基于密钥协商的防范 DHCP 中间人攻击方案

姚志强[1,2]，竺智荣[1,2]，叶惘华[1,2]

（1. 福建师范大学计算机与网络空间安全学院，福建 福州 350108；
2. 福建省公共服务大数据挖掘与应用工程技术研究中心，福建 福州 350108）

摘 要：为应对动态主机设置协议在使用过程中遇到的中间人攻击问题，提出一种轻量的解决方案。引入公钥密码技术，设计新的密钥协商算法并产生相关密钥，以减轻密钥存储负担；基于该算法提出安全方案，通过参与方的双向认证防范攻击行为，构造符合协议规范的数字签名确保消息来源。安全分析表明，该算法可有效抵御中间人攻击以及其他常见攻击类型；实验结果表明，所提方案较同类方案具有更好的性能表现，且可同时兼容 DHCPv4 与 DHCPv6。

关键词：动态主机设置协议；中间人攻击；密钥协商；消息认证
中图分类号：TP393
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021154

Achieving resist against DHCP man-in-the-middle attack scheme based on key agreement

YAO Zhiqiang[1,2], ZHU Zhirong[1,2], YE Guohua[1,2]

1. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350108, China
2. Fujian Engineering Research Center of Public Service Big Data Mining and Application, Fuzhou 350108, China

Abstract: In order to deal with the issue of the man-in-the-middle attack in the process of using dynamic host configuration protocol, a lightweight scheme was proposed. A new key agreement algorithm was developed based on public key cryptography to generate relevant keys, reducing the key storage burden. On the basis, a secure scheme was proposed, where two-way authentication of participants was designed to prevent the man-in-the-middle attack and digital signatures conforming to protocol specifications was constructed to ensure the legitimacy of the message source. By security analysis, the proposed scheme was demonstrated to be secure and valid against the man-in-the-middle attack and other common attacks. Experimental results show that the proposed scheme has the better performance compared with the related schemes, and can be compatible with both DHCPv4 and DHCPv6.

Keywords: dynamic host configuration protocol, man-in-the-middle attack, key agreement, message authentication

1 引言

动态主机设置协议（DHCP, dynamic host configuration protocol）简化了访问网络的配置过程，方便了网络管理员对 IP 地址的管理，有效缓解了由于 IPv4 地址不足所导致的问题，但 DHCP 所受到的安全威胁也越来越严重，它在设计之初并未充分考虑安全问题。当互联网呈现高移动特性时，需由配套的安全协议来保障 DHCP 安全，其中防范中间人攻击成为 DHCP 安全保障体系中最重要的问题[1-2]。中间人攻击是指敌手隐藏在 2 个或多个受害者之间，利用欺骗、冒充等手段截取信道中的数据，破

收稿日期：2021−03−02；**修回日期**：2021−06−21
基金项目：国家自然科学基金资助项目（No.61872090, No.61972096, No.61872088）；福建省引导性科技项目计划基金资助项目（No.2019H0010）
Foundation Items: The National Natural Science Foundation of China (No.61872090, No.61972096, No.61872088), The Guiding Science and Technology Planning Project of Fujian (No.2019H0010)

坏数据的机密性、完整性和可用性[3]。如图 1 所示，当 2 个受害者开始传输公钥 M_1 和 M_2 而被敌手截获并替换成 M'_1 和 M'_2 时，敌手冒充受害者参与通信。这种类型的攻击由来已久，理论上可以发生在每一次的信息交互中，既可以独立的攻击方式造成危害，也可作为实施更高级攻击之前的准备。例如在当前快速发展的 5G 或 6G 网络时代，自动驾驶和车路协同应用场景网络部署具有广泛密集与异构融合的特点，相关设备均具有高移动性，将会在不同制式的开放网络下频繁切换配置信息，这对 DHCP 的安全性和效率都提出了更高的要求。

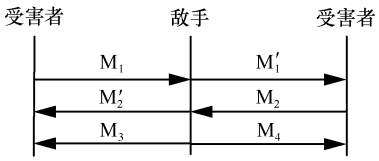


图 1 典型的中间人攻击

为此，本文研究一种轻量化的 DHCP 安全方案，防止恶意的第三方攻击，同时考虑效率和开销并兼容原有协议，做到在原有基础设施上的有效部署和运行。随着互联网协议第 6 版（IPv6, Internet protocol version 6）应用进程，所提方案可兼容 IPv6 的部分场景，实现 DHCP 第 4 版（DHCPv4）到 DHCP 第 6 版（DHCPv6）的平滑演进。所提方案分为 2 个部分：执行协议前的实体认证与密钥协商，以及协议主体中的消息认证。前者利用密码学理论进行身份认证并产生会话密钥，后者通过密钥生成相关签名以保证消息的完整性和可用性。此外，所提方案在提供目标安全的前提下考虑协议执行效率，以达到轻量化的目的。本文的主要贡献总结如下。

