软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(Suppl.(2)):90−97
©中国科学院软件研究所版权所有.

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于标识密码的数据报传输层安全协议*

李鹏坤, 王小峰, 苏金树, 薛 天

(国防科技大学 计算机学院,湖南 长沙 410073)

通讯作者: 王小峰, E-mail: xf_wang@nudt.edu.cn

摘 要: TLS 作为目前应用最为广泛的安全传输协议,只能保证可靠传输 TCP 上数据的安全性.DTLS(datagram TLS)在 TLS 协议架构上进行了修改,能够为 UDP 提供安全保护.但 DTLS 在会话建立过程中仍然需要依赖第三方认证中心和证书完成通信双方的认证,连接建立过程时间长,安全开销大,不能满足物联网等资源受限的网络通信环境.将标识密码引入 DTLS 中,避免了握手协议中处理证书所带来的各种开销,在计算会话密钥的同时完成通信双方的认证;并使用新的密钥协商协议重新设计 DTLS 的握手协议,减少交互次数和消息数量,缩短连接建立时间.实验结果表明,基于标识密码的 DTLS 在不降低安全性的同时,将通信建立时间缩短了近 50%.

关键词: 安全协议;标识密码;网络传输协议;密钥协商;认证

中文引用格式: 李鹏坤,王小峰,苏金树,薛天.基于标识密码的数据报传输层安全协议.软件学报,2017,28(Suppl.(2)):90−97. http://www.jos.org.cn/1000-9825/17022.htm

英文引用格式: Li PK, Wang XF, Su JS, Xue T. Datagram transport layer security protocol with identity-based cryptography. Ruan Jian Xue Bao/Journal of Software, 2017,28(Suppl.(2)):90−97 (in Chinese). http://www.jos.org.cn/1000-9825/17022.htm

Datagram Transport Layer Security Protocol with Identity-Based Cryptography

LI Peng-Kun, WANG Xiao-Feng, SU Jin-Shu, XUE Tian

(School of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract: TLS is the most widely deployed security protocol, however, it can only secure the applications that are based on reliable transport. Datagram TLS (DTLS) is a modified version of the TLS protocol which provides security protection in datagram environments. In DTLS, however, the communication parties need complete authentication though the certification authority when they establish connection. Consequently, the connection establishment process takes long time with a high security overhead, which cannot meet the requirement for resource-constrained network communication environment such as Internet of Things. This paper introduces identify-based cryptography to DTLS. It provides authentication while calculating the session key, and avoids the overhead associated with handling certificates in the handshake protocol. The paper designs a new DTLS handshake protocol, which reduces the number of interactions and messages, and shortens the connection establishment time. Experimental results show that the DTLS with identity-based cryptography reduces the communication setup time by nearly 50% without compromising the security.

Key words: security protocol; identity-based cryptography; network transport protocol; key agreement; authentication

TLS 用于在两个通信应用程序之间提供保密性和数据完整性的保护,是目前网络中使用最广泛的传输层安全协议.TLS 建立在可靠的传输层协议 TCP 上,可以保证 TCP 上应用的安全,但不能保证 UDP 上应用的安全.然而,近年来出现了许多延迟敏感、实时性强的应用程序,包括实时视频会议、Internet 电话和在线游戏等,这些应用程序都使用不可靠的 UDP 传输.不断增多的应用层协议,比如 SIP(session initial protocol)[1]、RTP(real time protocol)[2]和 MGCP(media gateway control protocol)[3]等,也都是基于 UDP 传输而设计.另外,物联网的发展使得

* 基金项目: 国家重点研发计划(0802300)
Foundation item: National Key Research and Development Program of China (0802300)
收稿时间: 2017-06-30; 定稿时间: 2017-10-20

网络接入设备小型化、集成化.这些设备受限于成本和尺寸等资源,相对于通用计算机,其计算能力一般较弱.因此,与 TCP 相比,轻量级 UDP 更加适合这样的网络.另外,这些设备之间传递的消息一般较短,但往往需要安全保护和实时传输,在这种环境下,TCP 中建立和关闭连接的开销是很难接受的.

