Computer Science and Application 计算机科学与应用, 2021, 11(9), 2387-2395
Published Online September 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.119244

Hans汉斯

面向智慧城市监控的无人机网络身份认证方案的分析与改进

李　蕊，亢保元，麦凯强

天津工业大学计算机科学与技术学院，天津
Email: 1103814823@qq.com, baoyuankang@aliyun.com, 337167647@qq.com

收稿日期：2021年8月21日；录用日期：2021年9月16日；发布日期：2021年9月26日

摘　要

智慧城市中的无人机在环境监测领域的应用越来越广泛，无人机被用来收集信息，用户通过他们的移动设备与特定飞行区域的无人机通信，以实时获取数据，所以无人机通信实体间传输数据的安全变得尤为重要。所以，为了避免敏感信息遭到截获和篡改则需要一个高效和安全的认证方案来使用户和无人机之间实现保密通信。2020年，Nikooghadam等人提出了一个可证明安全的轻量级智能城市监控无人机互联网认证方案。然而，本文分析了Nikooghadam等人提出的方案的安全性指出了该方案不能抵抗跟踪攻击、假冒用户攻击和假冒无人机攻击，为了克服该方案的安全缺陷，本文通过更新与用户有关的重要信息，提出一个改进方案。经过逻辑安全性分析以及与相关认证方案安全功能、计算通信开销的分析比较，证明了改进方案可以抵抗多种攻击，能够实现安全和高效的身份认证。

关键词

认证方案，密钥协商，无人机，智慧城市

Analysis and Improvement of Identity Authentication Scheme for UAV Network for Smart City Surveillance

Rui Li, Baoyuan Kang, Kaiqiang Mai

School of Computer Science and Technology, Tiangong University, Tianjin
Email: 1103814823@qq.com, baoyuankang@aliyun.com, 337167647@qq.com

Received: Aug. 21st, 2021; accepted: Sep. 16th, 2021; published: Sep. 26th, 2021

文章引用: 李蕊, 亢保元, 麦凯强. 面向智慧城市监控的无人机网络身份认证方案的分析与改进[J]. 计算机科学与应用, 2021, 11(9): 2387-2395. DOI: 10.12677/csa.2021.119244

Abstract

UAVs in smart cities are increasingly widely used in the field of environmental monitoring. UAVs are used to collect information, and users communicate with UAVs in specific flight areas through their mobile devices to obtain real-time data. Therefore, the safety of data transmission between UAVs becomes particularly important. Therefore, in order to avoid the interception and tampering of sensitive information, an efficient and secure authentication scheme is needed to achieve secure communication between the user and the UAV. In 2020, Nikooghadam *et al.* proposed an Internet certification scheme for a lightweight and provably safe smart city surveillance drone. However, this paper analyzes the security of the scheme proposed by Nikooghadam *et al.* and points out that the scheme cannot resist tracking attack, impersonating user attack and impersonating drone attack. In order to overcome the security defects of the scheme, this paper proposes an improved scheme by updating important information related to users. Through the analysis of logical security and the comparison with the security function and computational communication cost of related authentication schemes, it is proved that the improved scheme can resist various attacks and achieve secure and efficient identity authentication.

Keywords

Authentication Scheme, Key Agreement, UAV, Smart City

1. 引言

智慧城市由智慧治理、智慧出行、智慧生活、智慧环境、智慧经济、智能人 6 个部分组成[1]，以云计算为数据储存平台，智能设备为信息交互工具。市民用户可以通过智能设备登录、发送和接受数据信息。例如，在智慧城市中将传感器嵌入到交通系统中，人们可以通过自己的移动设备实时监测所要乘坐交通工具的位置以及满座率等实用信息[1]。智慧城市是一种城市规划、建设、管理和服务智慧化的新理论和新模式。

无人机称为 UAV (英文)，是智慧城市的重要组成部分，是目前应用较为广泛的一种无人驾驶的航空器。无人机配备有比较完善的航拍系统、高清摄像头以及红外热像仪等。无人机的应用较为广泛，种类比较繁多[2]。为市民提供智能移动和监视，这些无人机将占据低空空域并提供各种服务。无人机包括不同类型的传感器，比如无线电探测和测距传感器、飞行时间(ToF)传感器、光脉冲距离传感器、磁场变化传感器、方向传感器以及热和化学传感器[3]。并且通过它们之间的协同编队可以支持各种应用[4] [5] [6]。无人机已经潜移默化地渗透到了人们的日常生活中，随着技术的不断更新，无人机传感器收集的数据面临着新的安全挑战和隐私问题，在无人机网络中，通过无人机上的传感器进行通信和收集数据，然后将数据发送到控制服务器。持有移动设备的用户可以通过控制服务器在特定飞行区域通过其移动设备监控和访问一些无人机。因为数据的传输都处于公开的信道，容易遭到恶意黑客截获和篡改，因此需要一种相互认证方案 AKA (Authenticated Key Agreement schemes)，可用于在共享秘密之前验证通信参与者的真实身份，方案中通信实体间可以建立共享密钥，并用其加密传送中的敏感信息。1981 年 Lamport [7]提出

