue.
400 rules inserted. The rule base contains 359 rules. 24 rules in the queue.
Starting query inj-event(End) ==> inj-event(ServerAcPN)
RESULT inj-event(End) ==> inj-event(ServerAcPN) is true.
PS D:\proverif\proverif2.00> ./proverif
```

图 5 代码运行验证结果

运行结果表示，查询谁是 MID 和 Request 的攻击者，查询结果都显示不是 MID 和 Request 的攻击者，则没有攻击者获取到 MID 和 Request 的数据信息。认证协议代码没有出现报错并且顺利运行到最后，even PNACServer（感知节点对服务器已经成功验证）和 even ServerAcPN（服务器成功验证感知节点对应身份信息）也顺利验证结束，这意味着服务器和感知节点之间的认证方案的可行性并且是安全的。

4．3 安全性分析

（1） 去同步化攻击

攻击者有可能通过破坏三方密钥一致性来进行去同步化攻击。为了应对这种情况，在本协议中，后端数据库利用随机数 n 来更新共享密钥信息。后台数据库中存放了上一轮的共享密钥信息 K1 和最新的 Kn。如果使用 K1 进行 PN 的认证失败，后端数据库会利用 Kn 进行再次认证。只有在认证通过的情况下，协议才能继续进行。这样的设计使得协议能够防止密钥不同步问题的发生。

（2）假冒攻击

假冒攻击是一种潜在的威胁。攻击者试图冒充身份验证消息并以合法身份对 PN 进行攻击，以获取有效信息。为了防止这种攻击，PN 向服务器 Server 发送消息数据时，会生成一个时间戳 T1 并计算 S2=h(IDPN,APN,S1,t1,n1)。其中，IDPN 为 PN 的标识符，APN 为 PN 接入的网络标识符，S1 为已知的明文消息，t1 为时间戳，n1 为随机数。通过计算 S2，攻击者无法计算出真正的加密结果 S2，从而确保时间戳 T1 不会被更改，并确保数据的安全性。

（3）重放攻击

在防止重放攻击这种机制中，PN 在向服务器 Server 发送信息之前，会生成一个时间戳 T1，并使用计算出的随机数 S2 作为消息的签名。为了确保攻击者无法创建新的有效签名，PN 将使用加密密钥 PKs 对 S2 进行自组合交叉位算法运算，并将结果与 T1 一起发送给 Server。Server 将检查 T1 的有效性，并根据它来确定是否接受信息。同样地，当服务器 SN 向 PN 接收信息时，它将生成一个时间戳 T2，并使用计算出的随机数 S2 作为消息的签名。为了确保攻击者无法创建新的有效签名，SN 将使用加密密钥 PKr 对 S2 进行自组合交叉位算法运算，并将结果与 T2 一起发送给 PN。PN 将检查 T2 的有效性，并根据它来确定是否接受信息。由于攻击者无法获得加密密钥 PKs 或 PKr，因此他们无法创建新的有效签名或修改已经生成的签名。这确保了信息的安全性，并且防止了未经授权的访问或篡改。

（4）暴力破解攻击

在本文的协议中，所有信息都是加密传输的，不会直接暴露给攻击者。即使攻击者通过攻击截获和窃取数据信息，然后使他们可能获取其中的几个参数信息，但他们无法获得完整的 n1，因此无法正确破解出 K。此外，攻击者也不会知道具体的运算方式，因此无法破解出秘密信息 c。因此，即使攻击者能够获取一部分数据，也无法完整地解密和获取真实的敏感信息。

（5）窃取攻击

无线传感器网络中的硬件设备容易受到攻击，因此必须采取多种安全措施来确保数据的安全性。首先，我们采用保密措施来保护 Request、MID 和会话密钥 K 的机密性。其次，我们使用单向函数来保护 S1 和 S2 的数据信息的完整性。最后，我们采用加密算法和认证机制来防止攻击者的攻击。这些措施确保无线传感器网络数据的安全性，为用户提供可靠的数据服务。

我们比较了本文提出的协议与其他类似协议在安全性能方面的差异。具体来说，我们比较了该协议与

文献[10]、文献[9]和文献[8]的安全性能差异，这些文献分别提出了不同的协议。

在文献[10]中，协议的关键信息存储在设备中，因此无法防御物理攻击。这意味着，如果攻击者通过物理手段获取了存储设备中的信息，那么他们可以轻松地获取到关键信息。在文献[9]和文献[8]中，攻击者可以通过窃听、修改、假冒等攻击方式获取信息，所以些协议缺乏不可追踪性，因此攻击者可以轻松地跟踪认证信息，并追踪到前一轮或下一轮的认证信息。相比之下，本文提出的协议采用了多种安全技术，例如加密、身份验证等，可以有效地防御物理攻击和其他攻击方式。

表 3 协议安全性能比较

协议	双向认证	不可追踪性	暴力破解	重放攻击	去同步化	物理攻击
文献[9]	√	×	√	√	√	√
文献[8]	√	×	√	√	×	√