1) 提出一种轻量级的安全 DHCP，实体间的双向认证可以抵抗中间人攻击，数字签名可以确保消息的完整性和合法性。此外，该协议可以同时兼容 DHCPv4 与 DHCPv6 设置。

2) 分析协议安全性，经分析该协议可以有效抵御中间人攻击、参数窃取攻击，并能防止前后密钥泄露。实验结果表明，该协议相较于现有方案具有更高的执行效率。

2 相关工作

DHCP 所面临的中间人攻击通常是恶意的服务器给出错误的配置信息，使客户机所得到的服务降级，或是重定向流量为更高级的攻击做准备；也可以是恶意的客户机非法占用服务器的网络资源，使合法客户机无法进行正常的网络活动。国际互联网工程任务组在 DHCP 中加入了身份验证选项[4]，为 DHCP 身份验证提供了 2 种方法：延迟身份认证和配置令牌，但是前者容易受到拒绝服务攻击且不能用于域间认证，后者存在大量的密钥管理问题且未得到广泛使用。文献[5]提出 S-DHCP 方案来强化 DHCP 的安全性，通过综合运用椭圆曲线密码技术、单向哈希函数与数字签名技术，提供消息认证和实体认证，但该方案基于一个预共享的秘密，与延迟认证没有本质区别，同样存在密钥的管理问题，还需配合传统安全信道，影响效率与增加成本，并且在密钥协商阶段缺少服务器对发起者的身份验证以及对消息新鲜性的检测，容易遭受重放攻击及其带来的拒绝服务攻击。文献[6]提出应用椭圆加密曲线提高 DHCP 保护程度的方法，包括密钥协商算法、消息验证码和消息令牌来保证完整性、防止重放攻击。文献[7]的安全认证模型 OTP_SAM 结合当前系统时间来计算一次性密钥，利用哈希算法生成消息认证码，通过验证 Option 字段中的认证码进行安全认证；该模型具有良好的兼容性，不用修改原数据分组长度，客户机可以自主选择是否开启该模块功能，但是基于时间的会话密钥要求客户机与服务器的时钟同步，其实现条件较高。

另一类 DHCP 安全方案不采用 DHCP 验证选项。如文献[8]提出基于公钥密码学和数字证书的认证方案，使用不同的密钥长度配合不同的证书类型测试通信开销和处理时间，但客户机无法检测服务器的证书撤销状态。文献[9]提出针对耗竭攻击的检测方案，通过收集正常时段 DHCP 请求的概率分布作为标准来检测异常情况，但对异常数据敏感，易出现误报现象。文献[10]收集和标记 DHCP 欺骗产生的网络流量，为定量分析提供了数据支持，并讨论若干欺骗攻击行为引起的流量异常表现。文献[11]提出一种基于隐马尔可夫模型的恶意域名检测方案，配合 Baum-Welch 算法和 Viterbi 算法的马尔可夫模型可以快速准确分类未知域名，从而实现有效检测，然而，因训练数据的随机性和不确定性，建模过程中容易产生误差。

综上所述，现有方案普遍存在难以部署、与原始协议不兼容以及密钥管理等问题，本文方案将针对这些问题展开研究，并在满足目标安全性的前提下提升方案效率，以达到轻量化的目的。

3　威胁模型与设计目标

本节主要描述方案的威胁模型和设计目标。首先，本文方案考虑 4 种类型的安全威胁。

1) 恶意服务器攻击。敌手假冒合法的 DHCP，服务器向客户机提供虚假的网络配置，从而使客户机服务降级，无法正常享受网络服务；或借此重定向客户机流量到非法的钓鱼网站，为进一步的攻击做准备。

2) 恶意客户机攻击。敌手假冒合法的客户机向 DHCP 服务器请求配置相关参数，从而非法占用网络服务；或进一步发动耗竭攻击耗尽服务器有限的 IP 地址，使合法客户机无法享受网络服务。

3) 参数窃取攻击。敌手攻击服务器并窃取数据库中的客户端信息，例如网络标识、密码与验证参数等，最后尝试使用这些信息冒充合法客户机。

4) 前/后向安全威胁。对应到本文场景指的是，当会话密钥泄露时，敌手以此推算出上一个会话密钥或下一个会话密钥，同时获得受其保护的内容。

其次，本文方案旨在实现 3 个方面的设计目标。

1) 安全目标。方案要能抵御威胁模型中定义的攻击类型。

2) 效率目标。在达到安全目标的前提下，较同类型方案具有更高的执行效率。

3) 兼容目标。方案要与 DHCP 原始协议具有良好的兼容性，具体表现在：①满足协议基本格式要求；②不引入新的状态、消息类型和参与方；③方案部署后可选择是否启用。