首个基于可记忆口令的用户身份认证方案。在 2016 年，Seo [8]针对智慧城市中无人机通信过程提出了三种适用于不同通信场景的加密方案，允许无人机有效地从数百个智能对象收集数据。在 2017 年 Won 等人[9]提出了一种高效的无证书签密标签密钥封装机制，该机制支持认证密钥协商、不可否认和用户撤销，减少了在无人机和智能对象之间建立共享密钥所需的时间。在 2018 年，Cheon 等人[10]提出了一个实时同态认证加密方案的无人机网络应用。为了处理远程访问和身份验证问题，Srinivas 等人[11]设计了一个轻量级的身份验证方案，称为 TCALAS，是为无人机网络环境设计的。然而，Ali 等人[12]指出，Srinivas 等人[11]的模型无法抵抗被盗验证器攻击和用户可追溯性。他们进一步引入了一个被称为 iTCALAS 的改进方案，以解决这些问题并为无人机网络提供可扩展性。Teng Li 等人[13]提出了一种基于椭圆曲线的无人机认证机制。此外，Bera 等人[14]提出了一个基于区块链的方案，以确保无人机网络环境中的通信安全。Ever [15]提出了一个基于椭圆曲线的无人机网络环境认证框架，在该框架中，无人机被视为 WSN 物联网应用的移动接收器，旨在提高传感器节点的生命周期和连通性。该方案与无人机技术兼容，能够抵抗密钥泄露假冒攻击和密码猜测攻击。2020 年，Nikooghadam 等人[1]提出了一个可证明安全的轻量级智能城市监控无人机互联网认证方案，该方案中有三个参与者，分别是用户 U_i 、无人机 V_j 和控制服务器 CS。在控制服务器的协助下用户 U_i 与无人机 V_j 可以相互认证并建立会话密钥以保证通信安全。他们声称此方案可以抵抗所有攻击，然而通过对方案的分析，我们发现此方案存在许多安全漏洞：不能抵抗假冒攻击、跟踪攻击、假冒用户攻击等。针对此方案的安全问题我们提出一个改进方案，并对改进方案进行了逻辑安全性分析。通过与相关认证方案在计算通信开销和安全属性方面的比较，结果表明改进方案在降低计算量条件下有效地保证了方案的安全高效性。

组织结构

文章第二节回顾 Nikooghadam 等人方案；第三节对 Nikooghadam 等人方案存在的安全问题进行分析；第四节提出了改进的新方案；第五节对改进方案进行安全性分析；第六节从性能与安全两方面对比分析相关协议；第七节结束语。

2. Nikooghadam 等人方案回顾

首先简单回顾 Nikooghadam 等人的方案，此方案包括三个参与者：用户(U_i)，无人机(V_j)和控制中心(CS)。该方案包括 6 个阶段，分别是建立阶段、用户注册阶段、无人机注册阶段，登录和认证阶段、口令更新阶段以及动态无人机加入阶段。但限于篇幅，本节只回顾重点的系统建立阶段，用户以及无人机注册阶段，用户登录以及用户与无人机相互认证阶段。本文所用到的符号及意义如表 1 所示。

Table 1. Notations used in this paper
表 1. 符号定

符号	定义
U_i	第 i 个用户
V_j	第 j 个无人机
ID_i	U_i 的身份值
ID_j	V_j 的身份值
CS	控制服务器
S	CS 的密钥

Continued

P	$E_p(a,b)$ 上的点
sk	会话密钥
ΔT	允许的最大延迟
T_x	时间戳
$h(.)$	哈希函数
$\oplus$	异或运算
$\|\|$	比特连接运算
$a_j, d_i, q_i, z_i, g_j, r_1, r_2, r_3, r_4, r_5$	从 z_p 选出的随机数