有许多工作对轻量级的传输层安全协议进行了探索.TFO(TCP fast open)[4]通过请求 TFO cookie 并在之后的连接中发送这个 cookie 来避免 TCP 的 3 次握手带来的开销.Tcpcrypt[5]和 MinimaLT[6]希望提供一种传输层的普适加密服务.Tcpcrypt 将密钥协商整合到 TCP 的 3 次握手协议中,从而获得比 TLS 更快的连接建立时间.MinimaLT 结合目录服务器和新的隧道建立方式也缩短了连接建立的延迟.但这些安全协议都更注重基于 TCP 连接的客户服务器模式的安全,不适用于基于 UDP 的应用.Google 公司提出的 QUIC(quick udp Internet connections)[7]协议虽然是在 UDP 协议的基础上建立,但本质上还是模拟 TCP 协议进行通信,仍然无法适用于 UDP 应用.另外,QUIC 协议中包含许多拥塞避免和减小延迟的机制,协议复杂度较高,无法适用于资源受限的网络.

Rescorla 等人[8]提出了可支持数据报传输安全的协议(datagram TLS,简称 DTLS).DTLS 在现存的 TLS 协议上进行了修改,使其在最小改动的基础上能够支持不可靠的数据传输.但 DTLS 更关注于如何使基于可靠传输的 TLS 能够在不可靠的传输上建立,对 TLS 密钥协商和认证的过程并没有本质的改变.和 TLS 一样,DTLS 仍然依赖第三方认证中心(certification authority,简称)和证书完成通信双方的认证,但这会带来几个问题:(1) 证书处理过程需要较大的计算开销,而且,认证过程中的证书传递也增加了通信建立时间;(2) 证书管理和维护需要大量的处理资源和带宽资源;(3) 基于证书的认证体系存在被假冒的风险.本文第 1 节将进一步介绍 DTLS 协议及其弊端.

针对以上问题,本文提出了基于标识密码(identify-based cryptography,简称 IBC)的数据报传输层安全协议.IBC 是由 Shamir[9]首次提出的概念,其基本思想是将用户的身份信息作为公钥,通过这种方式将用户的身份与其公钥进行最自然的绑定,摆脱传统公钥证书需要 CA 签名的体制.另外,在 IBC 中,私钥生成器(private key generator,简称 PKG)完成用户的身份注册、私钥的生成和分发等功能.一个用户只需知道另一个用户的身份信息,即可知道其公钥信息,无需再去获取和验证公钥证书,极大地降低了密码系统中密钥管理的难度.我们将 IBC 引入到 DTLS 中,通过新的密钥协商协议,设计了新的握手过程,从而缩短 DTLS 的连接建立时间.本文主要贡献如下.

(1) 将 IBC 应用于密钥协商过程,使用基于身份的认证密钥协商协议,在协商会话密钥的同时,完成双方的认证,避免证书的生成、传递、验证和销毁等过程,也解决了 CA 不可信和证书使用带来的问题.

(2) 在 DTLS 的基础上,根据新的密钥协商协议,为 DTLS 设计新的握手过程,减少交互次数和消息数量,降低计算量和性能消耗,在保证安全性的同时缩短建立连接所需时间.

(3) 对新设计的握手协议进行了实现,以可选密码套件的形式提供给用户,使得新的握手过程与 DTLS 完全兼容.

为了验证本文提出的基于标识密码的数据报传输层安全协议的性能,本文在 Linux 内核的协议栈中实现了 DTLS,并将本文设计的基于 IBC 的握手协议作为密码套件实现.通过与 DTLS 配备的两个密码套件的性能进行对比分析表明:本文提出的基于标识密码的数据报传输层安全协议在不降低原来 DTLS 安全性的同时,缩短了近 50%的通信连接时间.

本文第 1 节对 DTLS 协议进行概述,并分析其弊端.第 2 节对基于 IBC 的 DTLS 协议的设计进行详细介绍,包括基于 IBC 的标识管理和具体的握手协议设计.第 3 节介绍基于 IBC 的 DTLS 协议的实现,并与传统 DTLS 协议的连接时间进行测试对比.最后是结束语.

1 DTLS 协议概述

DTLS 协议整体分为两层,包括握手(handshake)协议、修改密码规范(change cipher spec)协议、警报(alert)协议和记录(record)协议[8],其层次关系如图 1 所示.

