

IEEE 802.1X 的安全性分析及改进

周超¹,周城²,郭亮¹

(1. 重庆通信学院 研究生管理大队,重庆 400035; 2. 重庆通信学院 机动作战通信系,重庆 400035)

(augustin@163.com)

摘要: IEEE 802.1X 标准存在一些设计缺陷,为消除拒绝服务攻击(DoS)、重放攻击、会话劫持、中间人攻击等安全威胁,从状态机运行角度对协议进行了分析,指出产生这些问题的根源在于协议状态机的不平等和不完备,缺乏对消息完整性和源真实性的保护。提出并实现了一种双向挑战握手及下线验证的改进方案,并用一种改进的 BAN 逻辑对其进行了形式化分析。经验证,该方案能有效抵御上述安全威胁。

关键词: 网络访问控制;IEEE 802.1X 标准;可扩展认证协议;状态机;形式化分析;BAN 逻辑

中图分类号: TP393.08 **文献标志码:** A

Security analysis and improvement of IEEE 802.1X

ZHOU Chao¹, ZHOU Cheng², GUO Liang¹

(1. Graduate School, Chongqing Communication Institute, Chongqing 400035, China;

2. Department of Maneuvering Fighting Communication, Chongqing Communication Institute, Chongqing 400035, China)

Abstract: It has been proved in many researches that there are some design flaws in IEEE 802.1X standard. In order to eliminate the Denial of Service (DoS) attack, replay attack, session hijack, Man-In-the-Middle (MIM) attack and other security threats, the protocol was analyzed in view of the state machines. It is pointed out that the origin of these problems is the inequality and incompleteness of state machines as well as the lack of integrity protection and source authenticity on messages. However, an improvement proposal called Dual-way Challenge Handshake and Logoff Authentication was proposed, and a formal analysis was done on it with an improved BAN logic. It is proved that the proposal can effectively resist the security threats mentioned above.

Key words: Network Access Control (NAC); IEEE 802.1X standard; Extensible Authentication Protocol (EAP); state machine; formal analysis; BAN logic

0 引言

IEEE 802 LAN/WAN 委员会为解决局域网网络安全问题,在2001年制定了标准 IEEE Std 802.1X-2001,之后在2004年提出其修订版:IEEE Std 802.1X-2004^[1]。目前,基于802.1X的网络访问控制(Network Access Control, NAC)系统在学校、企业等单位得到广泛应用。然而802.1X存在安全缺陷,面临拒绝服务攻击、会话劫持、重放攻击、中间人攻击等安全威胁^[2-4]。研究表明802.1X存在安全问题的根源是状态机的缺陷,因此可从协议状态转移过程出发来构造攻击状态转移机制,据此设计出有效的攻击检测方法^[5]。为了消除协议缺陷,目前已有四次握手认证解决方案,该方案在无线网络得到广泛应用,是IEEE 802.11i标准的一部分,但其仍然存在一定安全隐患,面临几种不同形式的拒绝服务攻击的威胁^[3,34-40]。另外,文献^[2,6]提出对局域网上的扩展认证协议(Extensible Authentication Protocol over LAN, EAPOL)数据帧增加保护字段并建立共享密钥和密钥轮换机制,对逐条消息进行完整性和源真实性保护,这些方案可有效改进协议,但需要对数据格式加以改变,在当前基于802.1X的NAC系统上实施具有一定难度。

本文针对协议状态机运行过程进行研究,剖析产生安全问题的原因,提出一种解决方案,完善了状态机,保留了协议

原有数据帧格式。

1 IEEE 802.1X 分析

1.1 802.1X 简介

IEEE 802.1X 对基于802.x技术的网络提供逻辑链路级的标准化认证和控制服务,是基于C/S模式的访问控制和认证协议,实现该协议的系统包含3个组成部分:客户端(Supplicant)、认证者(Authenticator)和认证服务器(Authentication Server)。在客户端和认证者系统,各包含一个执行算法和协议操作的实体对象,称为端口访问实体(Port Access Entity, PAE)。协议认证过程是客户端、认证者与服务器交互的过程,实际由上层协议可扩展认证协议(Extensible Authentication Protocol, EAP)^[7]完成。在以太网内EAP消息封装在EAPOL帧里,认证者到服务器之间的通信目前常采用EAPOR(EAP over RADIUS)。EAP协议只是一个规范性协议,它支持多种实现方式,故而在802.1X体系结构中,客户端PAE和认证者PAE各包含了两个独立的组件,分别是实现端口访问控制协议PACP的状态机和上层协议(即EAP认证协议)实现。图1体现了这种结构,从图中可见,客户端的上层组件实现了EAP功能,认证者系统在上层组件结合了EAP和AAA功能。两个PAE中,上层组件和状态机之间通过一

