**3.2 核心防御方案：基于预共享密钥的认证机制**

研究表明，传统DH协议由于缺乏身份验证机制，使得攻击者能够轻易伪造公钥并进行中间人拦截[1]。为有效应对Diffie-Hellman密钥交换协议面临的中间人攻击威胁，同时确保方案具备良好的工程可实现性与演示效果，本研究采用基于预共享密钥的认证机制作为核心防御方案。该方案在完整保留D-H协议密钥协商功能的前提下，通过引入轻量级身份验证机制，从根本上解决了通信双方身份确认的问题。

**3.2.1 技术原理**

在技术实现层面，该防御机制的核心是在标准D-H密钥交换过程中集成消息认证功能。通信双方在进行密钥交换前，需通过安全渠道预先共享一个认证密钥。该密钥独立于密钥协商过程，专门用于对交换的公钥数据进行认证。具体实现中，发送方在传输D-H公钥时，会使用预共享密钥通过HMAC算法生成对应的消息认证码。接收方在获取数据后，采用相同的密钥和算法对公钥进行验证。若认证码验证失败，则表明通信链路中可能存在恶意攻击者试图篡改或伪造公钥，此时接收方将立即终止会话建立过程。

**3.2.2 实现流程**

该防御机制的实施涵盖以下关键步骤：

1. **初始化阶段**：通信双方（例如Alice与Bob）在通信建立前，通过安全的带外通道共同约定一个预共享密钥。该密钥通常为一个具有一定复杂度的字符串。
2. **密钥交换与认证阶段**：

Alice生成其D-H公钥 A，并计算认证码 HMAC(PSK, A)，其中PSK为预共享密钥。随后，将公钥与认证码的组合 (A, HMAC(PSK, A)) 发送至Bob。

Bob接收到数据后，使用本地存储的PSK对收到的公钥 A' 重新计算HMAC值。若计算结果与接收到的认证码一致，则认定公钥真实有效，源自Alice；反之，则判定信道中存在中间人攻击，立即终止会话。

Bob采用相同机制向Alice发送其D-H公钥 B 及对应认证码，Alice执行类似的验证操作。这种双向认证机制与近年来提出的改进Diffie-Hellman方案中的身份验证思路相吻合[2]。

1. **安全会话建立**：仅在双方均成功通过上述PSK认证后，才会利用D-H协议协商出的共享密钥建立后续的安全通信信道。任何一方的认证失败都会导致连接中断，从而确保未经验证的实体无法参与密钥协商。

**3.2.3 方案优势分析**

从实际应用角度看，该防御方案具有多方面优势。实现层面仅需在现有协议栈中集成HMAC计算模块，无需部署复杂的公钥基础设施，大幅降低了工程实现复杂度。演示效果方面，认证结果的二元特性使得攻击检测过程直观可见，极适合用于教学展示环境。系统架构上，方案完全自包含，不依赖外部认证服务，特别适合临时性或封闭性通信场景。这种自包含特性在某些无线通信场景中已被证明具有实用价值[3]。安全性方面，在预共享密钥妥善保管的前提下，该方案能够有效识别并阻断各类身份伪造攻击，为密钥交换过程提供了可靠的身份认证保障。

1. Khader, A.S. and Lai, D., 2015, April. Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol. In *2015 22nd international conference on telecommunications (ICT)* (pp. 204-208). IEEE.
2. Galu, T.S., Adeyelu, A.A. & Otor, S.U. (2024) 'An Improved Deffie Hellman Scheme for Mitigating an Eavesdropping Attack on a Network'. *International Journal of Innovative Science and Research Technology (IJISRT)*, 9(4), pp. 3101-3108. Available at: <https://doi.org/10.38124/ijisrt/IJISRT24APR2479>
3. Shen, W., Cheng, Y., Yin, B., Du, J. and Cao, X., 2021. Diffie-Hellman in the air: A link layer approach for in-band wireless pairing. *IEEE Transactions on Vehicular Technology*, *70*(11), pp.11894-11907.