2.1. 系统建立

在这个阶段，控制服务器 CS，选一个大素数 p，自己的私钥 $s \in Z_p$，并选取椭圆曲线 $E_p(a,b)$ 和该椭圆曲线上的一个基点 P，有限域为 Z_p，选取单向哈希函数 $h:\{0,1\}^* \to \{0,1\}^l$，公开系统的参数 $\{E_p(a,b), p, P, h(\cdot)\}$ 以及保密自己的私钥 $s \in Z_p$。

2.2. 无人机注册阶段

无人机 V_j 通过下面的步骤向控制服务器 CS 注册：

1) V_j 选取身份值 ID_j 并且通过安全信道传给 CS。

2) CS 收到注册请求，检查 ID_j，选择随机数 $a_j \in Z_p$，计算，$PID_j = h(a_j \| ID_j)$，$Key_j = h(ID_j \| s \| a_j)$，将 (ID_j, PID_j, Key_j) 存在数据库中，并向 V_j 发送 $\{ID_j, PID_j, key_j, h(\cdot)\}$，$V_j$ 收到 $\{ID_j, PID_j, key_j, h(\cdot)\}$ 后并保存起来。

2.3. 用户注册阶段

用户 U_i 通过如下步骤向控制服务器 CS 注册：

1) 用户 U_i 选择自己的身份值 ID_i 和口令 PW_i。他的移动设备选择一个随机数 $d_i \in Z_p$，计算 $ppw_i = h(h(ID_i \| d_i) \oplus h(PW_i \| d_i))$，并通过安全信道向 CS 发送 $\{ID_i, ppw_i\}$。

2) 当 CS 接收到 $\{ID_i, ppw_i\}$ 后，CS 选择两个随机数 $f_i, q_i \in Z_p$，并计算：

$FID_i = h(ID_i \| f_i)$，$K_i = h(FID_i \| s \| q_i)$，$A_i = h(FID_i \| ppw_i \| f_i \| K_i)$，$B_i = h(A_i \| FID_i)$ CS 存储 (ID_i, FID_i, K_i)，并向用户 U_i 通过安全信道发送 $\{f_i, K_i, B_i, h(\cdot)\}$。

3) 用户 U_i 存储 $\{d_i, f_i, K_i, B_i, h(\cdot)\}$ 于移动设备中。

2.4. 登录与认证阶段

1) 用户 U_i 向移动设备输入 ID_i, PW_i，用户的移动设备计算 $ppw_i^* = h(h(ID_i \| d_i) \oplus h(PW_i \| d_i))$，$FID_i^* = h(ID_i \| f_i)$，$A_i^* = h(FID_i^* \| ppw_i^* \| f_i \| K_i)$，$B_i^* = h(A_i^* \| FID_i^*)$ 移动设备检查 B_i^* 是否与 B_i 相等，如果不相等则就中止会话。

用户 U_i 移动设备选择时间戳 T_1（T_1 为用户当前时刻），随机数 $z_i \in Z_p$，并计算 $A1_i = h(T_1 \| FID_i \| K_i)$，通过公开信道向 CS 发送 $\{T_1, z_i P, A1_i, FID_i, PID_j\}$。

2) CS 收到 $\{T_1, z_i P, A1_i, FID_i, PID_j\}$ 信息后，检查时间戳：$|T_2 - T_1| \le \Delta T$，如果时间戳有效，CS 根据 FID_i

从数据库中提取(ID_i, FID_i, K_i)并计算$A1'_i = h(T_1 \| FID_i \| K_i)$，检查$A1'_i$是否与$A1_i$相等？如果不相等则终止会话，若相等，$CS$计算$K_{ij} = K_i \oplus key_j$，$A2_i = h(PID_j \| key_j \| ID_j \| K_i)$。$CS$通过公开信道向$V_j$发送$\{A2_i, T_2, z_i P, PID_j, k_{ij}, FID_i\}$。

3) V_j收到$\{A2_i, T_2, z_i P, PID_j, k_{ij}, FID_i\}$后，$V_j$首先检查时间戳$T_2$，通过$|T_3 - T_2| \le \Delta T$，如果满足条件，计算$K_i = K_{ij} \oplus key_j$，$A2_j = h(PID_j \| key_j \| ID_j \| K_i)$，然后检查$A2_i$是否与$A2_j$相等，如果不相等则终止会话。如果相等$V_j$选择一个随机数$g_j \in Z_p$，并计算$sk_j = h(ID_j \| g_j z_i P \| K_i \| FID_i)$，$Auth_j = h(sk_j \| FID_i \| T_3 \| K_i)$，最后$V_j$通过公开信道向用户$U_i$发送$\{g_j P, T_3, Auth_j\}$。