收稿日期:2010-11-10;修回日期:2011-01-18。

作者简介:周超(1984-),男,湖南望城人,硕士研究生,主要研究方向:军事信息安全;周城(1963-),男,江苏无锡人,副教授,主要研究方向:信息安全;郭亮(1984-),男,湖南湘潭人,硕士研究生,主要研究方向:信号设计与编码。

系列接口实现信号量的传递^{[1]33-34}。

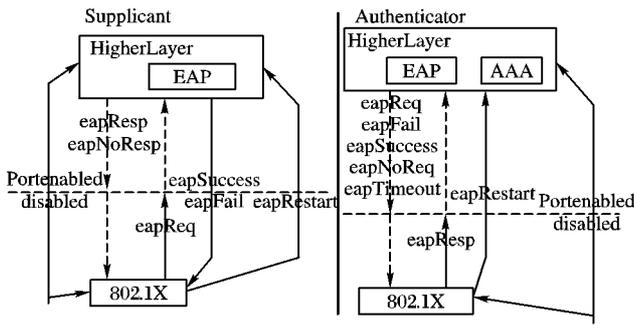


图 1 客户端和认证者 PAE 的上层接口

1.2 状态机分析

1.2.1 客户端 PAE 状态机分析

图 2 是客户端 PAE 的状态机交互模型。图中共有两个简化模型,左侧为客户端状态机,右侧为客户端后台状态机。图中虚线箭头代表上层(Higher Layer)协议组件和状态机之间信号量的传递。为简明起见,本图及后续图省略了一些状态操作和状态转换的触发事件。可以看到,两个状态机的状态转换过程中都没有对认证者的认证过程,也没有对认证结果 eapSuccess/eapFail 的验证。如果攻击者伪装成合法认证者,伪造或篡改认证结果,客户端也将执行相应的状态转换。

