文献引用格式： 李良 , 杨竞 , 陶建军 , 等 . 中继式无人机自组网安全协议研究 [J]. 通信技术 ,2022,55(1):58-62. doi:10.3969/j.issn.1002-0802.2022.01.009

中继式无人机自组网安全协议研究 *

李 良[1]，杨 竞[2]，陶建军[2]，王小骥[2]，刘星江[2]

（1. 海军参谋部，北京 100841；2. 中国电子科技集团公司第三十研究所，四川 成都 611041）

摘 要： 为了提高无人机集群战术通信链路传输的连贯和安全，针对当今无人机自组链路网络的不足，提出了一种中继式无人机自组网安全协议。该协议将无人机集群划分为普通节点和中继节点，中继节点担任空间网络环境信息采集和分析的作用，并作为无人机集群协同化中心通过获得的信息为整个集群规划路径，此时新加入的无人机节点不会影响整个战术通信链路，保证了整个自组链路网络的安全可靠。

关键词： 无人机集群；自组网；安全协议；形式化分析

中图分类号： TP391.9 **文献标识码：** A **文章编号：** 1002-0802(2022)01-0058-05

Research on Security Protocol of Relay UAV Ad Hoc Network

LI Liang[1], YANG Jing[2], TAO Jianjun[2], WANG Xiaoji[2], LIU Xingjiang[2]

(1.Naval Staff, Beijing 100841, China;2.No.30 Institute of CETC, Chengdu Sichuan 611041, China)

Abstract: In order to improve the coherence and security of UAV cluster tactical communication link transmission, aiming at the deficiency of current UAC ad hoc link network, a relay UAV ad hoc network security protocol is proposed. Firstly, the protocol divides the UAV cluster into ordinary nodes and relay nodes, and the relay nodes play the role of collecting and analyzing the environmental information of the space network. Then, as the coordination center of the UAV cluster, relay nodes plan a path for the entire cluster through obtained information. At this time, the newly added UAV node will not affect the entire tactical communication link, which ensures the security and reliability of the entire ad hoc link network.

Keywords: UAV cluster; ad hoc network; security protocol; formal method

0 引 言

无人化作战力量是指参加无人化作战行动的武装力量的总成。随着现代军事信息化、智能化、集成化的进程不断推进，无人化作战系统愈发受到各军事强国的重视。与有人化作战系统相比，无人化作战系统在作战能力、作战智能、作战方式等方面拥有“非对称”的制胜优势。

信息化战争是体系和体系的对抗[1]，在现代战争中战场的信息化、智能化的占比不断增加，领域不断深入，空间不断拓展，传统的作战思维和观念已经需要进行改变，因此需要持续保持对未来战场中新技术使用的研究。作为海空地一体化作战中关键的枢纽和重要补充，无人化作战体系的深入挖掘是必要的。相比于传统的有人化作战体系，无人化作战体系具有作战持久性、成本低廉性和空间拓宽性等特点，善于使用无人化作战体系的一方在未来战场上将具有压倒性的优势。

无人机（Unmanned Aerial Vehicle，UAV）是一

* **收稿日期：** 2021-09-10; **修回日期：** 2021-12-08 Received date:2021-09-10;Revised date:2021-12-08

种由无线控制设备或由预先设计并挂载到机体内部的程序控制的无人驾驶飞行器[2]。无人机通过远程控制进行操作，故不用放置驾驶设备在机体上，因此可以在有限的空间中尽可能多地安装作战设备。但由于其需要通过无线传输指令，所以需要地面或者空中控制单位持续保持通信，这就产生了通信距离的问题。目前通常使用通信中继的技术来解决无人机控制单位通信距离的问题，具体分为使用卫星网络作为中继，使用 4G 和 5G 网络作为中继和使用地面基站 3 个方向。但是战场环境变幻莫测，长距离跨域通信、敌方的通信干扰、复杂的自然环境等都会导致通信不畅，影响实际作战效果。基于此本文提出采用无人机组网的方式，将中间的无人机作为中继基站，以此延长无人机的任务巡航范围。无人机在近些年来的多次军事对抗中发挥作用出众，已经成为一个重要的无人作战平台[3]。相比于有人机，无人机有着体积小、价格低、部署灵活、不造成人员伤亡等优点。在军事应用领域，无人机在战场侦察、火力打击、人机协同、信息对抗、集群作战等方面发挥着日益重要的作用。