4) 当用户U_i接收到$\{g_j P, T_3, Auth_j\}$，首先检查时间戳，通过$|T_4 - T_3| \le \Delta T$，如果满足条件，U_i计算$sk_i = h(ID_j \| z_i g_j P \| K_i \| FID_i)$，$Auth_i = h(sk_i \| FID_i \| T_3 \| K_i)$，用户的移动设备检查$Auth_i$是否等于$Auth_j$，如果相等，$U_i$认证了$V_j$。如果不相等，则终止会话。

3. Nikooghadam 等人方案的安全分析

3.1. 跟踪攻击

在 Nikooghadam 等人方案的用户U_i注册过程中，CS计算U_i的伪身份$FID_i = h(ID_i \| f_i)$，而在整个方案中，FID_i是固定不变的。所以，当一个攻击者截获用户的登录信息$\{T_1, z_i P, A1_i, FID_i, PID_j\}$后，攻击者可以由此信息中$FID_i$追踪用户的访问行为。

3.2. 假冒无人机攻击

当U_i与V_j进行相互认证时，在登录与认证阶段的第 3 步，V_j可以通过计算$K_i = K_{ij} \oplus key_j$获得用户$U_i$的秘密值$K_i$。如果$U_i$下一次想要与$V_e$进行通信，恶意的服务器$V_j$可以假冒无人机$V_e$欺骗用户$U_i$。具体步骤如下：

1) 恶意服务器V_j可以通过用户登录消息$\{T_1, Z_i P, A1_i, FID_i, PID_e\}$中的$FID_i$来跟踪$U_i$，并截获由$CS$向$V_e$传输的信息$\{A2_i, T_2, z_i P, PID_e, k_{ie}, FID_i\}$，再计算$key_e = K_{ie} \oplus K_i$。

2) V_j随机选择$r_e \in Z_p$，接着计算$sk'_e = h(ID_e \| r_e z_i P \| K_i \| FID_i)$，$Auth'_e = h(sk_e \| FID_i \| T_3 \| K_i)$，并向用户$U_i$传送$\{r_e P, T_3, Auth_e\}$。

3) U_i收到此信息后，计算$sk_i = h(ID_e \| z_i r_e P \| K_i \| FID_i)$，$Auth_i = h(sk_i \| FID_i \| T_3 \| K_i)$，并验证$Auth_i$与$Auth'_e$是否相等？显然，它们是相等的。于是，$V_j$成功假冒了$V_e$。

3.3. 假冒用户攻击

当U_i与V_j完成一次相互认证过程，V_j可以获得与用户私密相关并且固定不变的K_i，并存下(K_i, FID_i)。如果U_i要与V_e进行通信，恶意无人机V_j会假冒用户U_i欺骗无人机V_e。具体步骤如下：

1) 恶意无人机V_j通过跟踪用户登录消息$\{T_1, Z_i P, A1_i, FID_i, PID_j\}$中的$FID_i$来判定$U_i$的行为动向，然后选取$z'_i \in Z_p$并生成登录信息$\{T_1, z'_i P, A1_i, FID_i, PID_e\}$冒充用户$U_i$，然后将登录信息发送给控制服务器$CS$。

2) CS收到$\{T_1, z'_i P, A1_i, FID_i, PID_e\}$后，$CS$根据$FID_i$从数据库中提取$(ID_i, FID_i, K_i)$并计算$A1'_i = h(T_1 \| FID_i \| K_i)$，检查$A1'_i$是否与$A1_i$相等?再计算$K_{ie} = K_i \oplus key_e$，$A2_i = h(PID_e \| key_e \| ID_e \| K_i)$。$CS$通过公开信道向$V_l$发送$\{A2_i, T_2, z'_i P, PID_e, k_{ie}, FID_i\}$。

3) V_l收到$\{A2_i, T_2, z'_i P, PID_e, k_{ie}, FID_i\}$后，计算$K_i = K_{ie} \oplus key_e$，$A2_e = h(PID_e \| key_e \| ID_e \| K_i)$，然后检查$A2_i$是否与$A2_e$相等？如果不相等则终止会话。如果相等$V_l$选择一个随机数$g_e \in Z_p$，并计算$sk'_e = h(ID_e \| g_e z'_i P \| K_i \| FID_i)$，$Auth'_e = h(sk_e \| FID_i \| T_3 \| K_i)$，最后$V_e$通过公开信道向用户$U_i$发送$\{g_e P, T_3, Auth_e\}$。