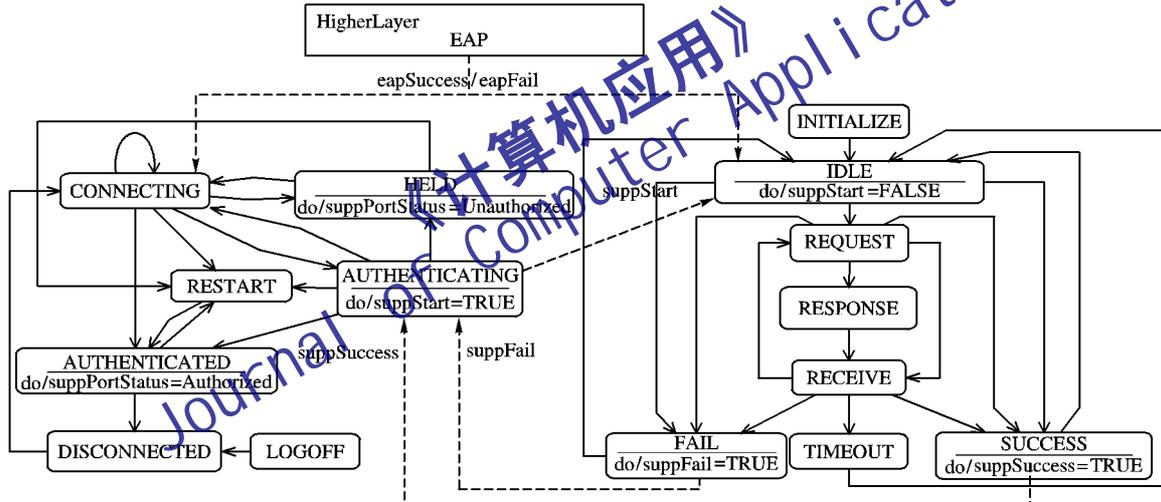


图 2 客户端状态机交互模型

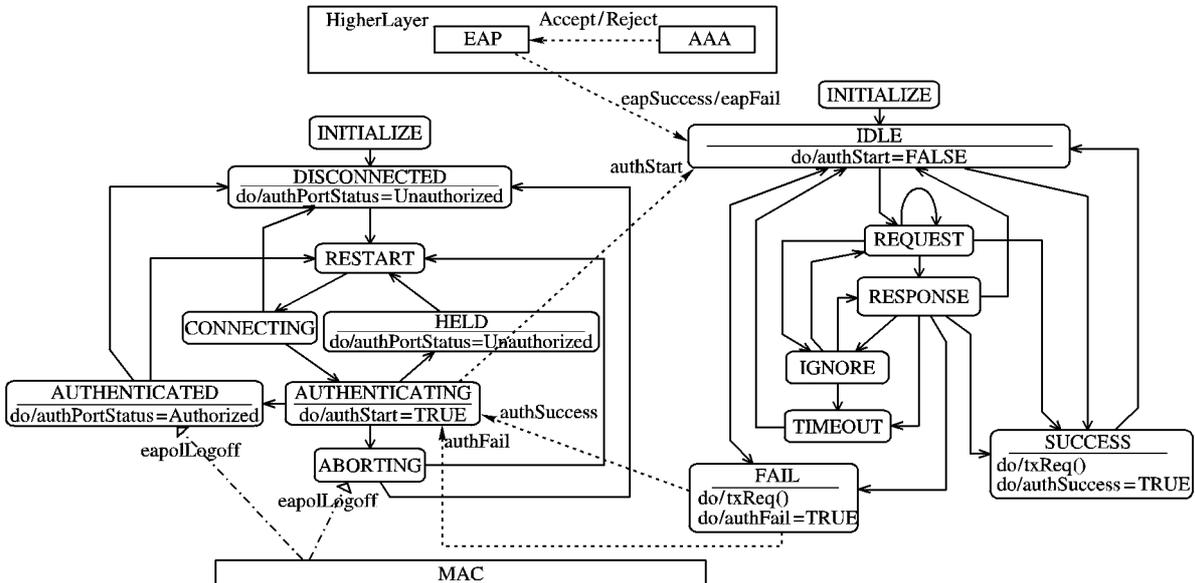


图 3 认证者状态机交互模型

1.2.2 认证者 PAE 状态机分析

图 3 是认证者 PAE 的状态机交互模型。图中共有两个状态机简化模型,左侧为认证者状态机,右侧为后台认证状态机。图中带实心箭头的虚线代表上层协议组件和状态机之间的信号量传递,反映了在认证成功或失败情形下认证者的状态转换过程。分析这一过程发现认证者系统并没有提供对 EAP-Success/Failure 消息的验证功能,攻击者可以伪装成认证者向客户端发送 EAP-Success/Failure 消息,破坏状态机的运行。带空心箭头的虚线代表底层端口与状态机之间信号量的传递,体现了认证者收到客户端主动下线请求时的状态转换过程。可见在收到 EAPOL-Logoff 帧后,认证者状态机直接转入 DISCONNECTED 状态并将端口关闭,没有对 EAPOL-Logoff 帧进行确认。那么攻击者伪装成客户端向认证者发送 EAPOL-Logoff,将导致其关闭合法用户的网络端口。

1.2.3 状态机安全性分析

结合对客户端和认证者系统的状态机分析可以得知,802.1X 协议状态机在认证成功/失败,以及客户端主动下线等相关状态转移过程中存在安全问题,攻击者可以通过伪造、篡改或者重放 EAPOL-Logoff 帧、EAP-Success/Failure 消息等手段,破坏协议状态机正常运行,进而威胁到协议对端口的控制。出现这些问题的根本原因在于协议状态机不平等和不完备,协议中客户端与认证者仅执行对客户端的单向认证,以及

协议中缺乏对双方所发送消息的确认和验证。这使得基于 802.1X 协议的 NAC 系统过分依赖上层认证协议的安全性,如果上层认证协议也仅执行单向认证,或者上层协议存在缺陷,那么系统的整体安全将更加脆弱。

1.3 上层认证协议对比

当前应用较为广泛的 EAP 认证方法有 EAP-MD5、EAP-TLS、EAP-TTLS/PEAP、LEAP 和 EAP-FAST 等,表 1 对这些认证协议做了简单的对比分析^[8-9]。由于 EAP-TTLS 和 PEAP 具有较大的相似性,将这两种方法归为一类。