1　中继式无人机研究现状

在移动通信使用愈发频繁的当下，越来越多的应用使用地面移动网络进行通信，这使得地面移动网络变得非常容易阻塞，从而影响服务用户的质量。为了解决这一问题，中继技术被提出并被广泛使用。中继起着引流的作用，可以将高负载的流量引到相对空闲的基站中，从而提高整个通信网络的效率。

在无人机应用领域中，中继式通信是一个重要的研究方向。在传统的固定中继通信中，存在着中继构建慢、部署不方便等问题，而使用中继式无人机进行通信则可解决上述问题，所以近些年很多专家学者对中继式无人机进行了大量的研究[4-6]。使用中继式无人机技术可以将无人机看作一个空中通信平台，能够将搜集到的空间网络信息进行处理和分流。此外，由于无人机具有部署快、移动范围广、投入场景快等特点，因此无人机中继通信具有很大的优势。图 1 就是一个无人机中继通信网络架构图。

目前，关于中继式无人机的研究主要集中在中继式无人机信道模型建立研究，中继式无人机通信性能优化研究，中继式无人机安全认证协议研究 3 个方面。其中，中继式无人机安全认证协议研究是提高整个无人机链路网络安全的重要技术手段，保障了无人机集群间的安全通信。文献 [7] 在考虑路径损耗等实际参数的前提下建立了多个 UAV 中继协作传输系统模型，并给出了仿真结果。文献 [8] 提出了中继式无人机信道主动窃听技术，从攻击的角度对中继式无人机安全协议提出了挑战。文献 [9] 将中继式无人机部署问题形式化表示为全跳最优路径（All Hop Optimal Path，AHOP）问题，通过改进的 BF（Improved Bellman-Ford，IBF）算法给出了无人机通信中继链路构建问题的解决方案，并通过仿真试验和试验分析，证明了 IBF 算法的有效性。

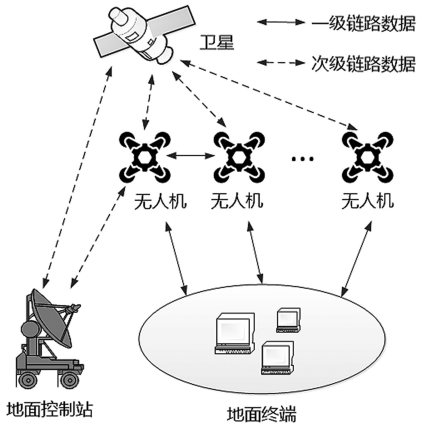

图 1　无人机中继通信网络架构

2　中继式无人机安全协议研究

在使用无人机作为中继时，无人机的中继节点与普通节点之间存在着互相认证的问题，如果有非法的无人机进入无人机集群中冒充中继节点发送伪造的信息，则会使整个无人机集群面临瘫痪的风险。为了防止这种情况发生，必须有一种可靠的中继节点与普通节点之间的双向认证协议。

2.1　中继节点网络结构

中继式无人机集群结构无须维护复杂的路由信息，可以对系统的变化做出快速反应。中继式无人机通信网络适用于节点数目多、节点移动性大的场景，与平面结构相比，节点数目越多，中继式结构的优势越明显。

因此，中继式无人机集群的网络拓扑结构符合集群无人机对组网的要求。中继式无人机集群网络中的节点有 4 类，即中继节点、普通节点、网关节点以及外部节点。中继式无人机集群拓扑结构如图 2 所示。

2.2　符号约定及角色描述

首先给出本文的符号约定如表 1 所示。

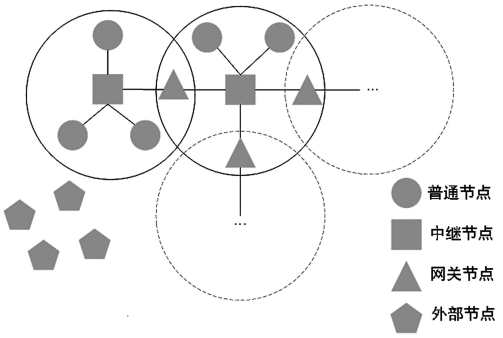

图 2 中继式无人机集群网络拓扑结构

表 1 本文符号约定

含义	符号
随机数	R
证书	$Cert$
中继节点	$Head$
普通节点	P
外部节点	OP
主公钥	PK^M
辅公钥	PK^S
会话密钥	K

其次定义中继式无人机集群网络系统的五元组 $\prod=(G_i,E_p,S_p,Sign,Verf)$，具体定义如下文所述。

（1）节点建立密钥的过程为 G_i。具体为普通节点配对主公钥 PK_P^M 和私钥 SK_P，设系统安全参数集为 K，节点 P 执行算法计算得到主公钥 PK_P^M 和私钥 SK_P，并配对为 (PK_P^M,SK_P)。

