WTLS关键协议的仿真研究*)

向生建 刘 勇 杨四铭 佘 堃 熊光泽
(电子科技大学计算机科学与工程学院 成都610054)

摘 要 当前移动电子商务正在从其第一个阶段向第二个阶段发展,安全问题是整个业务成败的关键。WAP协议栈中的WTLS层为移动电子商务提供了一个安全的传输协议,如同TLS对于Internet的作用一样,WTLS足以确保WAP的安全。准确、真实地对协议进行仿真是无线技术研究的一项重要课题。在深入研究WTLS协议的基础上,提出了一种对WTLS协议仿真的模型和方法,以期对实际应用系统提供有价值的参考,最后给出了仿真的结果和结论。

关键词 WTLS,TLS,WAP,WPKI,协议仿真

Research and Simulation on WTLS Protocol

XIANG Sheng-Jian LIU Yong YANG Si-Ming SHE Kun XIONG Guang-Ze
(College of Computer Science and Engineering,UEST of China,Chengdu 610054)

Abstract Nowadays,with the development of M-Commerce,security has become a keystone to the whole operations. WTLS is a protocol layer in WAP Protocol stack,and provides a security transmission protocol for M-Commerce,and can ensure the security of WAP service as TLS do security job for Internet. The very important subject in the wireless technologies is simulating the protocols of communacation accurately and truly. This paper proposes a model/aproach to simulate WTLS protocol based on in-depth study on WTLS and gives some simulation results and conclusions. Hoping this model can provide useful reference for actural system.

Keywords WTLS,TLS,WAP,WPKI,Protocol simulation

1 引言

当前移动电子商务的发展正在从其第一个阶段,即:主要提供信息服务,如天气和路况的预测、股市行情、新闻、E-mail等向第二个阶段,即:提供具有在线支付能力的移动商务服务过渡,比如:移动电子银行、移动贸易、移动购物、移动证券、移动缴费等。这些服务的支付发起于用户操作移动终端进行所见即所得的购买。由于涉及到移动环境下的资金流动,安全问题就成为整个业务成功的焦点。

WAP协议栈中的WTLS层为移动电子商务提供了一个安全的传输协议,它基于Internet上众所周知的TLS协议,如同TLS对于Internet的作用一样,WTLS足以确保WAP的安全。通过WTLS与无线公钥基础设施WPKI的结合,移动电子商务的各个实体的安全性都能得到保障。

准确、真实地对协议进行仿真是无线技术研究的一项重要课题。对于像移动网络这样复杂的系统,理论上难以进行分析。即使可以分析,也能够列出数学模型,却很难得出数值解。这些设想在实验室的网络上实现也是相当复杂的;而直接在实际网络中应用,无论在经济上还是在实现难度上都有无法克服的障碍。因此为了进一步研究WTLS技术,其性能(如用户数量、响应时间、吞吐量、带宽要求等)进行仿真,从而在非现场情况下,通过运行仿真程序,得到WTLS的性能参数,进行性能评估,并提出指导性建议,使移动网络在一定的条件下达到最佳性能。当前对WTLS协议的讨论一方面主要集中在性能分析上,如文[6,7],另一方面主要侧重于协议本身的实现,如文[8,9]。从建模仿真的角度而言,相关研究较少。本文在相关研究的基础上提出了一种对WTLS协议进行仿真的方法及其模型,并对该模型进行了初步仿真。

2 WTLS概述

2.1 协议结构

WTLS协议是由记录协议层组成的,记录协议从WTLS上层协议接收数据然后压缩和加密数据并传送出去。记录协议RP(Record Protocol)又被分为四层,分别是:HP(Handshake Protocol);AP(Alert Protocol);ADP(Application Data Protocol);CCP(Changecipherspec Protocal)。

其中,HP负责在握手阶段协商安全相关的参数,这些参数包括:协议版本号、使用的加密算法、鉴别的信息和由公开密钥技术生成的密钥素材。AP处理安全连接中的报警信息,警报消息主要有错误、严重、致命三种。警报消息使用当前的安全状态发送。ADP是一个从邻近层接收原始数据的协议,仅在安全连接状态下运行。CCP是一个用来在WAP会话的双方间进行加密策略改变的通知协议,此消息在双方的安全参数协商一致后,在握手阶段由客户方或服务方发送给对方实体,用于通知另一方:以后的数据记录将采用新协商的密码规范和密钥。