4) 当恶意无人机 V_j 截获 $\{g_eP,T_3,Auth_e\}$ 后，V_j 根据存下的 K_i 和自己选取的 $z_i' \in Z_p$，计算 $sk_i'=h(ID_e \| z_i'g_eP \| K_i \| FID_i)$，$Auth_i'=h(sk_i \| FID_i \| T_3 \| K_i)$。并验证 $Auth_i'$ 与 $Auth_e'$ 是否相等？显然，它们是相等的。于是，V_j 成功假冒了用户 U_i。

4. 改进方案

针对 Nikooghadam 等人的方案存在的不能抵抗跟踪攻击、假冒用户攻击、假冒无人机攻击的问题。我们通过更新与用户相关的重要信息，提出一个改进的安全认证和密钥协商方案，所提改进方案包括三个实体分别是用户 U_i，无人机 V_j，控制服务器 CS，改进方案包括四个阶段分别是：用户注册阶段，无人机注册阶段，用户登录阶段以及相互认证密钥协商阶段。

4.1. 用户注册阶段

用户 U_i 通过如下步骤向控制服务器 CS 注册：

1) 用户 U_i 选择自己的身份值 ID_i 和口令 PW_i。他的移动设备选择一个随机数 $r_1 \in Z_p$，计算 $ppw_i=h(h(ID_i \| r_1) \oplus h(PW_i \| r_1))$，并通过安全信道向 CS 发送 $\{ID_i,PPW_i\}$。

2) 当 CS 接收到 $\{ID_i,PPW_i\}$ 后，CS 选择一个随机数 $r_2,r_3 \in Z_p$，并计算：$FID_i=h(ID_i \| r_2)$，$K_i=h(FID_i \| s \| r_3)$，$A_i=h(FID_i \| PPW_i \| r_2 \| K_i)$ 和 $B_i=h(A_i \| FID_i)$。当上述计算完成后，CS 存储 $\{ID_i,FID_i,K_i\}$，并将 $\{r_2,K_i,B_i,h(\cdot)\}$ 通过安全信道发送给用户 U_i，U_i 收到此消息后将 $\{r_1,r_2,K_i,B_i,h(\cdot)\}$ 存储到移动设备中。

4.2. 无人机注册阶段

无人机 V_j 通过下面的步骤向控制服务器 CS 注册：

1) V_j 选择身份值 ID_j，并通过安全信道将 ID_j 发送给 CS。

2) CS 收到 ID_j 后，选择一个随机数 $a_j \in Z_p$，并计算 $PID_j=h(ID_j \| a_j)$，$key_j=h(PID_j \| ID_j \| s \| a_j)$，$CS$ 存储 $\{ID_j,PID_j,key_j\}$ 于数据库里。CS 将 $\{ID_j,PID_j,key_j,h(\cdot)\}$ 通过安全信道传送给 V_j，V_j 收到 $\{ID_j,PID_j,key_j,h(\cdot)\}$ 后并存储。

4.3. 用户登录阶段

1) 在此阶段，用户 U_i 想要成功登录 V_j，首先需要在移动设备中输入 ID_i,PW_i，移动设备收到后则进行以下计算：$ppw_i^*=h(h(ID_i \| r_1) \oplus h(PW_i \| r_1))$，$FID_i^*=h(ID_i \| r_2)$，$A_i^*=h(FID_i^* \| PPW_i^* \| r_2 \| K_i)$ 和 $B_i^*=h(A_i^* \| FID_i^*)$。最后，用户的移动设备检验 $B_i^* ?= B_i$，如果条件成立，表示用户 U_i 的身份和口令 ID_i,PW_i 通过了移动设备的验证。

2) 用户 U_i 的移动设备选择时间戳 T_1 和一个随机数 $r_4 \in Z_p$，计算 $A1_i=h(FID_i \| K_i \| T_1)$，并将 $\{A1_i,FID_i,r_4P,PID_j,T_1\}$ 通过公开信道传送给 CS。

4.4. 认证与密钥协商阶段

在此阶段，用户 U_i 与无人机 V_j 在 CS 的协助下实现相互认证，建立一个会话密钥 SK，SK 用于用户 U_i 与无人机 V_j 完成未来保密通信。具体步骤如下：

1) CS 收到登录信息后，首先通过 $|T_1-T_1^*| \le \Delta T$，检查时间戳 T_1，其中 T_1^* 是 CS 收到信息的当前时间戳。如果条件成立，CS 通过 FID_i 检索到 $\{ID_i,FID_i,K_i\}$，并计算 $A1_i'=h(FID_i \| K_i \| T_1)$，验证 $A1_i' ?= A1_i$，如果条件不成立，CS 则终止会话，否则 CS 选择一个随机数 $r_5 \in Z_p$，计算：$FID_i^n=h(ID_i \| r_5)$，