（2）中继式无人机集群网络中普通节点通过中继节点 $Head$ 获得辅公钥的过程为 E_P。具体为在系统安全参数集为 K、上级认证中心给出的私钥为 SK_P、中继节点的主公钥为 PK_{Head}^M 和节点的身份参数为 ID_P 的情况下，输出节点 P 的辅公钥 PK_P^S 的过程。

（3）配对普通节点 P 的主公钥 PK_P^M 和辅公钥 PK_P^S 的过程定义为 S_P。具体过程是，在输入为系统安全参数集 K、中继节点的私钥 SK_{Head}、节点 P 的主公钥 PK_P^M、辅公钥 PK_P^S 和节点 P 的身份参数 ID_P 的情况下，得到节点 P 的主、辅公钥对 (PK_P^M,PK_P^S)。

（4）签名算法定义为 $Sign$。签名算法具体是在系统安全参数集为 K、签名者的私钥为 SK 的情况下，签名者对输入为一个信息 m 进行签名的过程，其中签名者使用的签名算法为 $Sign$，用数学语言表达过程是 $s=Sign_{SK}(m)$。

（5）验证算法 $Verf$。输入为签名信息对 (m,s)、系统安全参数集 K 和签名公钥 PK，通过权威验证方执行验证算法 $Verf$ 输出 true 或 false 的过程称为验证过程。

2.3 中继式无人机双向认证协议

中继式无人机集群网络中中继节点和普通节点双向协议认证的过程如图 3 所示。

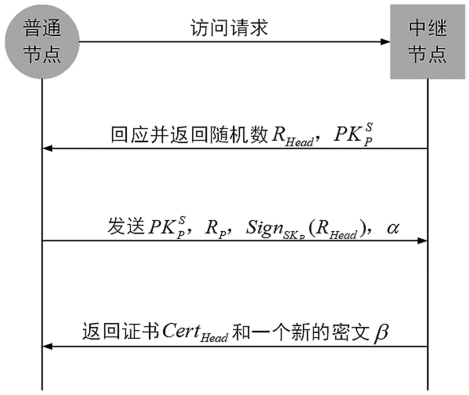

图 3 中继式无人机集群网络双向认证过程

如果普通节点想要与中继节点进行访问认证，则具体协议流程如下文所述。

（1）中继节点在收到普通节点的访问请求之后，执行 $Head \rightarrow P:R_{Head}$，$PK_P^S$，其中 R_{Head} 是中继节点为了这次交互所生成的随机数。

（2）普通节点 P 在收到中继节点的返回之后，使用 SK_P 对 R_{Head} 执行签名算法，并将辅公钥 PK_P^S 和一个新产生的随机数 R_P 及签名后的数据再使用 PK_{Head} 加密，具体计算方式为：

$$\alpha = E_{PK_{Head}}\left[h(PK_P^S \left| R_P \right| Sign_{SK_P}(R_{Head}))\right] \quad (1)$$

并随后返回 $\alpha=E_{PK_{Head}}[h(PK_P^S|R_P|Sign_{SK_P}(R_{Head}))]$。

（3）中继节点利用私钥解密 α，验证传输过程中数据的完整性，具体表达式为：

$$PK_P^S = Sign_{SK_{Head}}(IDP \left| PK_P^M \right.) \quad (2)$$

中继节点通过公钥验证 PK_P^S，得到 $(IDP|PK_P^M)$，便可判断出节点 P 的身份真假，然后使用 PK_P^M 验签 $Sign_{SK_P}(R_{Head})$ 来得到 R_{Head}，根据结果判断普通节点 P 是否据有 PK_P^M 所相应的私钥。这就是中继节点对节点 P 的认证过程，如果节点 P 是合法节点，那么它也可以通过式（3）来判断中继节点的身份：

$$\beta = E_{PK_P^M}\left[h(Cert_{Head} \left| Sign_{SK_{Head}}(R_P)\right.)\right] \quad (3)$$

返回 $Head \rightarrow P:\{Cert_{Head},Sign_{SK_{Head}}(R_P),\beta\}$，其中 $Cert_{Head}$ 是由上一级认证中心为其签署的证书，也是中继式无人机集群网络中唯一的证书。