1.4 面临的安全威胁

从以上分析可知,802.1X 协议存在一定的安全缺陷,当前研究也表明,基于 802.1X 的 NAC 系统面临多种安全威胁。例如:攻击者可通过伪造网络数据,如 EAPOL-Logoff、EAP-Failure 等实现拒绝服务攻击;可在上述拒绝服务攻击基础上,冒充合法的认证者或客户端实现会话劫持;通过截获并保存一次成功的认证过程的数据包,并在其后某个时候重放,实现重放攻击;在 LAN/WLAN 中伪造未经授权的认证设施(如 WLAN 中的 AP,LAN 中的网络接入设备),达到监听、截获、伪造网络数据的目的;通过截获并转发客户端和认证者之间传输的所有数据,实现中间人攻击;等等。

2 认证机制的改进

802.1X 协议最大的缺陷是状态机不完整,缺乏双向认证,以及对消息的完整性和源真实性缺乏保护。本文提出一种改进方案,在不改变原 EAPOL 数据帧格式的基础上,完善了状态机,加强了消息完整性和源真实性保护,提供客户端不

线验证机制,可有效防止会话劫持、重放攻击和中间人攻击,减轻拒绝服务攻击。

2.1 双向挑战握手及下线验证

为改进 802.1X 协议,消除存在的安全问题,提出双向挑战握手及下线验证解决方案。该方案的主要思想是在认证阶段进行双向认证和密钥协商,下线阶段使用密钥进行验证。图 4 描述了该方案的交互过程。图中 PW 是客户端和服务端共享的密钥(用户密码), N_a 、 N_b 、 N_s 分别是 A、B、S 生成的一次性随机数,Flag 为下线标志:客户端主动下线则 Flag 置为 TRUE,认证者强制要求其下线则 Flag 置为 FALSE。虚线箭头表示只有在客户端主动要求下线时才发送 EAPOL-Logoff 帧,此时认证者将回应 EAP-Failure 消息,并在随后发起一次下线确认的会话过程,如果是认证失败或者认证者强制客户端下线,都会在发送 EAP-Failure 消息后发起下线确认。考虑到 EAP 协议的可扩展性,将确认消息封装到 EAP-Request/Response 消息中传递。

从图 4 可知,方案分为认证和下线两个阶段,分析如下。

1) 认证阶段。

本阶段实现对客户端和认证系统(认证者和认证服务器)的双向认证,并由服务器分配共享密钥 Key。首先是对认证者和服务器的认证,由消息(6)完成。由于只有客户端和服务端持有 PW ,故而客户端收到消息(6)以后,经过解密并核对 N_a 的真实性即可完成对服务器的认证。同时,认证服务器是可信第三方,它可以鉴定认证者的身份,故而在消息(6)中包含的 B 信息实现了对认证者身份的鉴定。这里 $PW(N_a, B)$ 等效于 $\text{Hash}\{N_a, S, B, PW\}$,是一个消息鉴别码(Message

表 1 EAP 认证方法对比

认证方法	相互认证	客户端证书	服务器证书	会话密钥派生	用户名保护	认证特点	部署实现	安全性
MD5	否	否	否	否	否	挑战回应	容易	差
TLS	是	是	是	是	否	证书认证	难	高
TTLS/PEAP	是	可选	是	是	是	隧道认证	一般	中等
LEAP	是	否	否	是	否	挑战回应	一般	一般
FAST	是	否	否	是	是	隧道认证	一般	中等