$CID_i = FID_i^n \oplus h\left(K_i \| ID_j\right)$， $A2_i = h\left(FID_i^n \| K_i\right)$， $K_{ij} = h\left(K_i \| ID_j\right) \oplus key_j$，$A3_i = h\left(PID_j \| key_j \| ID_j \| h\left(K_i \| ID_j\right)\right)$。$CS$ 存储 $\left\{FID_i^n\right\}$ 于数据库中并将 $\left\{A2_i, T_2, r_4P, PID_j, K_{ij}, CID_i A3_i\right\}$ 通过公开信道传送给 V_j。

2) V_j 收到信息后，首先通过 $\left|T_2 - T_2^*\right| \le \Delta T$，检查时间戳 T_2，其中 T_2^* 是 V_j 收到信息的当前时间戳，如果验证通过，V_j 计算： $h\left(K_i \| ID_j\right) = K_{ij} \oplus key_j$， $A3_j = h\left(PID_j \| key_j \| ID_j \| h\left(K_i \| ID_j\right)\right)$，$FID_i^n = CID_i \oplus h\left(K_i \| ID_j\right)$。$V_j$ 检验 $A3_j ? = A3_i$，如果验证通过，则表明可信机构 CS 身份认证成功。

3) V_j 选择一个随机数 $r_6 \in Z_p$，计算会话密钥 $SK_j = h\left(ID_j \| r_6 r_4 P \| h\left(K_i \| ID_j\right) \| FID_i^n\right)$ 和验证信息 $Auth_j = h\left(SK_j \| FID_i^n \| T_3 \| A2_i\right)$，最后 V_j 将当前有效信息 $\left\{r_6P, T_3, Auth_j, CID_i\right\}$ 通过公开信道发送给用户 U_i。

4) U_i 收到上述信息后首先检查时间戳 T_3，通过 $\left|T_3 - T_3^*\right| \le \Delta T$，其中 T_3^* 是 U_i 收到信息的当前时间戳，如果条件成立，U_i 则计算 $FID_i^{n\prime} = CID_i \oplus h\left(K_i \| ID_j\right)$， $A2_i' = h\left(FID_i^n \| K_i\right)$ 以及会话密钥和验证信息 $SK_i = h\left(ID_j \| r_4 r_6 P \| h\left(K_i \| ID_j\right) \| FID_i^{n\prime}\right)$， $Auth_i = h\left(SK_i \| FID_i^n \| T_3 \| A2_i'\right)$。最后 U_i 验证 $Auth_j ? = Auth_i$，若两者不相等，U_i 则中止会话，用户与无人机通信失败；若验证通过，则表明用户认证无人机 V_j。从上述步骤分析，可以得出 $SK_i = SK_j$，用户 U_i 与无人机 V_j 相互认证并建立会话密钥。

5. 改进方案的安全性分析

5.1. 抵抗跟踪攻击

在改进方案中的每一次会话过程中，即使攻击者截获 $\left\{A2_i, T_2, r_4P, PID_j, K_{ij}, CID_i A3_i\right\}$ 和 $\left\{r_6P, T_3, Auth_j, CID_i\right\}$，也无法通过计算并获得 $FID_i^n = CID_i \oplus h\left(K_i \| ID_j\right)$。并且 CS 计算的 $FID_i^n = h\left(ID_i \| r_5\right)$ 是动态变化的，其中参数 r_5 在每一次会话中随机产生的，每次会话选取的随机数不同，用户每次发起的会话都不相同。在不同的会话过程中用户的伪身份 FID_i 是不同的，用户的行为轨迹不能被攻击者追踪。通过以上分析，改进方案成功实现了抵抗跟踪攻击。

5.2. 抵抗假冒无人机攻击

根据本文 5.1 改进方案抵抗跟踪攻击，所以恶意无人机 V_j 无法再通过原方案中存在于消息 $\left\{A3_i, T_2, z_iP, PID_j, k_{ij}, FID_i\right\}$ 和 $\left\{T_1, z_iP, A1_i, FID_i, PID_j\right\}$ 中的 FID_i 判断用户 U_i 下一步要与哪个无人机通信。并且恶意无人机 V_j 与用户 U_i 完成一次通信获得了仅能获得 $h\left(K_i \| ID_j\right)$。即使截获了用户 U_i 与 V_l 通信过程中的信息 $\left\{A2_i, T_2, r_4P, PID_l, K_{il}, CID_i\right\}$，也无法通过 $key_l = h\left(K_i \| ID_l\right) \oplus K_{il}$ 计算得到无人机 V_l 秘密值 key_l，更无法假冒无人机计算会话密钥 SK。综上所述，改进方案成功实现了抵抗假冒无人机攻击。