（4）普通节点 P 先对 β 执行解密操作，得到 $h(Cert_{Head}|Sign_{SK_{Head}}(R_P))$，对比可以验证其完整性，再使用 $Cert_{Head}$ 验证 $Sign_{SK_{Head}}(R_P)R_P$ 是否为真，来判断

中继节点是否是可信的。

（5）中继节点验证普通节点完成，同时普通节点也完成对中继节点的验证，双方互相验证完成之后，中继节点为普通节点签发辅公钥。

2.4　中继式无人机会话密钥协商协议

中继节点与普通节点构成的无人机集群作战时会遇到普通节点被击毁、能量耗尽等情况，此时需要外部节点进行补充。但是由于在中继式无人机集群网络的拓扑结构中，中继节点已经承担了大量的计算指挥通信作用，因此为了减少中继节点的额外损耗，需要外部节点拥有与普通节点直接通信联系完成作战任务的能力。

外部节点若需要与普通节点之间进行联系，首先要互相认证，协议流程如图 4 所示。

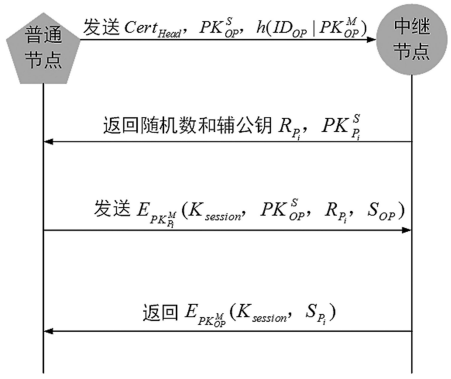

图 4　外部节点与普通节点双向认证协议流程

外部节点与普通节点双向认证协议的具体流程如下文所述。

（1）外部节点 OP 通过对普通节点发送证书和辅公钥 PK^S_{OP}:$OP \rightarrow P$:$\{Cert_{Head}, PK^S_{OP}, h(ID_{OP}|PK^M_{OP})\}$，表明其身份的合法性。

（2）普通节点在收到请求后首先验证证书的合法性。首先用中继节点的公钥 PK_{Head} 来解密外部节点的辅公钥 $PK^S_{OP}(PK^S_{OP}=Sign_{SK_{Head}}(ID_{OP}|PK^M_{OP}))$，确认外部节点是否是合法用户及其主公钥信息，用相同的哈希函数计算 $h'(ID_{OP}|PK^M_{OP})$，并比较哈希值，如果请求方身份合法，那么产生一个随机数 R_{P_i} 和辅公钥一并发送回外部节点：$P_i \rightarrow OP$:$\{R_{P_i}, PK^S_{P_i}\}$。

（3）外部节点收到请求的回应 $P_i \rightarrow OP$:$\{R_{P_i}, PK^S_{P_i}\}$，通过计算 $PK^S_{P_i}=Sign_{SK_{Head}}(ID_{P_i}|PK^M_{P_i})$ 得到普通节点的主公钥。生成 $K_{session}$ 作为会话密钥，并执行：

$$S_{OP}=Sign_{SK_{OP}}[h(K_{session}|PK^S_{OP}|R_{P_i})] \tag{4}$$

进行 $OP \rightarrow P_i : a = E_{PK^M_{P_i}}(K_{session}, PK^S_{OP}, R_{P_i}, S_{OP})$，其中 a 是 P_i 的主公钥 $K_{session}$、PK^S_{OP}、R_{P_i}、S_{OP} 进行加密的结果。

（4）普通节点 P_i 收到外部节点返回的 a，使用私钥对 a 进行计算得到 $(K_{session}, PK^S_{OP}, R_{P_i}, S_{OP})$，并比较 R_{P_i} 和 R'_{P_i}，如果 $R_{P_i}=R'_{P_i}$，那么对辅公钥 PK^S_{OP} 获得外部节点的主公钥 PK^M_{OP} 进行计算：

$$S_{OP}=Sign_{SK_{OP}}[h(K_{session}|PK^S_{OP}|R_{P_i})] \tag{5}$$

得到 $h(K_{session}|PK^S_{OP}|R_{P_i})$ 再与自己的哈希值进行比对，若相同，就把 $K_{session}$ 作为会话密钥；并计算 $S_{P_i}=Sign_{SK_{P_i}}[h(K_{session})]$。使用外部节点的主公钥加密，同时计算：