4　密钥协商算法

本节主要构造一种防范DHCP攻击的密钥协商算法，包括系统初始化、客户机注册和密钥协商等过程。在此之前，介绍该算法涉及的主要符号和含义，如表 1 所示。

1) 系统初始化

① 椭圆曲线初始化。选定 2 个大素数 p 和 q，构造有限域 F_p 上的椭圆曲线 $y^2 = x^3 + ax + b$，其中 a、b 满足 $4a^3 + 27b^2 \neq 0(\mathrm{mod}\, p)$，选定阶为 q 的基点 P 构成加法循环群 G，选择单向函数 $H_i : \{0,1\}^* \times G \to Z_q^*$。

② 系统参数初始化。选择服务器 S_i 的私钥 $S_s \in Z_q^*$，计算公钥 S_p。

$$S_p = S_s P \tag{1}$$

表 1　符号说明

符号	含义
p, q	大素数
F_p	有限域
P	基点
G	循环群
H_i	哈希函数
ID_i	客户机标识
S_i	服务器标识
S_s	服务器私钥
S_p	服务器公钥
x_i, M_{U_i}	客户机部分私钥
d_i	客户机完整私钥
D_i	客户机公钥
β_{U_i},cd	认证参数
c_1, c_2, c_3	伪随机数
A_{U_i}, F_{U_i}	消息令牌
$\mathrm{sk}_A, \mathrm{sk}_B$	会话密钥

2) 客户机注册

① 客户机发出注册申请。客户机或网络管理员为客户机 U_i 选择网络标识 ID_i，客户机选择部分私钥 $x_i \in Z_q^*$，计算部分公钥 X_i 以及 β_{U_i}，并将 $\{\mathrm{ID}_i, \mathrm{MAC}, \beta_{U_i}\}$ 发送给服务器 S_i，其中 MAC 是设备的物理地址。客户机可以通过广播同时向多个服务器注册，也可以按照优先级向指定的服务器注册。

$$X_i = x_i P \tag{2}$$

$$\beta_{U_i} = H_1(\mathrm{ID}_i, X_i, \mathrm{MAC}) \tag{3}$$

② 服务器验证注册信息。服务器收到消息后先判断是否注册过，有则跳过，没有则选择随机数 $c_1 \in Z_q^*$，并计算 A_{U_i} 和 M_{U_i}，存储 $\{\mathrm{ID}_i, \mathrm{MAC}, c_1\}$，同时将 $\{S_i, M_{U_i}, A_{U_i}\}$ 发送给客户机。

$$A_{U_i} = c_1 P \tag{4}$$

$$M_{U_i} = H_2(A_{U_i}, \beta_{U_i}) S_s \bmod q + c_1 \tag{5}$$

③ 客户机对服务器进行反向验证。客户机在收到回复后首先判断 A_{U_i} 是否是新鲜的，接着验证等式 $M_{U_i} P = H_2(A_{U_i}, \beta_{U_i}) S_p \bmod q + A_{U_i}$ 是否成立，若验证失败，则重新申请；若验证成功，则结合 2 个部分私钥计算客户机的完整私钥 d_i 和公钥 D_i，存储 $\{S_i, A_{U_i}\}$ 注册成功。

客户机注册过程如图 2 所示。

$$d_i = x_i + M_{U_i} \tag{6}$$

$$D_i = d_i P \tag{7}$$

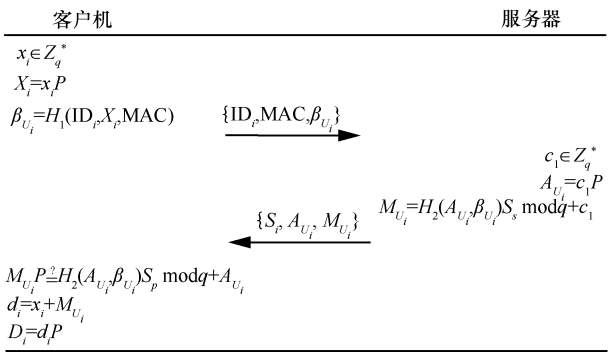


图 2 客户机注册过程

3) 密钥协商

① 客户机发起协商申请。客户机选择随机数 $c_2 \in Z_q^*$，计算参数 cd、F_{U_i} 以及 k_1，同时将 $\{\mathrm{ID}_i, \mathrm{MAC}, \mathrm{cd}, F_{U_i}\}$ 发送给服务器。

$$\mathrm{cd} = d_i + c_2 \tag{8}$$

$$F_{U_i} = c_2 P \tag{9}$$

$$k_1 = (c_2 + d_i)(S_p + A_{U_i}) \tag{10}$$

② 服务器验证客户机信息。服务器在收到客户机的协商请求后首先判断 F_{U_i} 是否是新鲜的，接着验证等式 $\mathrm{cd}P = D_i + F_{U_i}$ 是否成立，若不成立，则拒绝；若成立，则接收并计算 k_2，同时选择随机数 $c_3 \in Z_q^*$，并计算 Auth_1，存储 $\{\mathrm{ID}_i, \mathrm{MAC}, F_{U_i}\}$，然后将 $\{S_i, c_3, \mathrm{Auth}_1\}$ 发送给客户机。