文献[10]	√	√	√	√	×	×
本协议	√	√	√	√	√	√

本协议中的标签仅使用了三种简单的单位运算，包括自组合交叉位和移位运算一次，异或运算六次。在认证过程中，只利用了异或运算来进行位提取操作，以满足超轻量级标准并降低成本。在表 4 中，使用 Y 表示异或运算，Z 表示自组合交叉位运算，X 表示循环移位运算，H 表示哈希运算，W 表示伪随机函数操作，L 表示函数输出的字节长度，以及方案中所有参数的字节长度。

表 4 协议性能比较

协议	存储费用	通信费用	计算
文献[9]	4L	5L	4H+2&
文献[8]	5L	4L	5W+3X
文献[10]	3L	L	4Y＋4&＋3S
本文协议	2L	L	6Y+Z

通过表 4 可以看出，与其他协议相比，本协议在存储量和通信量方面并未增加成本，反而是最低的。在计算量方面，虽然协议需要进行一些复杂的加密算法计算以确保三方完整认证，但由于采用了轻量级计算算法，整体计算量并未增加。因此，本协议在成本方面表现出优势，同时满足安全要求。

5 结束语

在无线传感器网络中，数据的安全性是一个重要问题，因为存在篡改、监听和伪造等风险。节点的脆弱性和局限性增加了数据安全性的挑战。本文针对这一问题设计了更合理有效的认证方案。这种方案能够确保数据的完整性和可靠性，防止信息泄露和网络瘫痪，所以认证机制在无线传感器网络的发展中尤为重要。此方案能够满足数据信息采集的安全需求，促进无线传感器网络的可靠应用。

此方案的计算复杂度降低，但使用范围考虑不全面，仅关注了外部攻击而忽略了内部攻击的可能性，存在一定不足。

参 考 文 献

[1] 苏耀丁，刘珍珍.无线传感器网络在军事领域中的运用[J].电脑编程技巧与维护，2019(07):71-75.

[2] 孙环.无线传感器网络中数据采集的节点重部署算法研究[D].桂林电子科技大学，2021.

[3] Shi Haoming,Zhu Xueping,Chen Jichang,Li Jian,School of Information Engineering Nanning University Nanning 530200,China,Journal of Computer Technology and Education,September 2023 Vol.11 No.3,P50-56.

[4] Y. Lei, L. Zeng, Y. -X. Li, M. -X. Wang and H. Qin, "A Lightweight Authentication Protocol for UAV Networks Based on Security and Computational Resource Optimization," in IEEE Access, vol. 9, pp. 53769-53785,2021,doi:10.1109/ACCESS.2021.3070683.

[5] Yu S, Park Y. A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions[J]. IEEE Internet of Things Journal, 2022, 9(20): 20214-20228.

[6] K.Kalaiselvi,G.R.Suresh,V.Ravi.An efficient approach for the detection of link failures in WBAN system for health care applications[J]. International Journal of Communication Systems,2019,32(15).

[7] 汪小威，卢志翔，陆涛.基于自组合交叉位运算的超轻量移动认证协议[J].计算机工程与设计，2017，v.38；No.372，70-75.

[8] Mahmood Azhar Qureshi,Arslan Munir. PUF-RAKE: A PUF-Based Robust and Lightweight Authentication and Key Establishment Protocol[J]. IEEE Transactions on Dependable and Secure Computing,2022,19(4).

[9] Prosanta Gope,Jemin Lee,Tony Q. S. Quek. Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions.[J]. IEEE Trans. Information Forensics and Security,2018,13(11).

[10] 马志豪，程良伦. 基于字合成运算的移动双向认证协议[J]. 计算机应用研究，2017，33（8）：814.