$$P_i \rightarrow OP : b = E_{PK^M_{OP}}(K_{session}, S_{P_i}) \tag{6}$$

（5）外部节点在获得 b 后，利用私钥 SK_{OP} 解密得到 $K_{session}$ 和 S_{P_i}，比较 $K_{session}$ 与 $K'_{session}$ 是否一致，若一致就表明普通节点得到了外部节点的认可；外部节点在（2）得到了普通节点的主公钥，再判断 S_{P_i} 与 $Sign_{SK_{P_i}}[h(K_{session})]$ 的结果，如果相同，则外部节点也认可 $K_{session}$ 是其与普通节点的会话密钥。

通过步骤（1）~（5），外部节点与普通节点在不经过中继节点的情况下完成双方的认证，并得到会话密钥 $K_{session}$。

2.5　BAN 逻辑分析证明双向认证协议的安全性

BAN 逻辑是一种基于信念的模态逻辑 [10]。使用 BAN 逻辑进行推理对协议进行形式化分析，协议参与者的信息随着消息的交换而发展。在应用 BAN 逻辑时，第一步需要进行“理想化步骤”，即将协议的消息转换为 BAN 逻辑中的公式；第二步则根据具体情况做出合理的假设，并根据理想化的协议和假设使用逻辑推理规则进行推理，从而推断协议是否达到预期目标。

证明本文协议是安全的，最重要的是证明签名是合法的，那么由 BAN 逻辑可以认为主辅公钥都是真的、可信的。外部节点与普通节点之间的协议根据逻辑规则推理流程如下文所述。

（1）针对协议中第一步 $OP \rightarrow P$:$\{Cert_{Head}, PK^S_{OP}, h(ID_{OP}|PK^M_{OP})\}$，推理如下：

$$\frac{P|\equiv|\xrightarrow{Cert_{Head}} Head, P \lhd PK^S_{OP} \quad P|\equiv Head|\sim(PK^S_{OP}), P|\equiv\#PK^S_{OP}}{SN|\equiv Head|\equiv PK^S_{OP}}$$

根据初始假设，P 相信 $Cert_{Head}$ 是 $Head$ 的证书，且 P 看到 PK^S_{OP}，根据 BAN 逻辑规则可得 $SN|\equiv Head|\equiv PK^S_{OP}$。

再根据初始假设 $P|\equiv PK^S_{OP}$，由 BAN 逻辑规则得到 $P|\equiv Head|\equiv PK^S_{OP}$，由此可得 P 相信 $Head$ 相信 PK^S_{OP}。所以等同于 P 相信外部节点 OP 的身份参数

ID_{OP} 和外部节点的主公钥 PK^S_{OP}。

（2）根据协议中第二步中 $P_i \rightarrow OP:\{R_{P_i},PK^S_{P_i}\}$，推理如下：

$$\frac{OP|\equiv|\xrightarrow{Cert_{Head}}Head,OP \lhd PK^S_{P_i}}{\dfrac{OP|\equiv Head|\sim PK^S_{P_i},OP \lhd PK^S_{P_i}}{OP|\equiv Head|\equiv PK^S_{P_i}}}$$

根据初始假设，OP 相信 $Cert_{Head}$ 是 $Head$ 的证书，且 OP 看到 $PK^S_{P_i}$，根据 BAN 逻辑规则可得 $OP|\equiv Head|\sim PK^S_{P_i}$。$OP|\equiv \#PK^S_{OP}$ 是初始假设，且 R_{P_i} 是随机数，则可得 $P_i|\equiv Head|\equiv PK^S_{OP}$，故上述 BAN 逻辑推理中 OP 相信 $Head$ 相信 $PK^S_{P_i}$，等同于 OP 相信 P_i 的身份 ID_{P_i} 及其主公钥 $PK^M_{P_i}$。

（3）根据协议中第三步 $OP \rightarrow P_i:a=E_{PK^M_{P_i}}(K_{session},PK^S_{OP},R_{P_i},S_{OP})$，推理如下：

$$\frac{\dfrac{\dfrac{\dfrac{\dfrac{P_i|\equiv Head|\equiv PK^M_{OP},P_i|\equiv Head \Rightarrow PK^M_{OP}}{P_i|\equiv\xrightarrow{PK^M_{OP}}OP,P_i \lhd E_{PK^M_{P_i}}(K_{session},PK^S_{OP},R_{P_i},R_{OP})}}{P_i|\equiv OP|\sim E_{PK^M_{P_i}}[K_{session},R_{P_i}],SN|\equiv \#R_{P_i}}}{P_i|\equiv OP|\equiv E_{PK^M_{P_i}}[K_{session},R_{OP}]}}{P_i|\equiv E_{PK^M_{P_i}}[K_{session},R_{OP}],P_i|\equiv|\xrightarrow{PK^M_{P_i}}P_i}}{\dfrac{P_i|\equiv[K_{session},R_{P_i}]}{P_i|\equiv K_{session}}}$$