5.3. 抵抗假冒用户攻击

根据本文 5.1 的改进方案可以抵抗跟踪攻击，攻击者无法根据 FID_i 跟踪用户的行为轨迹。并且恶意无人机 V_j 与用户 U_i 完成一次通信并仅可获得 $h\left(K_i \| ID_j\right)$，每次会话 $h\left(K_i \| ID_j\right)$ 都是不同的。攻击者再无法获得 PW_i, r_1 的情况下，无法计算有效的登录请求 $\left\{A1_i, FID_i, r_4P, PID_j, T_1\right\}$，无法假冒合法用户登录相应的实体。所以改进方案成功实现抵抗假冒用户攻击。

6. 改进方案的比较

在本节中，就安全属性和计算成本两方面对改进方案同 Nikooghadam 等人方案进行对比分析。表 2 和表 3 分别显示了安全属性和计算成本的比较结果。从表 2 来看，改进的方案在安全性方面远优于 Nikooghadam [1] [15] [16] [17] [18]等人的方案。此外，从表 3 中，Nikooghadam [1] [16] [17] [18] [19]等人的方案的总计算

成本分别是 23H+4X、30H+16X、32H+18X、33H+16X、44H+25X，而改进的方案的总计算成本是 34H+7X。虽然计算成本高于原方案，但是改进方案可以抵抗各种攻击。综合分析得出改进方案在没有增加很多计算成本基础上保证了通信的安全性。

Table 2. Comparison of security features
表 2. 安全属性比较

方案	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
[1]	Yes	Yes	No	Yes	No	No	No	No	Yes	Yes
[15]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No
[16]	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
[17]	Yes	Yes	Yes	No	Yes	No	No	No	Yes	Yes
[18]	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes
改进方案	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

F1：相互认证；F2：用户匿名性；F3：抵抗假冒可信机构攻击；F4：抵抗重放攻击；F5：抵抗密钥泄露攻击；F6：抵抗跟踪攻击；F7：抵抗假冒用户攻击；F8：抵抗假冒传感器攻击；F9：支持完全前向保密；F10：抵抗内部攻击。

Table 3. Comparison of the computational cost
表 3. 计算成本比较

方案	P1	P2	P3	P4
[1]	9H+1X	7H+1X	7H+2X	23H+4X
[16]	6H+2X	6H+5X	18H+9X	30H+16X
[17]	11H+5X	8H+8X	13H+5X	32H+18X
[18]	10H+4X	5H+2X	18H+10X	33H+16X
[19]	12H+6X	12H+9X	20H+10X	44H+25X
改进方案	9H+1X	7H+1X	18H+5X	34H+7X

P1：注册阶段；P2：登陆阶段；P3：认证阶段和密钥协商阶段；P4：总计算成本；H：哈希计算及时间成本；X：XoR 操作及时间成本。

7. 结束语

本文首先分析了 Nikooghadam 等人的方案，指出其方案不能抵抗跟踪攻击、假冒无人机攻击、假冒用户攻击。为了消除以上安全缺陷，本人通过更新与用户相关的重要信息，提出了一个改进的面向智慧城市监控的无人机网络身份认证方案。并且通过逻辑分析对方案进行了安全证明。与现有的无人机相关的身份认证协议在计算开销以及安全属性方面进行了比较，结果表明本文方案的计算量相对比较低，且满足了所有的安全属性，适用于资源受限且安全性要求高的无线传感网络领域的应用。然而，今后还需要在保证方案的安全性的同时降低计算量以及研究设计适用于多服务器多网关环境下的身份认证方案等方面做进一步研究。

参考文献

[1] Nikooghadam, M., Haleh, A., Hafizulislam, S.K. and Moghadam, M.F. (2020) A Provably Secure and Lightweight Authentication Scheme for Internet of Drones for Smart City Surveillance. *Journal of Systems Architecture*, **115**, Article No. 101955. https://doi.org/10.1016/j.sysarc.2020.101955

[2] 李超. 基于无人机的安防监控系统在智慧城市中的应用前景与实现[J]. 科技广场, 2014(6): 72-75.