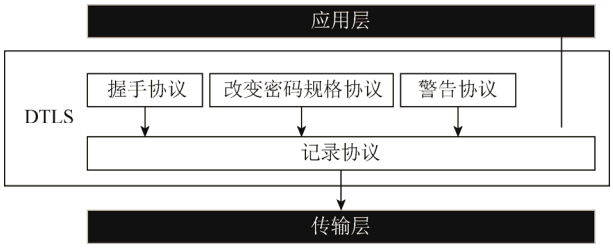


Fig.1 Structure of DTLS

图 1 DTLS 协议结构

记录协议承载来自其他 3 个协议的消息,以及来自应用层的数据,并对上层数据进行分片、压缩、加密等操作后交给 UDP 进行传输.握手协议利用消息来协商安全参数,并在通信双方之间完成共享密钥协商.安全参数包括协议版本、压缩算法、密码算法和散列算法等.如有需要,握手协议也实施客户机和服务器的认证等操作.修改密码规范协议更新当前连接使用的密码组,示意安全密码信息已准备就绪.警报协议向对方传递与 DTLS 相关的错误与警报.

DTLS 必须保证握手消息的可靠传输,才能在通信双方之间成功建立会话.但是 DTLS 协议基于不可靠的传输层协议,因此在传输过程中,握手消息有可能发生丢失、乱序的问题.另外,由于一些握手消息过大,超过一个记录的负载,因此需要对消息进行分段,握手协议也应该把几个记录重组成一个完整的握手消息.DTLS 采用计时器来重传丢失或超时的握手消息.它为每个终端配置一个计时器,在发送一条握手消息的同时启动计时器.在定时器超时之前若没有收到预期的反馈消息,就重传该消息.另外,DTLS 在 TLS 握手消息头格式中添加了几个字段来处理消息的乱序、丢失、分组和重组.

1.1 协议弊端

DTLS 协议提供两种密钥套件 TLS_PSK_WITH_AES_128_CCM_8 和 TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8,使用的密钥协商和计算方法为 PSK 和 ECDHE.

PSK(pre-shared key)为预共享密钥,即双方预先配置静态密钥,通信时通过发送与密钥对应的标识信息来确定使用哪组密钥进行安全传输.虽然 PSK 中不存在证书的传递和验证过程,但由于密钥为静态配置,相对固定,因此安全性较低,并且需要定期更新.一旦密钥丢失,攻击者可以冒充用户与他人进行通信,也可以冒充他人与用户进行通信或对通信进行监听.另外,当通信用户增多时,密钥量呈线性增长,存储和维护的开销过大,不适合大规模网络环境下使用.

ECDHE 是 DH 密钥协商算法在 ECC 中的实现,困难性基于 CDH 问题.相对于 PSK,该方法安全性较高,但该方案仍需要依赖证书完成通信双方的认证,因此在握手过程中需要传递和验证两次证书,计算量较大,延迟较高.另外,握手过程中需要交换两次密钥材料,交互次数多,连接建立时间长.

2 基于 IBC 的 DTLS 协议设计

握手协议是 DTLS 协议的重要组成部分,但目前 DTLS 握手协议在实施通信双方的认证时,仍然要依靠基于证书的认证体系.证书的传输和验证不仅增加了握手协议的复杂性和通信建立时间,而且带来了额外的计算开销.因此,我们将 IBC 引入到 DTLS 协议,结合基于身份的密钥协商算法,重新设计新的握手过程,避免证书的交换和验证,减少交互次数和消息数量,缩短建立连接所需时间.

2.1 基于IBC的标识管理

在基于标识密码系统建立之前,首先要完成标识的选取和私钥分发.为保证身份的唯一性,个人邮箱作为用户的身份信息,会话参与者将邮箱地址作为其公钥.PKG 作为密钥管理机构,为系统中的主机生成以邮箱地址为

基础的身份基私钥.需要指出的是,本文设计的通信协议基于双方处于同一个 PKG 管理的可信域.

标识管理部分主要包括两个步骤,是整个基于身份密码系统运行的基础,分别为 PKG 的初始化和私钥管理,如图 2 所示.本文以 BF-IBE 方案[10]为例,对密钥管理的流程进行介绍,该方案为目前被研究和应用最广泛的方案,本文所使用的密钥协商算法也以该方案为基础.

