第32卷 第14期 计 算 机 工 程 2006年7月
Vol.32 № 14 Computer Engineering July 2006
·安全技术· 文章编号：1000—3428(2006)14—0157—03 文献标识码：A 中图分类号：TP393.08

# 基于 Kerberos 的移动 Ad-hoc 网络安全认证方案

唐 枫，钟 珞
(武汉理工大学计算机科学与技术学院，武汉 430070)

**摘 要**：提出了基于 Kerberos 的移动 Ad-hoc 网的安全认证机制 KADH，它继承了传统 Kerberos 系统中一些在 Ad-hoc 网络环境中实用的特性。同时针对结点的移动性和简短性，引入了复制、选择和校验机制确保了连接的安全性，同时使来自网络内部的恶意攻击的危险性降到最低。

**关键词**：安全认证；移动 Ad-hoc 网络；网络安全；Kerberos 协议

# Secure Authentication in Mobile Ad-hoc Network Based on Kerberos

TANG Feng, ZHONG Luo
(College of Computer Science and Technology, Wuhan University of Technology, Wuhan 430070)

**【Abstract】** This paper presents a new Kerberos assisted Authentication Mechanism in Mobile Ad-hoc Networks named KADH,KADH migrates a number of features from traditional, wired Kerberos environments to the Ad-hoc environment and provides secure extensions to support the more challenging demands of ad-hoc network. Due to the mobility and short range of the nodes, we introduce measures like replication, elections and optional check to ensure maximum connectivity of the clients with the servers and minimize the risk of malicious attacks from within the network.

**【Key words】** Secure authentication; Mobile ad-hoc network; Network security; Kerberos protocol

Ad-hoc网络是一种特殊的，不需要固定设施支撑的，由若干移动节点组成的自组织无线网络。作为一种无线移动网络，Ad-hoc网络和传统的移动网络主要的区别为移动Ad-hoc网络不依赖于任何固定的网络设施，而是通过移动节点间的相互协作来进行网络互联。由于单个结点具有比较低的传输能力，结点之间必须相互协作使数据在各个结点之间传输，因此恶意结点伪造、篡改或毁坏原始数据，可能使结点之间的信任关系受到威胁。安全认证是影响有线和无线网络通信安全的主要因素之一，它一般包括直接认证和间接认证 2 种方式[1]。在直接认证中，通信双方利用共享的对称或非对称加密密钥来验证双方的身份。在间接认证方式中，引入了可信任的第三方，如CA(认证中心)来负责将一方安全地引荐给另一方。

目前，多数为Ad-hoc网络开发的安全路由协议都是利用PKI(Public Key Infrastructures)来认证通信结点的间接认证机制[2]。PKI是基于非对称加密的安全系统，但也存在许多缺点，如对计算以及通信资源要求较高，从而使基于PKI的系统容易受到拒绝服务攻击(DoS)。与此相比，Kerberos[3]是基于对称加密的间接认证机制，Kerberos的安全性和有效性经历了时间的考验。它具有其他认证机制所不具有如下的特性：

(1)有效防止对客户和服务器自身的伪造；
(2)防御重放攻击；
(3)在终端之间建立安全信道；
(4)相互认证。

## 1 基于 Kerberos 的网络认证方案 KADH

在 Kerberos 系统中，认证服务器存储了所有用户的密钥哈希值，所有用户使用一个认证服务器，一旦认证服务器出现错误会影响整个认证系统的运行。

为移动 Ad-hoc 网络提出一种新的安全认证方案 KADH。KADH 是由许多分布式的 Kerberos 认证服务器来实现分布式的认证服务，所有服务器之间实时的相互通信，使数据库保持同步；同时，采用了可选择的校验机制和服务器选择调度机制，从而使结点之间的单播和多播通信可以利用服务所提供的会话密钥进行安全的认证。

### 1.1 假设

在 KADH 方案中，首先提出几条假设如下：

(1)所有用户都拥有一个只有自己知道的密码或密钥；

(2)所有的服务器知道所有用户密码的哈希值；

(3)所有的服务器每两个之间都有一个彼此共享的会话密钥。

### 1.2 认证过程

KADH 的认证过程如图 1 所示。

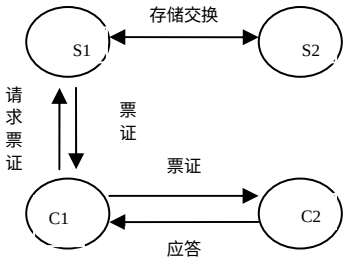


**图 1 认证过程**

当结点 C1 要与结点 C2 进行安全通信时，C1 首先将通信请求发送到认证服务器之一 S1(1)。S1 根据 C1 的请求产生一个包含会话密钥的票证(Ticket)，并传回给客户机 C1(2)。C1 收到票证后将之发送给目标主机 C2(3)。C2 将票证解密从