2.2 安全

WTLS的保密性依靠加密通信通道来实现,所使用的加密方法和计算共享密钥所需的值在握手时进行交换。首先,客户端和服务器交换Hello消息,此后,客户端和服务器交换Pre-MasterSecret,这个值用来计算MasterSecret,计算所使用的加密算法在服务器的Hello消息中进行选择。在这条消息中,服务器通知客户端已经选择了一个密码组,客户端向服务器提供一个密码组列表。如果服务器未发现合适的密码组,则握手失败,连接关闭。当前常用的大批量加密算法有:RC5、DES和IDEA。所有的算法都是块加密算法。加密密钥在密钥

*)本文得到国家创新基金、国家军事预研项目支持。向生建,刘 勇,佘 堃 博士研究生,主要研究方向为信息安全。杨四铭 硕士研究生,研究方向为信息安全。熊光泽 教授,博导,研究方向为实时系统,信息安全。

块的基础上进行操作，密钥块根据协商的密钥刷新频率在一段时间后重新运算。

为了保证安全的联系通道，加密密钥或计算密钥的初始值必须以安全方式进行交换。WTLS 的密钥交换机制提供了一种匿名交换密钥的方法。在密钥交换过程中，服务器发送包含服务器公钥的服务器密钥交换消息。密钥交换算法可能是 RSA、Diffie-Hellman 或 Elliptic Curve DiffieHellman。

WTLS 的身份鉴别依靠证书实现。身份鉴别可以在客户端和服务器之间进行，也可以在服务器允许的情况下，只由客户端鉴别服务器，服务器还可以要求客户端向服务器证明自己。WTLS 证书包括以下证书：用户认证证书，用户签名证书，X.509兼容的服务器证书，机构证书。

数据完整性通过使用消息鉴别编码(Message Authority Code，MAC)而得到保证，MAC 算法同时也被认为是加密算法。客户端发送一系列所支持的 MAC 算法，服务器在返回的 Hello 消息中标出所选的算法。WTLS 支持通用的 MAC 算法，如 SHA 和 MD5。

WTLS 有三个安全级别，WTLS 级别1在无线设备和 WAP 网关间提供保密和完整性；级别2增加了 WAP 网关到安全服务间的认证；级别3增加了无线客户的认证。

2.3 连接管理

WTLS 工作在面向连接的和/或数据报传送协议上。安全层被认为是在传送层上的可选的层，它保留了传送服务的接口。应用管理或会话管理实体为安全连接管理(如建立和终止)的需求提供了附加的支持。

WTLS 连接管理允许一个客户端连接到一个服务器上，并就要使用的协议选项达成一致。一个安全连接的建立过程包括几个步骤，客户端或服务器端都可以根据需要中断这一协商过程(例如，如果有对的端提供的参数不可接受)。协商的内容包括：安全参数(如加密算法，密钥长度)、密钥交换及授权。服务器或客户端在任何时间都可以中止连接。安全会话可以是完整的握手，也可以是简单的握手，本文的讨论均使用完整握手。

2.4 WTLS 与 TLS

TLS 的前身是 SSL，它是 Internet 上最重要的安全标准。虽然 TLS 建立在传输层上，其实它是介于应用层和真正的传输层之间的附加层。同样，WTLS 也是建立在传输层之上，但在它上面是 WTP 事务层和 WSP 会话层，这2层在 Internet 模型中是不存在的。这种安排使得它们与应用层所要求的服务无关。我们认为 TLS 与 WTLS 的不同在于：