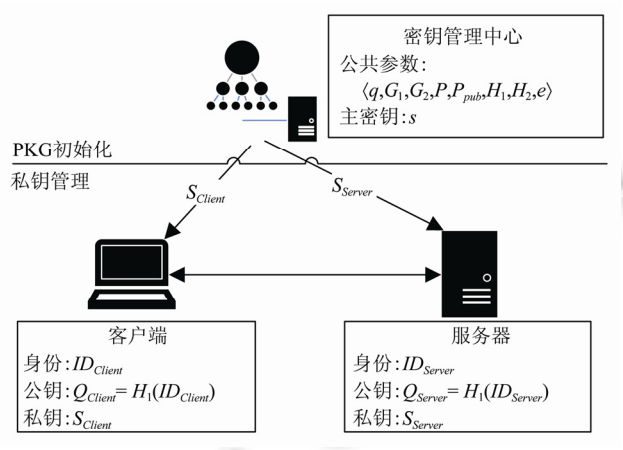


Fig.2 IBC-Based identity management

图 2 基于 IBC 的标识管理

PKG 的初始化:作为一个域的可信管理机构,PKG 在整个系统中最先启动和建立.首先选择某条特定的椭圆曲线,并由其上的点构成 p(p 为素数)阶加法循环群 G_1, 其中生成元为 P.随机选择 $s \in Z_p^*$, 作为 PKG 的主私钥,计算 $P_{pub} = sP$.再根据群 G_1 选择双线性映射 e ,使得 $e: G_1 \times G_1 \to G_2$, G_2 为 p 阶乘法群.最后选择相关哈希函数 $H_1: \{0,1\}^* \to G_1$, $H_2: G_2 \times G_1 \times G_2 \to \{0,1\}^n$, 其中, n 为常量,表示密钥长度.完成初始化后,在该域内广播自己的公共参数 $\langle p, G_1, G_2, e, P, P_{pub}, H_1, H_2 \rangle$.

私钥管理:初始化步骤完成之后,PKG 为其域内所有生成私钥,并通过安全通道进行分发.另外,PKG 还需要负责私钥的撤销和更新.例如,管理域内的某个客户端 Client 请求加入系统,它首先向 PKG 证明自己的身份.这里的认证方式可以是通过预留密钥,也可以基于传统的证书机制和 PKI 体系.虽然传统方法中存在计算和开销大的缺陷,但只需在加入系统时进行 1 次,对大的整体来说,复杂性可以忽略.

如果 Client 通过了身份认证,PKG 会对应其身份生成私钥.首先将其身份 ID_{Client} (例如邮箱地址)映射到椭圆曲线上一个点 $Q_{Client} = H_1(ID_{Client})$. 而后,将自己的主私钥与该点做点乘运算,生成 Client 的私钥,即 $S_{Client} = sQ_{Client}$. 最后,PKG 将私钥 S_{Client} 通过一种安全的方式颁发给 Client 作为其私钥,供解密、签名、密钥协商等时候使用.

2.2 握手协议设计

Sakai 基于 BDH 问题提出了基于身份的零交互密钥协商算法(identity-based non-interactive key agreement, 简称 IBNIKA),Chen 等人[11]对其安全性使用挑战者模型和形式化方法进行了详细地证明.本文利用 IBNIKA 算法进行密钥协商,充分利用 IBNIKA 零交互的特性,设计简单、方便的握手过程,免去证书的交换和验证的过程,节省内存和带宽资源.

2.2.1 握手消息格式

握手过程主要完成安全参数的协商和安全会话的建立,本文新设计的握手过程中使用的消息有 ClientHello,HelloVerifyReuqest,ServerHello,ChangeCipherSpec 和 Finished 这 5 种.

(1) ClientHello 消息中包括版本号、客户端生成随机数、会话标识、cookie、所支持密码套件、所支持压缩方式和扩展部分,其中扩展部分包含客户端的身份信息.其结构定义如下.

struct {
ProtocolVersion client_version;
Random random;
SessionID session_id;
opaque cookie:⟨0..32⟩;
CipherSuite cipher_suites⟨2..2^{16-1}⟩;
CompressionMethod compression_methods⟨1..2^{8-1}⟩;
Extension extensions⟨0..2^{16-1}⟩;
} ClientHello;

(2) HelloVerifyRequest 消息中包括版本号和服务端产生的 cookie,结构定义如下.

struct {
ProtocolVersion server_version;
opaque cookie⟨0..32⟩;
} HelloVerifyRequest;

(3) ServerHello 消息中包括版本号、服务端生成随机数、会话标识、密码套件、压缩算法和扩展部分,其中扩展部分包含服务端的身份信息.其结构定义如下.

struct {
ProtocolVersion server_version;
Random random;
SessionID session_id;
CipherSuite cipher_suite;
CompressionMethod compression_method;
Extension extensions⟨0..2^{16-1}⟩;
} ServerHello;

(4) ChangeCipherSpec 为密码变更协议,长度为一个字节,其值为 1,用于通知密码规格的改变,其结构如下.

struct {
enum { change_cipher_spec(1), (255) } type;
} ChangeCipherSpec;

(5) Finished 消息在各自 ChangeCipherSpec 之后发送,用于验证密钥交换过程是否成功,并校验握手过程的完整性,其结构如下.

struct {
Opaque verify_data[verify_data_length];
} Finished;

其中,verify_data 为校验数据,该数据产生方法如下:

PRF(master_secret, finished_label, Hash (handshake_messages).