**作者简介**：唐 枫(1980—)，男，硕士，主研方向：智能信息系统，信息安全与密码学；钟 珞，博导
**收稿日期**：2005-08-08 **E-mail**：Tangfeng177@sina.com

而得到会话密钥，并对 C1 作出响应，二者之间的安全通信机制便建立起来。

### 1.3 初始化

在初始化配置过程中，可以仅存在单独一个存储服务器，它存储了所有用户的用户 ID、密码哈希值、优先级以及生命期。生命期的大小是由网络环境的安全程度来决定的。网络环境安全程度越高，密码的生命期越长，相反则越短。数据库服务器中主要包括 4 个字段(UserID、Password、Priority、Lifetime)。如表 1 所示。

**表 1 数据库主表主要字段**

| UserID | Hashed Password | Priority | Lifetime |
|---|---|---|---|
| Server1 | 1101010101010101 | 6 | 5 400 |
| Server2 | 1010101110011110 | 2 | 1 200 |
| Client1 | 1001110111111001 | 9 | 600 |
| Client2 | 0101010111010011 | 5 | 3 600 |

### 1.4 用户认证

本方案利用一个改进后的 Kerberos5 协议为移动 Ad-hoc 网络提供认证服务。在 Kerberos 中，票证授予服务器(TGS)用来为已经通过认证服务器(AS)认证的用户提供通信票证。在本方案中去除了票证授予服务器，从而使本方案更适合与 Ad-hoc 网络的环境。

当一个结点需要与另一个结点建立安全连接时，认证过程如表 2 所示。

**表 2 客户-客户的认证过程**

| |
|---|
| (1) Client1 → Server<br>Options, $ID_{C1}$,$ID_{C2}$, Times, Nonce<br>(2) Server → Client1<br>$ID_{C1}$,$Ticket_{C2}$,{$K_{C1,C2}$,Times,Nonce,$ID_{C2}$}$K_{C1}$<br>(3)Client1 → Client2<br>Options, $Ticket_{C2}$,$Authenticator_{C1}$<br>(4) Client2 → Client1<br>{TS,Subkey,Seq#} $K_{C1,C2}$ |
| $Ticket_{C2}$={Flags,$K_{C1,C2}$,$ID_{C1}$,$AD_{C1}$,Times}$K_{C2}$<br>$Authenticator_{C1}$={$ID_{C1}$,TS}$K_{C1,C2}$ |
| Options: 通知服务器返回的票证中需要包含 flags 信息<br>Times: 在票证中用来说明开始、结束和更新的时间<br>Flags: 票证的状态信息<br>Nonce: 防止重放攻击的随机数<br>Subkey: 用来代替 KC1,C2 的另一个会话密钥<br>Seq#: 用来检测重发攻击的序列号。<br>$ID_{C1}$：客户机 C1 的身份 ID<br>$ID_{C2}$：客户机 C2 的身份 ID<br>$AD_{C1}$：客户机 C1 的网络地址<br>$K_{Cn}$：用户 Cn 基于用户哈希密码值的加密密钥<br>$K_{C1,C2}$：客户机 C1 和 C2 之间的会话密钥<br>TS: 认证符产生的时间 |

在认证服务交换中，客户机 C1 向 KADH 服务器发送一个希望与 C2 安全通信的请求，KADH 服务器首先通过用户 ID 检验客户机 C1 和 C2 生命期是否有效。如果它们具有有效的生命期，服务器就向 C1 提供一个包含会话密钥的用来访问 C2 的票证(Ticket)，客户机 C1 随之将票证发送给 C2；C2 接收到票证后通过发送带时间戳的信息向客户机 C1 作出回应。

与原始 Kerberos5 协议相比，在本方案中，只利用了认证服务器来为用户请求提供安全通信票证，在 Ad-hoc 网络中，本方案具有单一服务器访问、认证速度显著提高和客户端计算负载小等优点。