1. TLS 需要一个可靠的传输层 TCP。而 WTLS 工作在 WDP 和 UDP 之上。WTLS 不支持数据的分组和重装，它将这个工作交给了下层协议处理。与此不同的是，TLS 可以对上层协议的数据包进行分组。

2. TLS 使用 X.509证书，而 WTLS 定义了新的专为移动设备使用的证书。

3. WTLS 的客户端对于性能的要求比 TLS 的高。WTLS 客户端一般是置于 CPU 处理能力低下，内存较少的手持设备上的，所以客户端通过带宽相对较小的无线网通信网通信时，性能问题显得格外突出，比如网络响应时间等。

3 模型及方法

3.1 消息流图

图1是 WTLS 仿真模型的消息序列图，该图给出了一个对客户端到网关的清晰的描述。

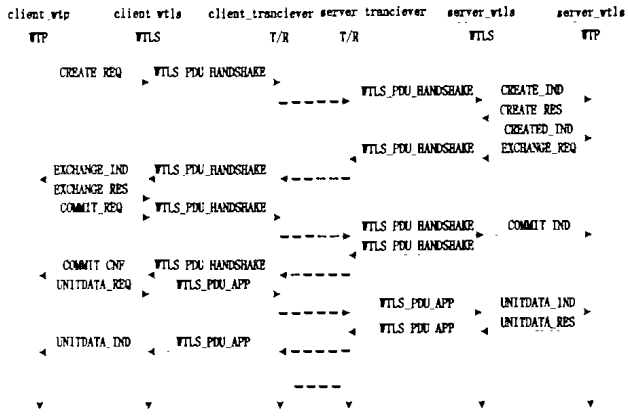

图1 WTLS 仿真模型消息时序图

其中，client_wtp 是客户端的 WTP 协议对象，client_wtls 是 WTLS 对象，首先由 WTP 发送一个 CREATE_REQ 创建安全会话请求，WTLS 再用 PDU 封装一个 ClientHello 消息通过收发器送到服务器的 WTLS 对象，服务器 WTLS 此时向 WTP 发送一个 CREATE_IND 的通知消息，等 WTP 返回 CREATE_RES 消息之后创建相应的服务器缓存再发送 CREATED_IND 给 WTP，在等到 EXCHANGE_REQ 后把完整的 ServerHelloDone 消息传送给客户。此时客户端 WTLS 通知 WTP 一个 EXCHANGE_IND，待收到 EXCHANGE_RES 之后开始创建密钥交换用到的缓存，等 COMMIT_REQ 到达时，再向服务器发送完整的密钥交换信息，如果密钥交换成功，则服务器再向客户发送一个使用 WTLS_PDU_HANDSHAKE 封装的结束消息，然后服务器等待应用数据。客户端还是由上层协议发起应用数据传输 UNITDATA_REQ，再由 WTLS_PDU_APP 封装该应用数据传送给服务器，服务器再完成相应的数据处理之后，产生一个应用数据回应发送给客户端，从而完成一次安全交互。

3.2 进程模型

WTLS 进程模型是在 WTLS 协议状态表基础上建立的有限状态机模型，通过对 WTLS 消息流图的分析，分别得到服务器和客户端的进程模型，如图2为客户端的简化进程模型。

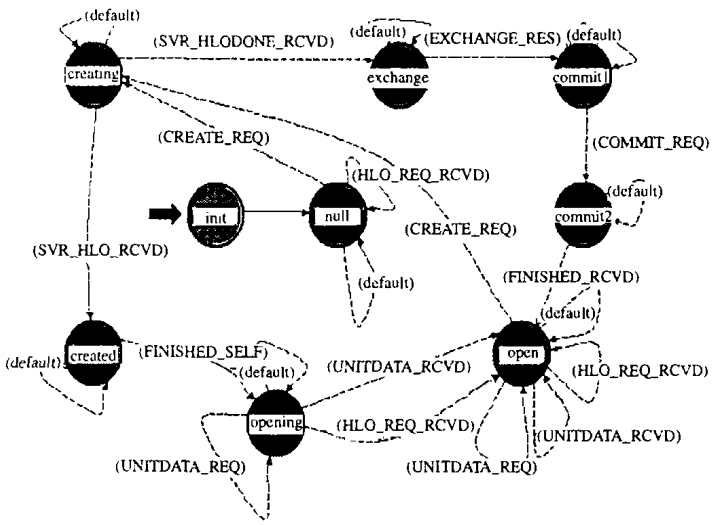

图2 客户端进程模型

在客户端模型中，init 状态首先完成仿真相关的初始化工作，无条件变迁到 null 状态后系统处于等待状态，主要是等待一个上层的安全会话连接请求，这个请求是由仿真系统的一个进程随机生成的。一旦该请求到达本状态机就会触发一个 CREATE_REQ 的中断事件，从而使状态机从 null 状态