[3] Cuffari, B. (2018) Using Sensors in Drones. https://www.azosensors.com/article.aspx?ArticleID=1149

[4] Sharma, V., Song, F., You, I. and Atiquzzaman, M. (2017) Energy Efficient Device Discovery for Reliable Communi-

cation in 5G-Based IoT and BSNS Using Unmanned Aerial Vehicles. *Journal of Network and Computer Applications*, **97**, 79-95. https://doi.org/10.1016/j.jnca.2017.08.013

[5] Chen, Y.-J. and Wang, L.-C. (2018) Privacy Protection for Internet of Drones: A Network Coding Approach. *IEEE Internet of Things Journal*, **6**, 1719-1730. https://doi.org/10.1109/JIOT.2018.2875065

[6] Aggarwal, S. and Kumar, N. (2020) Path Planning Techniques for Unmanned Aerial Vehicles: A Review, Solutions, and Challenges. *Computer Communications*, **149**, 270-299. https://doi.org/10.1016/j.comcom.2019.10.014

[7] Lamport, L. (1981) Password Authentication with Insecure Communication. *Communications of the ACM*, **24**, 770-772. https://doi.org/10.1145/358790.358797

[8] Seo, S.-H., Won, J., Bertino, E., Kang, Y. and Choi, D. (2016) A Security Framework for a Drone Delivery Service. *Proceedings of the* 2*nd Workshop on Micro Aerial Vehicle Networks*, *Systems, and Applications for Civilian Use*, Singapore, 26 June 2016, 29-34. https://doi.org/10.1145/2935620.2935629

[9] Won, J., Seo, S.H. and Bertino, E. (2017) Certificateless Cryptographic Protocols for Efficient Drone-Based Smart City Applications. *IEEE Access*, **5**, 3721-3749. https://doi.org/10.1109/ACCESS.2017.2684128

[10] Cheon, J.H., Han, K., Hong, S.-M., Kim, H.J., Kim, J., Kim, S., Seo, H., Shim, H. and Song, Y. (2018) Toward a Secure Drone System: Flying with Real-Time Homomorphic Authenticated Encryption. *IEEE Access*, **6**, 24325-24339. https://doi.org/10.1109/ACCESS.2018.2819189

[11] Srinivas, J., Das, A.K., Kumar, N., Rodrigues, J.J. (2019) TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment. *IEEE Transactions on Vehicular Technology*, **68**, 6903-6916. https://doi.org/10.1109/TVT.2019.2911672

[12] Ali, Z., Chaudhry, S.A., Ramzan, M.S. and Al-Turjman, F. (2020) Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles. *IEEE Access*, **8**, 43711-43724. https://doi.org/10.1109/ACCESS.2020.2977817

[13] Li, T., Ma, J., Feng, P., Meng, Y., Ma, X., Zhang, J., *et al.* (2019) Lightweight Security Authentication Mechanism towards UAV Networks. 2019 *International Conference on Networking and Network Applications* (*NaNA*), Daegu, 10-13 October 2019, 379-384. https://doi.org/10.1109/NaNA.2019.00072

[14] Bera, B., Chattaraj, D. and Das, A.K. (2020) Designing Secure Blockchain-Based Access Control Scheme in IoT-Enabled Internet of Drones Deployment. *Computer Communications*, **153**, 229-249. https://doi.org/10.1016/j.comcom.2020.02.011

[15] Ever, Y.K. (2020) A Secure Authentication Scheme Framework for Mobile-Sinks Used in the Internet of Drones Applications. *Computer Communications*, **155**, 143-149.

[16] Zhang, Y., He, D., Li, L. and Chen, B. (2020) A Lightweight Authentication and Key Agreement Scheme for Internet of Drones. *Computer Communications*, **154**, 455-464. https://doi.org/10.1016/j.comcom.2020.02.067

[17] Haq, I., Wang, J., Zhu, Y. and Maqbool, S. (2020) An Efficient Hash-Based Authenticated Key Agreement Scheme for Multi-Server Architecture Resilient to Key Compromise Impersonation. *Digital Communications and Networks*, **7**, 140-150. https://doi.org/10.1016/j.dcan.2020.05.001

[18] Dhillon, P.K. and Kalra, S. (2017) Secure Multi-Factor Remote User Authentication Scheme for Internet of Things Environments. *International Journal of Communication Systems*, **30**, Article No. e3323. https://doi.org/10.1002/dac.3323

[19] Wazid, M., Das, A.K., Kumar, N., Vasilakos, A.V., Rodrigues, J.J.P.C. (2019) 550 Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment. *IEEE Internet of Things Journal*, **6**, 3572-3584. https://doi.org/10.1109/JIOT.2018.2888821