### 1.5 密钥分发

当客户的生命期到期后，服务器将停止为其服务，票证也会自动过期。同时根据规则，当票证过期后，用户会话也会因此终止。如果客户希望继续得到服务，必须向认证服务器申请新的密码，新密码分配如表 3 所示。

**表 3 密钥分发过程**

| |
|---|
| (1)Client1 → Server<br>Options, $ID_{C1}$ , Nonce<br>(2)Server → Client1<br>$ID_{C1}$,{$K_C$,Times,Nonce,$ID_{C1}$}$K_{C1}$ |
| Options: 通知服务器返回的票证中需要包含 flags 信息。<br>Times: 在票证中用来说明开始、结束和更新的时间。<br>Nonce:防止重放攻击的随机数。<br>$ID_{C1}$：客户机 C1 的身份 ID。<br>$AD_{C1}$：客户机 C1 的网络地址。<br>$K_{C1}$：基于用户哈希密码值的加密密钥。<br>$K_C$：客户机 C1 的新密码。 |

### 1.6 服务器选择

由于结点的分布范围广泛，可能需要多个服务器存在。服务器之间可以定时地用Beacon和Echo数据包来检验其他服务器的可用性[4]。在这个过程中，当某个服务器因为无线传输范围、地理位置或生命期到期而失效时，服务器选择机制将被触发。在选择服务器的过程中，服务器首先会在数据库中查找结点的优先级，优先级最高的结点将先被考虑。如果 2 个或更多的结点具有相同的优先级，将考虑它们的生命期，那些具有最高优先级和最长生命期的结点，服务器将把数据库安全的传输给它使之升级为服务器。同样，如果服务器的数量增加(不可用服务器恢复正常)，优先级最低以及生命期最短的服务器将自动降级为客户机。

### 1.7 数据管理

实时的数据复制对于整个认证机制保持同步和操作完整性至关重要。数据库复制使账户数据库能够在各个服务器之间传输并保持同步，从而防止结点被攻击或被篡改。它也可保证所有用户的账户是最近更新的(通过将变化映射到各个服务器)。这种机制确保了所有到数据库最后一次更新起被增加、修改或撤消的结点的实时性和有序性。数据库复制的频度主要受到地域的分散性、结点的分布情况、环境的安全性和结点能量的影响[5]。如表 4 所示，R是服务器S1 当前的数据库，TS是复制时间，N是当前的复制序列号。

**表 4 存储复制**

| |
|---|
| Server1 → Server2<br>{TS, R, Seq# } $K_{S1,S2}$ |
| Seq#: 复制序列号。<br>R: 用户账户数据库。<br>$K_{S1,S2}$：服务器 S1 和 S2 之间的会话密钥。<br>TS: 复制发生的时间信息。 |

### 1.8 可选择的校验机制

在那些结点受攻击可能性相对较高的不安全环境中，引入了可选择的校验机制。本机制可以基于一个较为复杂的生物认证设备，也可以是基于一个简单的密码。当校验机制被激活时，用户需提供一个针对个别请求或所有请求的密码来向服务器确信结点仍在安全控制之下。如果当前客户不能提供密码，那么结点就通知其他服务器删除该用户账户信息并停止为其服务。校验机制的使用取决于 Ad-hoc 网络环境的安全程度。

## 2 安全性分析

本节介绍KADH如何防止网络中的各种可能的攻击。前面讨论过，本方案的安全基础主要是依赖于初始密钥交换来提供认证服务。一些其他服务如机密性、完整性和不可否认性都依赖于认证服务的质量。Kerberos协议被认为是能有效防御各种攻击的健壮的协议，同时也不可避免地存在一些安全漏洞[6]。在KADH中一个好的解决方案是利用加密IP数据包，同时在MAC层利用广播路由。一旦安全路由建立起来，在终端之间传输的信息数据包也需要加密。在IP数据包中需要加密的字段如表 5、表 6 所示。

**表 5 路由数据包**

| MAC | IP | DATA |
|---|---|---|
| 明文 | 加密 | 加密 |

**表 6 信息数据包**

| MAC | IP | DATA |
|---|---|---|
| 明文 | 明文 | 加密 |

### 2.1 主动攻击

2.1.1 路由破坏攻击

基于路由破坏的攻击一般是破坏路由表的完整性，从而通过修改路由信息、重定向到其他的目的地或经过更长的路由到达目标主机造成网络延迟。这样的攻击主要包括黑洞攻击、路由循环攻击、增加路由长度攻击和能量耗尽攻击等。