变迁到 creating 状态。在 creating 状态的进入执行部分要生成 ClientHello 的包，并且要发送到服务器，模型中其他模块的功能：exchange：在收到从上层协议的回应之后，产生一个密钥交换相关的缓冲区；commit1：收到上层协议的提交请求后，产生剩余的缓冲区，并发送给服务器；commit2：收到回应后通知上层协议相关状态；open：主要完成对应用数据的安全传输工作；created：简单握手情况下，产生一个结束缓冲区发送到服务器；opening：简单握手情况下的中间状态；

服务器模型同客户端模型完全不同，其中的模块功能概括如下：init：初始化进程；idle：空闲状态，接收并处理事件；creating：正在创建，向客户端发送 ServerHelloDone；created：已经创建，产生密钥交换的相关缓冲区；exchange：密钥交换状态，发送密钥交换信息；commit：简化握手时提交；open：完成应用数据发送和接收；opening：完成应用数据发送和接收。

3.3 WTLS 节点模型

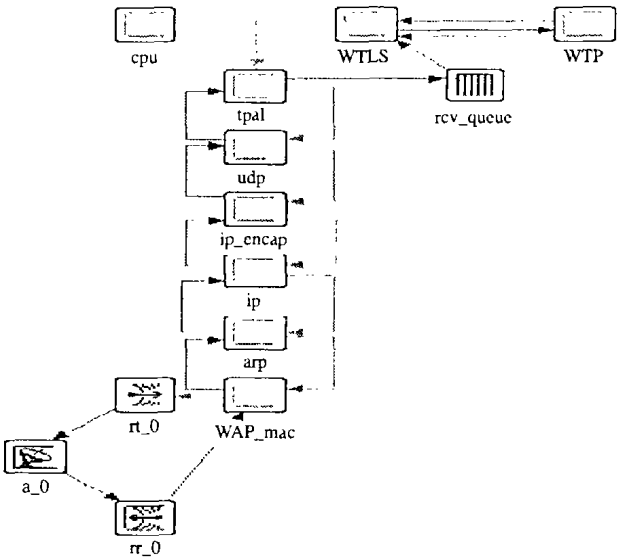

图3 服务器节点

考虑到 WAP 系统与计算机网络的相似性，我们的仿真系统采用 IP 协议来替代 WTLS 下层的 WDP 协议，相应的使用 UDP 完成传输工作。一个完整的服务器节点模型如图3所示。客户端节点模型同服务器相似，只是采用的是客户端的 WTLS 进程模型。

4 仿真结果与分析

仿真过程中，为了能表现 WTLS 的多种安全算法，且每种算法可能采用不同长度密钥的情况，我们使用了一个处理速率参数(Processing Rate)。该参数表示特定算法的特定密钥长度的运算速度，在仿真过程中，我们把它作为一个已知条件。鉴于实际安全会话可能多次建立和销毁，故仿真安全会话的多次重建依靠一个安全会话的平均时间(Mean Session Time)参数，我们将对会话时间分别为60秒和120秒的两种情况进行仿真。

仿真中的随机信号是一个以特定分布时间间隔产生特定分布大小的数据包的进程模型，且设定其分布为参数2s 的指数分布。以上参数取值如下表1所示。

表1 主要仿真参数

参数	值/分布	应用于
Processing Rate	1MB	
Processing Rate	30KB	
Mean Session Time	60 s	
随机信号间隔	参数2s 的指数分布	