$$k_2 = (S_s + c_1)(F_{U_i} + D_i) \tag{11}$$

$$\mathrm{Auth}_1 = c_3 S_s F_{U_i} \tag{12}$$

③ 客户机对服务器进行反向验证。客户机在接收到服务器发来的信息后，首先验证 $\mathrm{Auth}_1 = c_2 c_3 S_p$ 是否成立，若不成立，则重新发起申请；若成立，则计算 sk_A 以及 Auth_2，并将 $\{\mathrm{Auth}_2\}$ 发送给服务器。

$$\mathrm{sk}_A = H_3(0, \mathrm{ID}_i, S_i, k_1) \tag{13}$$

$$\mathrm{Auth}_2 = H_3(1, \mathrm{ID}_i, S_i, k_1) \tag{14}$$

④ 服务器进行最后确认。服务器验证 $\mathrm{Auth}_2 = H_3(1, \mathrm{ID}_i, S_i, k_2)$ 是否成立，若不成立，则拒绝；若成立，则计算 sk_B。协商完成，协商所产生的会话密钥为 $\mathrm{sk}_A = \mathrm{sk}_B$。

$$\mathrm{sk}_B = H_3(0, \mathrm{ID}_i, S_i, k_2) \tag{15}$$

协商过程如图 3 所示。

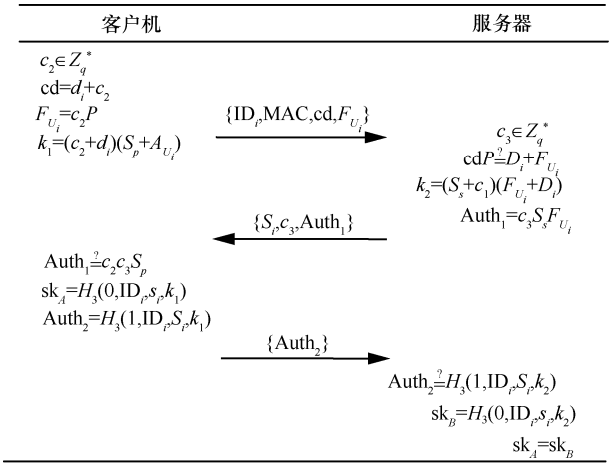


图 3 密钥协商

5 基于密钥协商的 DHCP 安全方案

为使新的方案能够匹配现行 DHCP，需遵循 RFC 3118 中定义的认证选项格式[4]，因此，在本文方案应用时将 Protocol 字段置为 6，并将 Algorithm 置为 8，同时将验证信息附加在 options180 中，采用默认 RDM（replay detection method）字段值，RD（replay detection）字段使用计数器模式来抵抗重放攻击。此外，设置签名默认长度为 256 B，满足 DHCP 长度限制[12-14]。

出于兼容 DHCPv4 与 DHCPv6 的考虑，方案应遵循 RFC 3315 中的相关定义。DHCPv6 是 DHCP 针对 IPv6 的改进，IPv6 地址分配方式大致可以分为 2 种：无状态地址自动配置和有状态地址自动配置[15]。DHCPv6 是一种有状态地址自动配置协议[16]，在配置过程中服务器分配一个完整的 IPv6 地址给主机，并提供 DNS 服务器地址等其他配置信息，将分配的地址与客户机进行绑定，从而增强了网络的可管理性。DHCPv6 协议下客户机与服务器的交互分为 4 步交互与 2 步快速交互，其报文与 DHCPv4 类似，具有对应关系[17]。