表达式中,

① finished_label

对于由客户端发送的结束消息,该标签是字符串“client finished”.对于服务端,该标签是字符串“server finished”.

② handshake_messages

指 ClientHello 消息开始直到本消息为止(不包括本消息、密码规格变更消息和 hello 请求消息)的所有与握手有关的消息,包括握手消息的类型和长度域.

2.2.2 握手流程

本文设计的新的握手流程如图 3 所示.

客户端首先发送未添加 cookie 的 ClientHello 消息给服务器,当服务器收到后,发送 HelloVerifyReuqest 消息给客户端,并在其中放置新生成的 cookie.客户端从收到的 HelloVerifyReuqest 消息中提取出 cookie,将它添加到新的 ClientHello 消息中,然后将信息 ClientHello 消息发送给服务端.这个 cookie 交换过程的目的是为了防止 DOS 攻击.由于本文使用的 IBNIKA 密钥协商算法计算简单,不需要密钥材料的交换,发送完 ServerHello 消息,即可进行共享密钥的计算.倘若服务器对每个 ClientHello 消息都进行密钥计算,自身会因为计算量过大而宕机,更不能抵御 DoS 攻击.所以需要通过 cookie 的发送和验证来防止这种情况.服务端将收到的 cookie 与自己保存的 cookie 进行对比,如果验证的 cookie 的结果是有效的,则继续握手过程.如果恶意用户一直发送未添加 cookie 或伪造 cookie 的 ClientHello 消息,服务器的握手过程则最多只停留在发送 HelloVerifyRequest 阶段,而不需要过多的计算量.

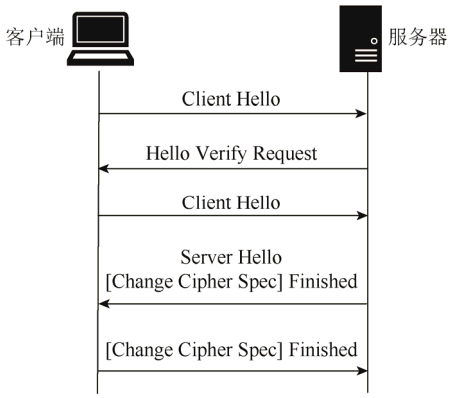


Fig.3 IBC-Based DTLS handshake

图 3 基于 IBC 的 DTLS 握手流程

本文采用基于 BDH 问题提出的 IBNIKA 算法为通信双方建立共享密钥.客户端和服务器首先通过 ClintHello 消息和 SeverHello 消息交换各自的身份 ID_{Client} 和 ID_{Server}.客户端通过服务器的身份计算其公钥 $Q_{Server}=H_1(ID_{Server})$,并用自身私钥 S_{Client} 与其进行双线性映射得到共享密钥 $e(S_{Client},Q_{Server})$.同样地,服务器将自身私钥 S_{Server} 与通过客户端的身份计算出的公钥 Q_{Client} 进行双线性映射得到共享密钥 $e(Q_{Client},S_{Server})$.根据双线性映射性质可证明其正确性:

$$e(S_{Client},Q_{Server})=e(sQ_{Client},Q_{Server})=e(Q_{Client},Q_{Server})^s=e(Q_{Client},sQ_{Server})=e(Q_{Client},S_{Server}).$$

IBNIKA 算法包含通信双方的身份信息,因此具有认证性,攻击者冒充任意一方都不能获得正确的共享密钥.

重新设计的握手协议的具体流程如下.

(1) 客户端发送 cookie 为空的 ClientHello 消息,询问服务端是否在线.

(2) 服务器收到一个没有 cookie 的消息时,通过 HelloVerifyRequest 返回一个 cookie 值.

(3) 客户端提取 cookie 并放在新的 ClientHello 消息中发送,还包括客户端所支持的密码套件和压缩算法,以及产生的随机数,扩展中附带自己的身份信息“client@company.com”.