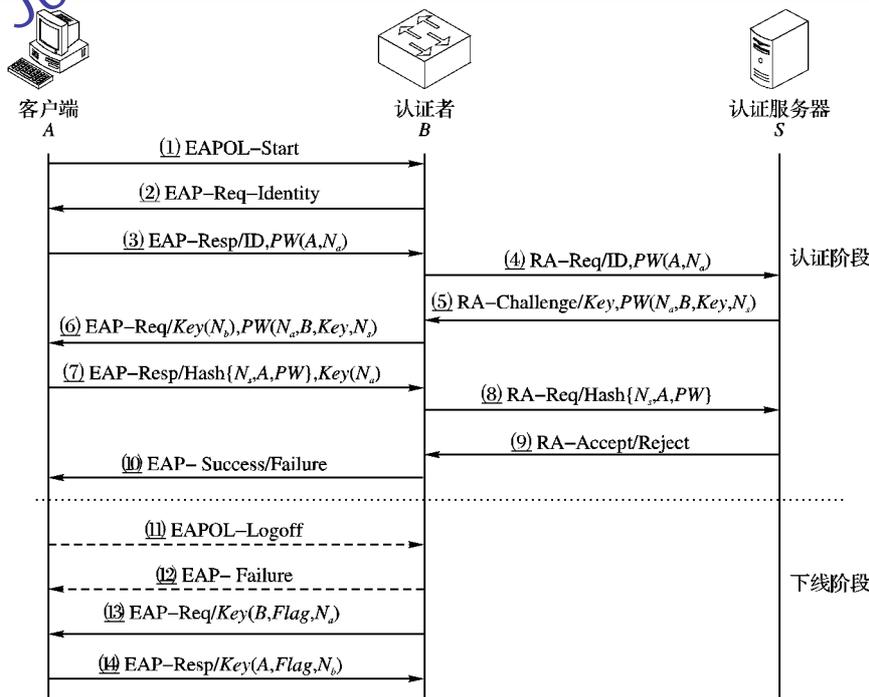


图 4 双向挑战握手和下线验证模型

Authentication Code, MAC)。其次是对客户端的认证,消息(7)完成这一过程,这与标准的挑战握手认证类似。另外,在消息(5)、(6)中实现了客户端与认证者的共享密钥 Key 的分配。

2) 下线阶段。

当客户端主动要求下线而发送 EAPOL-Logoff 帧时,认证者收到后返回 EAP-Failure 消息。接下来认证者发送消息(13),其中 $Flag$ 置为 TRUE。客户端收到后用 Key 解密,检查 B 、 N_c 是否有效,并验证 $Flag$ 是否为 TRUE,如果这三者中任一有误,则丢弃该消息,保持当前端口状态。如果验证无误则返回消息(14),其中的 $Flag$ 同样必须为 TRUE,之后正常下线。认证者接收到消息(14)并验证 A 、 $Flag$ 、 N_s 无误后,将端口断开,如果验证有误则丢弃该消息,保持当前端口状态。

当客户端没有发送 EAPOL-Logoff,而认证者发送 EAP-Failure 强制客户端下线,或者客户端认证失败,认证者在消息(10)中发送 EAP-Failure 时,认证者同样发送消息(13),其中 $Flag$

置为 FALSE,客户端验证 B 、 $Flag$ 和 N_c 的值并返回消息(14),认证者收到后同样进行验证。

2.2 状态机改进

双向挑战握手和下线验证方案改进了客户端和认证者的状态机,重点针对下线过程增加了 CONFIRM 状态、若干计时器和必要的信号量。

2.2.1 客户端 PAE 状态机改进

图 5 表示了改进的客户端状态机系统。在图中仍然用虚线表示信号的传递,在箭头上标注要传递的信号量;实线表示状态的转换,箭头尾端标注状态转换的触发事件。可以看到,客户端后台状态机增加了一个 CONFIRM 状态,伴随其还增加了一个 confirmWhile 计时器,同时对一些状态转换的触发事件做了改进。客户端状态机在 LOGOFF 状态增加了 logoffWhile 计时器。上层协议需检测 logoffSent 信号,发送 logoffConfirm/logoffNotConfirm 信号,并实现下线验证的算法。