除了上述的仿真参数之外，我们设定无线网络带宽为30kHz，数据传送速率为15kB。在模型中我们使用了两种数据包格式：应用数据包格式 WTLS_PDU_APP 和握手数据包格式 WTLS_PDU_HANDSHAKE，它们分别表示应用数据包和握手数据包。另外，当前的仿真没有考虑节点在移动时的影响。

我们使用了5客户端节点和一个网关服务器的模型进行仿真，仿真时间为30分钟。

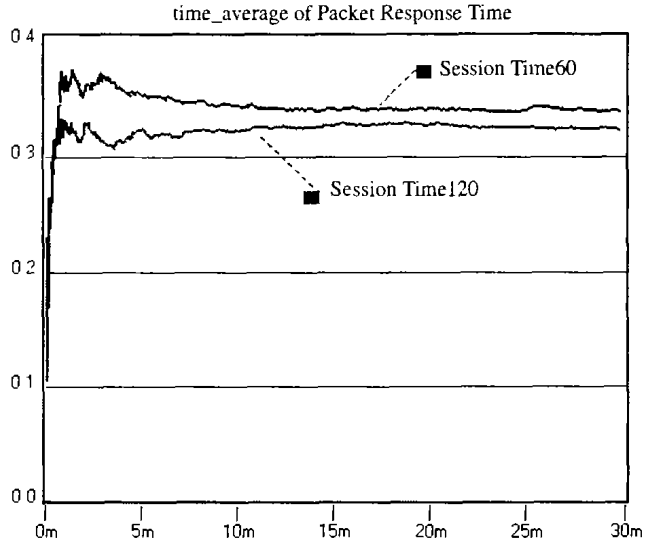

图4 平均会话时间对响应时间的影响

图4即为平均会话时间为60秒和120秒的响应时间对比，可以看出，平均会话时间较长的情况下其平均响应时间较小。我们同样对比了服务器端处理速率为1MB、客户端处理速率30kB 和服务器端处理速率为0.5MB、客户端速率15kB 两种情况下对响应时间的影响。可以看出，处理速率较高时其响应时间较短，换言之，使用性能好的算法或者密钥长度短的算法，其响应时间较短。而且由上述的结果我们认为，随着节点数目的增加，服务器利用率的提高，这种响应时间的差距会更明显。

结论 本文主要讨论了 WTLS 协议仿真相关的问题，在此基础上提出协议的仿真方法、模型及应该考虑的仿真参数。通过该仿真系统我们可以预估各种参数对无线 WAP 安全的影响，并提供一个实际应用系统设计和实现的参考，最终达到系统优化的目的。

参 考 文 献

1 WAP Forum，WAP2.0 Technical White Paper[S]. Janurary 2002 version. http://www.wapforum.com
2 WAP Forum，Wireless Application Protocol Architecture Specification: WAP-210-WAPArch-20010712-a[S]. July 2001. http://www.wapforum.com
3 WAP Forum，Wireless Transport Layer Security Specification: WAP-261-WTLS-20010406-a[S]. April 2001. http://www.wapforum.com
4 WAP Forum，Wireless Public Key Infrastructure: WAP-217-WPKI-20010424-a[S]. April 2001. http://www.wapforum.com
5 Hanle C，Hofmann M. Performance Comparison of Reliable Multicast Protocols using the Network Simulator ns-2[C]. In：Proc. of the Annual Conf. Local Computer Networks(LCN)[C]. Boston，MA，USA，Oct. 1998
6 Levi A，Savas E. Performance Evaluation of Public-Key Cryptosystem Operations in WTLS Protocol[C]. In：Proc. of Eighth IEEE Intl. Symposium on Comupters and Communication (ISCC'03)2003
7 Herwono I. Liebhardt I. Performance of WTLS and its Impact on an M-Commerce Transaction[C]. Xi'an China. In：Proc. of the Third Intl. Conf. on Information and Communications Security (ICICS'01)，Nov. 2001. 167～171
8 罗蕾，王庆，谭罗丽. WAP 安全构架研究及 WTLS 的实现[J]. 电子科技大学学报，2002，31(4)：387～392
9 田峰，谭寒生，周明天. 一种基于 WTLS 的无线安全网关的设计[J]. 计算机应用，2003，23(3)：70～72