当客户机与服务器完成第 4 节的注册与密钥协商过程，生成 sk_A 与 sk_B 后便可发起 DHCP 服务，如图 4 所示，详述过程如下。

① 客户机发起 DHCP 请求。客户机发送 Discover/Solicit 报文，并在报文的相关字段中表明启用本文方案，要求服务器进行消息认证；如果客

户机启用 2 步快速分配，则还需在报文中携带 Rapid Commit 选项（仅在 DHCPv6 中）。

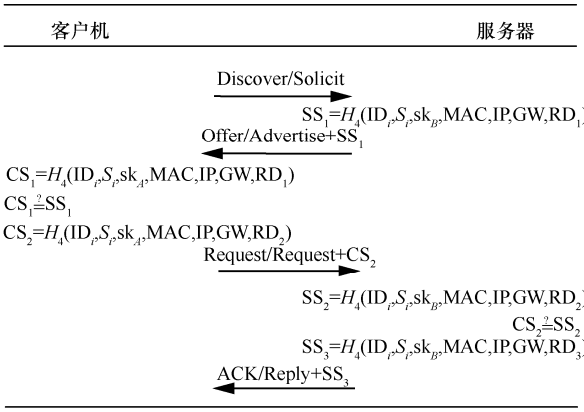


图 4　DHCPv4/DHCPv6 消息认证

② 服务器处理客户机请求。收到报文的服务器首先判断客户机选择的请求方案，如果采用本文方案，则先验证 RD 字段是否符合标准，不符合则跳过，符合则开始准备 Offer/Advertise 报文；若消息中携带有 Rapid Commit 选项，并且服务器支持快速分配过程，则跳到步骤④开始构建 Reply 报文，否则继续。Offer/Advertise 报文中包含提供给客户机的 IP 地址、租赁期以及默认网关等配置信息，同时更新 RD 字段。此外，为了认证消息，需要将服务器的签名附加在 Offer/Advertise 报文的 options180 字段中，签名为 $\mathrm{SS}_1 = H_4(\mathrm{ID}_i, S_i, \mathrm{sk}_B, \mathrm{MAC}, \mathrm{IP}, \mathrm{GW}, \mathrm{RD}_1)$，其中 MAC 是设备的物理地址，此外，还包含之前协商的会话密钥以及主要配置信息，同时加入 RD 值保证消息的新鲜性。

③ 客户机验证服务器。收到 Offer/Advertise 消息的客户机首先检测 RD 值是否严格高于旧的 RD 值，若不满足，则丢弃；若满足，则提取报文中的配置信息，并计算 $\mathrm{CS}_1 = H_4(\mathrm{ID}_i, S_i, \mathrm{sk}_A, \mathrm{MAC}, \mathrm{IP}, \mathrm{GW}, \mathrm{RD}_1)$，验证 $\mathrm{CS}_1 = \mathrm{SS}_1$ 是否成立，若不成立，则丢弃；若成立，则开始准备 Request 报文。Request 报文是客户机用来确认所要申请的具体 IP 地址以及其他网络参数，其主要内容与 Offer/Advertise 报文类似，同时更新 RD 值，并计算 $\mathrm{CS}_2 = H_4(\mathrm{ID}_i, S_i, \mathrm{sk}_A, \mathrm{MAC}, \mathrm{IP}, \mathrm{GW}, \mathrm{RD}_2)$，附加在 Request 报文中，发送给服务器。

④ 服务器验证客户机。服务器收到消息后首先验证 RD 是否符合要求，同时提取报文中的配置信息计算 $\mathrm{SS}_2 = H_4(\mathrm{ID}_i, S_i, \mathrm{sk}_B, \mathrm{MAC}, \mathrm{IP}, \mathrm{GW}, \mathrm{RD}_2)$，验证 $\mathrm{SS}_2 = \mathrm{CS}_2$ 是否成立，若不成立，则丢弃；若成立，则用相同的方法构建 ACK/Reply 报文，发送给客户机。

⑤ 客户机最后确认。客户机在接收到 ACK/Reply 报文后用相同的方法进行验证，若验证失败，则丢弃；若验证成功，则开始配置相关网络参数。

对 DHCPv6，上述过程和图 4 中 SS_1、CS_1、CS_2 和 SS_2 的计算是将 ID_i 和 S_i 分别替换为客户机设备唯一标识符 DUIDc 和服务器设备唯一标识符 DUIDs。另外，在实际应用中会有更多的状态和过程，都可以用相同的方式制作签名。

6　安全性分析

本文方案的安全性体现在 2 个方面：密钥协商过程的安全性以及 DHCP 认证过程中签名的不可伪造性，而后者的安全性依赖于前者的会话密钥安全，故本节主要对协商算法进行安全分析。

6.1　BAN 逻辑分析

BAN 逻辑是一种形式化的分析方法，普遍用来分析协议的正确性和安全性。本节将使用 BAN 逻辑对密钥协商算法进行形式化分析。现将符号表示如下：C 和 S 表示主体，K_{ij} 表示主体 i 和 j 之间共享的密钥，K_i 和 K_i^{-1} 分别表示 i 的公钥与私钥。