(4) 服务器验证 cookie,选择合适的密码套件(本文中选择的密码套件为 TLS_IBC_WITH_AES_128_CCM_8),选择合适的压缩算法,创建一个会话 ID,并产生一个随机数,通过 ServerHello 消息发送给客户端,扩展中附带自己的身份信息“server@company.com”.

(5) 服务端发送 ChangeCipherSpec 消息通知密码规格的改变,接下来的数据将使用新协商的安全参数来保护.服务端通过对方的身份信息和 PKG 公布的公共参数产生其公钥,并通过 IBNIKA 算法产生预主密钥,预主密钥通过与随机数进行伪随机运算产生主密钥和会话密钥.

(6) 服务端使用新协商的算法和密钥,加密并发送 Finished 消息,用于验证密钥交换过程是否成功,并校验握手过程的完整性.

(7) 客户端 ServerHello 消息并且收到 ChangeCipherSpec 消息后,计算会话密钥;收到 Finished 消息后,对其进行解密并验证校验数据,验证通过后发送 ChangeCipherSpec 消息通知客户端接下来的数据将使用新协商的安全参数来保护.

(8) 客户端使用新协商的算法和密钥,加密并发送 Finished 消息.服务端收到 Finished 消息后,对其进行解密

并验证校验数据,验证通过后,二者正式建立连接.

3 实验分析

本文在 Linux 内核的协议栈中实现 DTLS,并将本文提出的基于 IBC 的握手协议以可选密码套件的形式提供给用户.客户端发送带有新密码套件的 ClientHello 消息,当服务端选择此套件,则进行本文设计的握手方案;当服务端未选择此套件,依旧使用自带的 PSK 和 ECDHE 方案.这样使得本文设计的握手协议可以与 DTLS 完全兼容.本文提供的密码套件为 DTLS_IBC_WITH_AES_128_CBC_SHA256,表示密钥交换和认证算法为 IBC,对称加密算法为 128 位 AES,加密模式为 CBC,完整性校验算法为 256 位 SHA.

本文实验环境为个人台式机,处理器为 Core i5-4570,内存为 4GB,虚拟机软件为 VMware Workstation Pro,虚拟内存为 1GB,实现系统为 Linux Ubuntu 3.13.0.

DTLS 配备两个密码套件:PSK 方法和 ECDHE 方法.我们将本文提出的基于标识密码的传输层安全协议与 DTLS 自带的两种方案进行对比,通过比较它们的通信开销和连接延迟来测试本文所提方案的性能.

PSK 方案使用的是预先配置的静态密钥,虽然在通信过程中可以认为对方能解密本方发出的消息,即为预期的通信对象,但是存在着密钥刚开始建立时就存在欺骗的情况,因此不满足认证性.PSK 方案不交换密钥协商材料,ClientKeyExchange 消息中只发送与密钥对应的标识码,因此没有进行密钥协商的过程.ECDHE 方案中,双方先交换证书验证身份,后交换密钥协商材料,因此完成了双方的认证和密钥协商过程.本文设计的基于 IBC 的安全传输协议,在密钥协商的同时,完成了通信双方的认证.其安全性等同于 ECDHE,强于 PSK.

3.1 通信开销

通过抓取 3 种方案握手过程中传输的报文,我们对比了 3 种握手过程中产生的通信流量,结果见表 1,其中 ECDHE 中使用的证书大小为 89 字节.在本文设计的基于 IBC 的握手过程中,双方交互次数共 5 次,相对于 PSK 和 ECDHE 的方案,交互次数节省 1 次;握手消息数量共 8 条,比 PSK 方案消息数量节省 2 条,比 ECDHE 方案消息数量节省 7 条.由于在基于 IBC 的握手过程中不再需要处理和传输通信双方的证书,因此相对于 ECDHE 方案,其传输开销缩减了 63%,充分减少了握手通信流量.