解决方案：遵循 KADH 协议的 Ad-hoc 网络结点可以利用对网络流数据和控制信息进行加密，从而保证了哈希信息在内的所有传输数据包的完整性和机密性。有效地防止了基于篡改的各种攻击。

2.1.2 替换攻击

替换攻击通过产生替换的或错误的路由信息来进行攻击。由于替换的路由信息和原始真实的路由信息非常接近，因此这种攻击非常难于识别。对于替换攻击，本方案是通过会话密钥来验证收到的控制信息和数据包的正确性，因为会话密钥是唯一的，被替换的数据包将很容易被识别并丢弃。

2.1.3 模仿攻击

恶意结点能够通过在网络中伪装其他结点的方式来实施攻击。当一个恶意结点无法向服务器有效认证它自己身份时，就要通过修改它的 MAC 地址和 IP 地址来改变网络的拓扑结构。在本方案中，所有点到点的数据传输都被间接加密，从而保证对数据包的验证，同时会话只被已通过认证的终端所拥有。因此，所有数据包的合法性在解密过程中被验证，保证那些伪造的数据包被识别并丢弃。

### 2.2 被动攻击

在被动攻击中，攻击者只是被动地偷听网络信息，并截获有价值的信息，如结点等级和网络拓扑结构。比如路由到一个特殊结点的请求要多于其他结点，那么攻击者可能认为该结点对于整个无线网络运作是必不可少的。并对该结点采取一些攻击使整个网络陷入瘫痪。同样，当不可能确定某个结点的确切位置时，攻击者可以分析路由数据包的内容，来找出网络的拓扑结构信息。无线网络的信道没有物理保护，因此很容易被窃听，特别是基于全方向无线信号的无线网络。在无线网络环境中被动攻击是很难检测和预防的。在 KADH 中，解决方法是在传输之间将所有路由数据和信息数据包加密。使被动偷听者在有效期内利用有效信息进行攻击的可能性大大降低。

## 3 结束语

本文提出了一种在 Ad-hoc 网络中安全的基于改进的 Kerberos 协议的密钥交换机制。对于客户间通信，每个结点向认证服务器之一发出请求。服务器产生一个会话密钥并将之封装在票证中发给请求客户机。这时客户就可以利用票证来与所要通信的客户机建立会话。由于移动 Ad-hoc 网络中结点的移动性和简短性，我们引入了一些方法如复制和选择机制来确保客户机与服务器连接的安全性。同时，为了防止物理上的破坏和篡改，还引入了可选的校验机制，使来自网络内部的攻击危险性降到最低。

### 参考文献


1 Fox A, Gribble S D. Security on the Move: Indirect Authentication Using Kerberos[C]. Proc. of the Second Annual International Conference on Mobile Computing and Networking, 1996: 155-164.

2 Pirzada A, McDonald C. A Review of Secure Routing Protocols for Ad-hoc Mobile Wireless Networks[C]. Proc. of 2nd Workshop on the Internet, Telecommunications and Signal Processing, 2003.

3 Kohl J, Neuman S. The Kerberos Network Authentication Service [S]. RFC 1510, 1993.

4 Corson S. Papademetriou S, Papadopoulos P. An Internet MANET Encapsulation Protocol Specification[Z]. Internet Draft, 1999-08-07.

5 Gruenwald L, Javed M. Energy Efficient Data Broadcasting in Mobile Ad-hoc Networks[C]. Proc. of the International Database Engineering and Applications Symposium, 2002: 64-73.

6 Bellovin S M, Merritt M. Limitations of the Kerberos Authentication System[C]. Proc. of USENIX Winter Conference, 1991: 253-267.


（上接第 156 页）

### 参考文献


1 张焕国, 覃中平, 丁玉龙. 计算机安全保密技术[M]. 北京: 机械工业出版社, 1995-02.

2 吴世忠, 祝世雄, 张文政. 应用密码学[M]. 北京: 机械工业出版社, 2000-01.

3 戴英侠, 连一峰, 王 航. 系统安全与入侵检测[M]. 北京: 清华大学出版社, 2002-03.

4 胡 骏, 詹文军. 设计安全的体系结构[M]. 北京: 机械工业出版社, 2003-10.

5 范文慧, 李 涛, 熊光棱. 产品数据管理(PDM)的原理与实施[M]. 北京: 机械工业出版社, 2004-01.