1) 定义安全目标

G_1：$C \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S$

G_2：$S \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S$

G_3：$C \mid\equiv S \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S$

G_4：$S \mid\equiv C \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S$

2) 定义初始状态假设

A_1：$C \mid\equiv \overset{K_S}{\mapsto} S$

A_2：$S \mid\equiv \overset{K_C}{\mapsto} C$

A_3：$C \mid\equiv \#(c_1)$

A_4：$S \mid\equiv \#(c_2)$

A_5：$C \mid\equiv S \Rightarrow A_U$

A_6：$S \mid\equiv C \Rightarrow F_U$

3) 描述理想化协议

M_1：$C \to S : \{\mathrm{ID}, \mathrm{MAC}, \beta_U\}$

M_2：$S \to C : \{A_U = c_1 P, (A_U, \beta_U)_{K_S^{-1}}\}$

M_3：C 计算会话密钥 $K_{CS} = f(A_U)$

M_4： $C \to S:\{F_U = c_2 P,(F_U)_{K_C^{-1}}\}$

M_5： S 计算会话密钥 $K_{CS} = f(F_U)$

4) 基于 BAN 逻辑的形式化证明

根据 M_2 可得

P_1： $S \mid\equiv c_1$

P_2： $S \mid\equiv \#(c_1)$

P_3： $C \lhd A_U,\{A_U,\beta_U\}_{K_S^{-1}}$

根据 P_3 和接收消息规则，可得

P_4： $C \lhd \{A_U,\beta_U\}_{K_S^{-1}}$

根据 P_4、A_1 和消息含义规则，可得

P_5： $C \mid\equiv S \sim (A_U,\beta_U)$

根据 P_5、A_3 和消息新鲜性规则，可得

P_6： $C \mid\equiv \#(A_U,\beta_U)$

根据 P_5、P_6 和临时验证规则，可得

P_7： $C \mid\equiv S\mid\equiv (A_U,\beta_U)$

根据 P_7 和信念规则，可得

P_8： $C \mid\equiv S\mid\equiv A_U$

根据 P_8、A_5 和管辖规则，可得

P_9： $C \mid\equiv A_U$

根据 M_4 可得

P_{10}： $C \mid\equiv c_2$

P_{11}： $C \mid\equiv \#(c_2)$

P_{12}： $S \lhd F_U,\{F_U\}_{K_C^{-1}}$

根据 P_{12} 和接收消息规则，可得

P_{13}： $S \lhd \{F_U\}_{K_C^{-1}}$

根据 P_{13}、A_2 和消息含义规则，可得

P_{14}： $S \mid\equiv C \sim F_U$

根据 P_{14}、A_4 和消息新鲜性规则，可得

P_{15}： $S \mid\equiv \#(F_U)$

根据 P_{14}、P_{15} 和临时验证规则，可得

P_{16}： $S \mid\equiv C\mid\equiv F_U$

根据 P_{16}、A_6 和管辖规则，可得

P_{17}： $S \mid\equiv F_U$

根据 M_3、P_{11} 和消息新鲜性规则，可得

P_{18}： $C \mid\equiv \#(K_{CS})$

根据 P_8、P_{18} 和会话密钥规则，可得

P_{19}： $C \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S$

由于协议具有对称的结构，因此 C 相信 S 一定也能得出相同的信仰，即

P_{20}： $C \mid\equiv S \mid\equiv C \xleftarrow{K_{CS}} S$

根据 M_5、P_1 和消息新鲜性规则，可得

P_{21}： $S \mid\equiv \#(K_{CS})$

根据 P_{16}、P_{21} 和会话密钥规则，可得

P_{22}： $S \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S$

P_{23}： $S \mid\equiv C \mid\equiv C \xleftarrow{K_{CS}} S$

根据以上推理，得出全部 4 个安全目标，达到本文方案预期目的。

6.2 启发式安全分析

1) 抗恶意服务器攻击

在客户机注册阶段，客户机 U_i 首先通过检查参数 A_{U_i} 的新鲜性来抵抗重放攻击；接着通过参数 M_{U_i} 来检测参数 A_{U_i} 是否被篡改，同时验证服务器的身份，敌手若想伪造 M_{U_i}，需捕获参数 A_{U_i} 和参数 β_{U_i}，通过服务器的公钥 S_p，利用 $S_p = S_s P$ 反解出私钥 S_s，为椭圆曲线上的离散对数问题；在密钥协商阶段，客户机通过参数 Auth_1 来检测参数 c_3 是否被篡改，同时验证服务器的身份，敌手若想伪造 Auth_1，需捕获参数 c_3 和参数 F_{U_i}，以同样的方法求解私钥 S_s，这在计算上是不可行的[18-19]。

2) 抗恶意客户机攻击证明

在密钥协商阶段，服务器 S_i 为首次验证客户机，通过检查参数 F_{U_i} 的新鲜性来抵抗重放攻击；接着通过参数 cd 来检测参数 F_{U_i} 是否被篡改，同时验证客户机的身份，敌手若想伪造 cd，需要捕获参数 c_2 和客户机私钥 d_i，但这 2 个参数都未在信道中传输过，只能通过 $F_{U_i} = c_2 P$ 和 $D_i = d_i P$ 进行反解，也是离散对数问题；在密钥协商阶段，服务器 S_i 第二次验证客户机是通过参数 Auth_2 来判断客户机身份，敌手若想伪造 Auth_2，需要同时捕获参数 ID_i 和参数 S_i，以计算私钥 d_i 是不可行的。

3) 抗参数窃取攻击证明

服务器中存有客户机的 ID_i 和 MAC，但缺少客户机私钥则无法完美冒充合法客户机，客户机私钥由客户机自身和服务器两部分选取产生，只窃取一部分则无法计算出完整私钥。

4) 防前/后向安全威胁证明

会话密钥中除客户机、服务器的各自私钥外，还包含客户机与服务器各自选择的随机数，而随机数的选取依赖于所使用的伪随机数算法，如果客户机与服务器采用不同的伪随机数算法，敌手想要同时破解难度很大；即使敌手以极小的概率猜测出随

机数变化的规律，想要影响前/后安全性还需要同时获得客户机与服务器的私钥，所以认为会话密钥的产生是动态变化的，即使敌手获得某一时刻的密钥也不会造成前/后向的安全威胁。