（4）根据协议中第四步 $P_i \rightarrow OP:b=E_{PK^M_{OP}}(K_{session},S_{P_i})$，推理如下：

$$\frac{\dfrac{\dfrac{\dfrac{OP|\equiv Head|\equiv PK^M_{P_i},OP|\equiv Head \Rightarrow PK^M_{P_i}}{OP|\equiv\xrightarrow{PK^M_{P_i}}P_i,OP \lhd E_{PK^M_{OP}}(K_{session},S_{P_i})}}{OP|\equiv P_i\sim|E_{PK^M_{OP}}[K_{session},S_{P_i}],P_i|\equiv \#S_{P_i}}}{OP|\equiv P_i|\equiv E_{PK^M_{OP}}[K_{session},S_{P_i}],P_i|\equiv K_{session}}}{OP|\equiv P_i|\equiv K_{session}}$$

通过上述 4 步证明过程，可见外部节点与普通节点的协议是安全的。外部节点可以在无人机集群作战需要补充战力时立即加入，并且与普通节点直接通信，不需要通过中继节点，以免增加无人机集群大脑的通信与计算负担。

3 结 语

中继式无人机集群内中继节点与普通节点安全认证是无人机系统可以料敌于先、协同作战的关键与核心，是当今世界军事保密通信的重点研究方向。本文针对无人机自组网安全，在基于中继式无人机集群网络的环境下对无人机协同作战与新节点安全加入进行了研究，并在不影响无人机集群中的大脑——中继节点无人机的条件下设计了外部节点与普通节点之间的双向认证协议，同时给出了协议的形式化分析。

未来的工作中将研究外部节点加入不同个网关下的模型设计，保证在复杂战场环境下，无人机集群作战的机组补充，提高无人机集群的健壮性。

参考文献：

[1] 许炎 . 信息化战争应有怎样的作战观 [N]. 解放军报 ,2019-09-24(007).

[2] 樊锐 , 张鑫龙 , 马磊 , 等 . 有人 / 无人机协同作战研究 [J]. 中国电子科学研究院学报 ,2020,15(3):230-236.

[3] 袁全盛 , 胡永江 , 王长龙 . 无人机中继通信的关键技术与发展趋势 [J]. 飞航导弹 ,2015(10):26-29.

[4] 刘红军.. 美军无人机通信中继发展现状与趋势 [J]. 飞航导弹 ,2017(2):35-40.

[5] 孙翔 . 战场无人机中继通信系统关键技术研究 [J]. 信息系统工程 ,2015(7):122-123.

[6] 王志广 , 张春元 , 康东轩 . 中继式无人机自组网方案设计 [J]. 兵器装备工程学报 ,2017,38(12):233-235.

[7] 淡振雷 , 吴雪雯 , 欧阳键 , 等 . 基于门限判断 DF 协议的多无人机中继传输中断性能分析 [J]. 电信科学 ,2020,36(8):103-111.

[8] 陆海全 , 王保云 . 无人机辅助可疑中继系统下的主动窃听 [J]. 南京邮电大学学报 (自然科学版),2019,39(2):35-40.

[9] 方斌 , 陈特放 . 基于 IBF 算法的无人机中继链路部署问题研究 [J]. 控制工程 ,2015,22(1):32-37.

[10] 冯登国 , 范红 . 安全协议形式化分析理论与方法研究综述 [J]. 中国科学院研究生院学报 ,2003,20(4):389-406.

作者简介：

李 良（1985—），男，学士，工程师，主要研究方向为安全保密系统建设；

杨 竞（1986—），男，博士，工程师，主要研究方向为网络空间安全、密码学；

陶建军（1977—），男，硕士，高级工程师，主要研究方向为信息安全与保密；

王小骥（1979—），男，学士，高级工程师，主要研究方向为信息安全与通信保密；

刘星江（1984—），男，硕士，高级工程师，主要研究方向为信息安全与通信保密。