Table 1 Transmission overhead of three schemes

表 1 3 种方案传输开销对比

方案	交互次数	消息数量	字节数
PSK	6	10	458
ECDHE	6	15	1 070
IBC	5	8	397

3.2 连接延迟

我们测量了 3 种通信方案的连接延迟,测量标准为从发起连接的第 1 个报文开始到连接建立的时间.通过对 3 种方案通信连接时间进行多次测量,得到它们的平均连接建立时间,结果如图 4 所示.由于 PSK 方案预先设置好共享密钥,因此在握手过程中节省了计算密钥的时间开销.另外,PSK 方案也不需要传递和验证证书,因此安全性较低的 PSK 方案远远优于其他方案,仅需 2.18ms 即可完成连接建立;ECDHE 方案需要验证证书和交换密钥材料,建立连接时间变长,需要 199.78ms;与 ECDHE 方案安全性相当的 IBC 方案因为优化通信量,同时省去了验证证书的时间,仅需要 101.04ms 即可建立通信,比 ECDHE 方案节省了将近一半的时间.

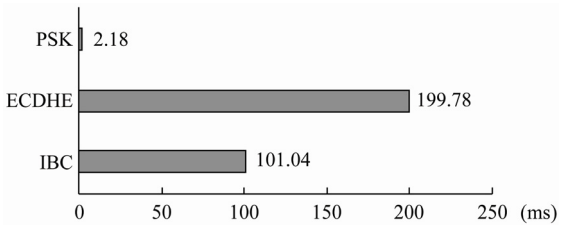


Fig.4 Connection setup time of three schemes

图 4 3 种方案连接建立时间对比

4 结束语

本文将标识密码应用于DTLS,重新设计了DTLS的握手协议.本文采用IBNIKA进行密钥协商,用户的身份即为公钥,并参与会话密钥的计算,使得我们能够在计算会话密钥的同时验证对方身份的合法性,从而减少握手协议中通信双方的交互次数,简化了握手过程.实验结果表明,本文提出的基于IBC的DTLS在不降低原来DTLS安全性的同时,缩短了近50%的通信连接时间.

References:

[1] Rosenberg J, Schulzrinne H, Camarillo G, Johnston A, Peterson J, Sparks R, Handley M, Schooler E. SIP: Session initiation protocol. RFC 3261, 2002.

[2] Schulzrinne H, Casner S, Frederick R, Jacobson V. RTP: A transport protocol for real-time applications. RFC 3550, 2003.

[3] Andreasen F and Foster B. Media gateway control protocol (MGCP). RFC 3435, 2003.

[4] Cheng Y, Chu J, Radhakrishnan S, Jain A. TCP fast open. RFC 7413, 2014.

[5] Bittau A, Hamburg M, Handley M, Mazières D, Boneh D. The case for ubiquitous transport-level encryption. In: Goldberg I, ed. Proc. of the 19th USENIX Conf. on Security (USENIX Security 2010). Washington: USENIX Association Berkeley, 2010. 403−418.

[6] Petullo WM, Zhang X, Solworth JA, Bernstein DJ, Lange T. MinimaLT: Minimal-Latency networking through better security. In: Virgil Gligor, ed. Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications Security (CCS 2013). Berlin: ACM New York, 2013. 425−438.

[7] Langley A, Riddoch A, Wilk A, Vicente A, Krasic C, Zhang D, Yang F, Kouranov F, Swett I, Iyengar J, Bailey J, Dorfman J, Roskind J, Kulik J, Westin P, Tenneti R, Shade R, Hamilton R, Vasiliev V, Chang W, Shi Z. The QUIC transport protocol: Design and Internet-scale deployment. In: Snoeren A. C, ed. Proc. of the Conf. of the ACM Special Interest Group on Data Communication (SIGCOMM 2017). New York: ACM, 2017. 183−196.

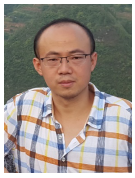
[8] Rescorla E, Modadugu N. Datagram transport layer security version 1.2. RFC 6347, 2012.

[9] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakley GR, ed. Proc. of the CRYPTO'84 on Advances in Cryptology. New York: Springer-Verlag, 1984. 47−53.

[10] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. SIAM Journal on Computing, 2003,32(3):586−615.

[11] Chen Y, Huang Q, Zhang Z. Sakai-Ohgishi-Kasahara identity-based non-interactive key exchange revisited and more. Int'l Journal of Information Security, 2016,15(1):15−33.

李鹏坤(1993－),男,河南周口人,博士生,主要研究领域为网络安全.



王小峰(1982－),男,博士,助理研究员,CCF专业会员,主要研究领域为可信网络及系统,网络安全,分布智能数据处理.

苏金树(1962－),男,博士,教授,博士生导师,CCF高级会员,主要研究领域为计算机网络与通信,信息安全.

薛天(1991－),男,硕士,主要研究领域为计算机网络与通信,信息安全.