7　性能分析和比较

本文实验分析利用开放密码库 OpenSSL 测试方案的性能[20]，在 2.6 GHz 处理器和 8 GB 内存的 Windows 10 环境上运行。忽略前期的密钥协商，对比方案主体部分与原始 DHCP 的时间开销。从图 5 中可以看出，加入数字签名和验证给协议带来一定的时延。虽然本文方案在原始协议的基础上会引入一些安全开销，但与此同时也提供了可靠的安全性，数字签名与消息摘要的加入使参与方可以进行实体认证与消息认证，安全分析也表明其能有效缓解中间人攻击的威胁，并且其带来的额外开销是轻量的。

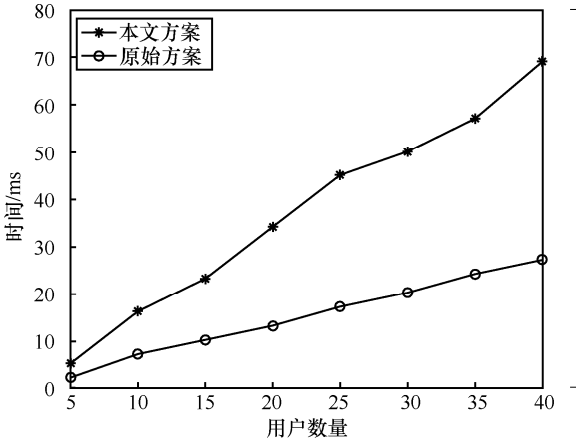


图 5　本文方案与原始方案的性能对比

本文方案与文献[5]的 CA、S-DHCP 方案和文献[2]的 DSec 方案的仿真数据如图 6 所示。从图 6 可以看出，本文方案在性能上要明显优于另外 3 种方案，且随着客户机数量的增加而越来越明显。从这些方案的安全性上看，本文方案与 S-DHCP 方案默认使用基于椭圆曲线的 256 bit 长度的密钥，CA 方案与 DSec 方案默认使用基于 RSA 的 3 072 bit 长度的密钥，两者的密钥安全性相当[21-22]，然而 CA 方案中的证书长度很容易超出 DHCP 限制，需将消息分段传输，因而增加了遭遇中间人攻击的风险；S-DHCP 方案在密钥协商阶段缺少服务器对发起者的身份验证和消息新鲜性的检测，容易遭受重放攻击及其带来的拒绝服务攻击；DSec 与 S-DHCP 方案的前提都是基于一个预共享的秘密，与延迟认证同样存在密钥的管理问题。

综上所述，本文方案能够有效缓解中间人攻击的威胁，且在性能表现上优于同类型方案，是更加轻量的安全方案。

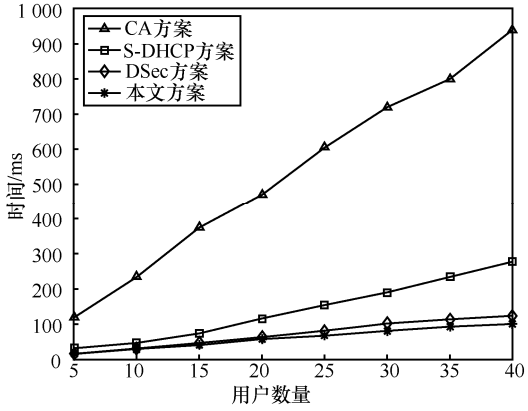


图 6　本文方案与不同方案的性能对比

8　结束语

本文针对互联网中普遍存在的中间人攻击问题，以 DHCP 为背景，提出安全快速的交互方案，旨在缓解有关网络攻击和安全威胁，即通过实体认证与密钥协商，结合数字签名与摘要进行消息认证。协商算法结构紧凑，通过双向认证防范攻击行为，有较高的执行效率；使用协商后的会话密钥构造数字签名，签名包含配置参数保持消息关联性，且容易附着在常规协议中对信息进行完整性和可靠性验证；遵循格式规范，不引入新的状态与参与方，使方案可以同时兼容 DHCPv4 与 DHCPv6；通过安全性分析本文方案防御攻击的能力，通过性能分析其执行效率的提高程度。下一步工作是研究在保证安全性的前提下如何减少参与方之间的交互次数。

参考文献：

[1] WANG H B, WANG J H, WANG J L, et al. Squeezing the gap: an empirical study on DHCP performance in a large-scale wireless network[J]. IEEE/ACM Transactions on Networking, 2020, 28(2): 832-845.

[2] AL-ANI A, ANBAR M, HASBULLAH I H, et al. Authentication and privacy approach for DHCPv6[J]. IEEE Access, 2019, 7: 73144-73156.

[3] CONTI M, DRAGONI N, LESYK V. A survey of man in the middle attacks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2027-2051.

[4] DROMS R. Authentication for DHCP messages[R]. RFC Editor, 2001.

[5] YOUNES O S. A secure DHCP protocol to mitigate LAN attacks[J]. Journal of Computer and Communications, 2016, 4(1): 39-50.

[6] YOO K J, KIM E G. Design and implementation of DHCP supporting network attack prevention[J]. Journal of the Korea Institute of Information & Communication Engineering, 2016, 20(4): 747-754.

[7] ZHANG F Q, CHEN L. OTP_SAM: DHCP security authentication model based on OTP[C]//2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design. Piscataway: IEEE Press, 2016: 346-350.

[8] DINU D D, TOGAN M. DHCP server authentication using digital certificates[C]//2014 10th International Conference on Communications. Piscataway: IEEE Press, 2014: 1-6.

[9] TRIPATHI N, HUBBALLI N. A probabilistic anomaly detection scheme to detect DHCP starvation attacks[C]//2016 IEEE International Conference on Advanced Networks and Telecommunications Systems. Piscataway: IEEE Press, 2016: 1-6.

[10] CALVERT C, KHOSHGOFTAAR T M, NAJAFABADI M M, et al. A procedure for collecting and labeling man-in-the-middle attack traffic[J]. International Journal of Reliability, Quality and Safety Engineering, 2017, 24(1): 1750002.

[11] LV P, BAI L L, LIU T W, et al. Detection of malicious domain names based on hidden Markov model[C]//2018 IEEE Third International Conference on Data Science in Cyberspace. Piscataway: IEEE Press, 2018: 659-664.

[12] AGYEMANG J O, JERRY K, ACQUAH I. Lightweight man-in-the-middle (MITM) detection and defense algorithm for Wi-Fi-enabled Internet of things (IoT) gateways[J]. Information Security and Computer Fraud, 2019, 7(1): 1-6.

[13] OLANREWAJU R F, ISLAM T, KHALIFA O O, et al. Data in transit validation for cloud computing using cloud-based algorithm detection of injected objects[J]. Indonesian Journal of Electrical Engineering and Computer Science, 2018, 10(1): 348-353.

[14] HUBBALLI N, TRIPATHI N. A closer look into DHCP starvation attack in wireless networks[J]. Computers & Security, 2017, 65(3): 387-404.

[15] LIU Z, MOHIUDDIN G, ZHENG J, et al. Privacy preserving IPv6 address DHCP configuration for Internet of things[J]. ACM Transactions on Information Systems, 2020, 6(2): 595.

[16] LI L S, REN G, LIU Y, et al. Secure DHCPv6 mechanism for DHCPv6 security and privacy protection[J]. Tsinghua Science and Technology, 2018, 23(1): 13-21.

[17] TIAN Q, LIN Y, GUO X H, et al. New security mechanisms of high-reliability IoT communication based on radio frequency fingerprint[J]. IEEE Internet of Things Journal, 2019, 6(5): 7980-7987.

[18] 张艳硕, 王泽豪, 王志强, 等. 基于特征值的可验证三方安全密钥交换协议[J]. 通信学报, 2019, 40(12): 149-154.
ZHANG Y S, WANG Z H, WANG Z Q, et al. Verifiable three-party secure key exchange protocol based on eigenvalue[J]. Journal on Communications, 2019, 40(12): 149-154.

[19] 杨亚涛, 韩新光, 黄洁润, 等. 基于 RLWE 支持身份隐私保护的双向认证密钥协商协议[J]. 通信学报, 2019, 40(11): 180-186.
YANG Y T, HAN X G, HUANG J R, et al. Bidirectional authentication key agreement protocol supporting identity's privacy preservation based on RLWE[J]. Journal on Communications, 2019, 40(11): 180-186.

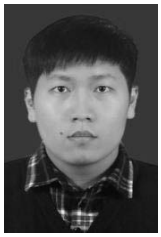
[20] CARRÉ S, DESJARDINS M, FACON A, et al. Exhaustive single bit fault analysis. A use case against Mbedtls and OpenSSL's protection on ARM and Intel CPU[J]. Microprocessors and Microsystems, 2019, 71: 1-13.

[21] LI Y, ZHU L, WANG H W, et al. A cross-layer defense scheme for edge intelligence-enabled CBTC systems against MitM attacks[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(4): 2286-2298.

[22] MALLOULI F, HELLAL A, SAEED N S, et al. A survey on cryptography: comparative study between RSA vs ECC algorithms, and RSA vs el-gamal algorithms[C]//2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud. Piscataway: IEEE Press, 2019: 173-176.

[作者简介]

姚志强（1967– ），男，福建莆田人，博士，福建师范大学教授、博士生导师，主要研究方向为大数据安全与隐私保护、多媒体安全、应用安全。



竺智荣（1993– ），男，浙江宁波人，福建师范大学硕士生，主要研究方向为大数据安全与隐私保护。

叶帼华（1976– ），女，福建霞浦人，福建师范大学副教授，主要研究方向为大数据安全与隐私保护、信息安全。