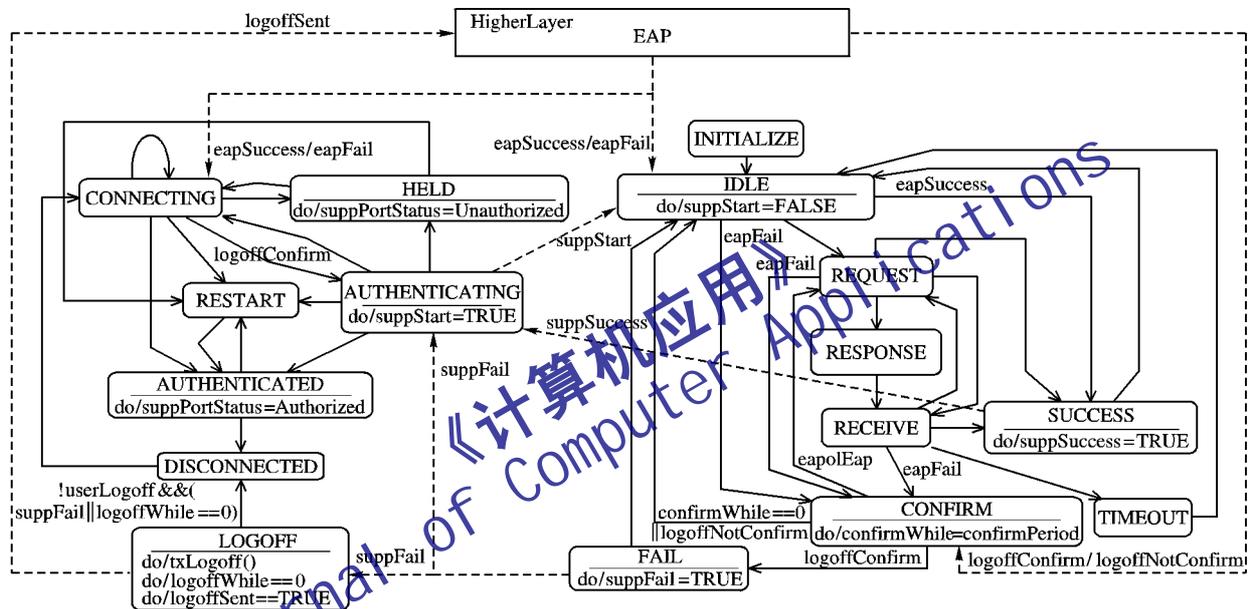


图 5 改进的客户端 PAE 状态机

2.2.2 认证者 PAE 状态机改进

图 6 表示了改进的认证者状态机系统。后台认证状态机增加了一个 CONFIRM 状态,在 FAIL 状态不再执行 txReq() 函数(即发送 EAP-Failure 消息),这个动作在 REQUEST 状态完成。值得注意的是,在检测到上层设置的 eapSuccess/eapFail 信号时,状态机运行与原方案相同,这是因为这里的 eapSuccess/eapFail 是 AAA 服务器发来的 EAPOR 消息经协议栈转换而来的,代表认证服务器的认证或决策信息。接收到 EAPOL-Logoff 帧以后,认证者状态机不再直接转入 DISCONNECTED 状态,而是经过下线验证,并且接收到后台认证状态机给出 authFail 信号后方执行下线。上层协议需接收 logoffRecv 信号,发送 logoffConfirm/logoffNotConfirm 信号,并实现下线验证的算法。

2.3 改进方案的分析

应用本改进方案能有效提高系统的安全性,具有一定的应用价值。体现在如下方面。

1) 攻击者伪造 EAPOL-Logoff 帧发送给认证者,截获到认证者发来的 EAP-Failure 和 EAP-Request 验证消息。然而攻击者没有共享密钥,也没有消息验证随机数,无法伪造随后的验证消息,所以无法通过下线验证,也就不能诱使认证者关闭端口。

2) 攻击者伪造 EAP-Failure 消息发送给客户端,然而没有共享密钥,也没有消息验证随机数,无法伪造随后的 EAP-Request 消息完成下线验证,所以无法诱使客户端关闭端口。

3) 本方案没有改变协议的消息格式,只需对支持 802.1X 的网络设备进行软件升级即可推广应用。

4) 本方案使用对称密钥技术和挑战回应验证,计算速度较快,配置管理方便,因而易于应用部署。

5) 本方案只对客户端和认证者状态机做了较小的改动,各增加了一个状态,以及少量下线验证信息,因而虽对 CPU 负载和存储空间有一定影响,但不会导致系统性能的下降。

6) 802.11i 中定义了强安全网络关联 RSNA,在 802.1X 认证之后有 4 次握手过程动态协商会话密钥,安全性较高。本方案实现较为简便,在认证过程中协商用于下线验证的共享密钥 Key ,但不能对其动态更新,可考虑周期性协商更新共享密钥。

3 对改进方案的形式化验证

3.1 BAN 逻辑介绍

BAN 逻辑是基于知识和信仰的形式逻辑分析方法,通过认证协议运行过程中消息的接收和发送来从最初的信仰逐渐发展为协议运行要达到的目的主体的最终信仰。虽然 BAN

逻辑在密码协议形式化分析领域获得广泛应用,取得了很大的成功,但其原型存在固有的缺陷,无法探测某些对协议的攻击,如:重放攻击、中间人攻击等。

本文为验证改进方案能否有效保护消息完整性、源真实性,采用一种改进的 BAN 逻辑^[10]对其进行分析。文献[10]提出继续沿用 BAN 逻辑的主要符号和推理规则,结合 N-u 理

想化方法,对 BAN 逻辑原型中存在缺陷的推理规则进行了改进,增加了必要的规则,可以有效克服 BAN 逻辑原型无法检测潜在的针对协议的重放攻击、中间人攻击等缺陷,对协议安全性的分析更加准确。本文应用的改进的 BAN 逻辑规则有消息含义规则和仲裁规则,增加了消息可识别规则、保密性规则和可信性规则。

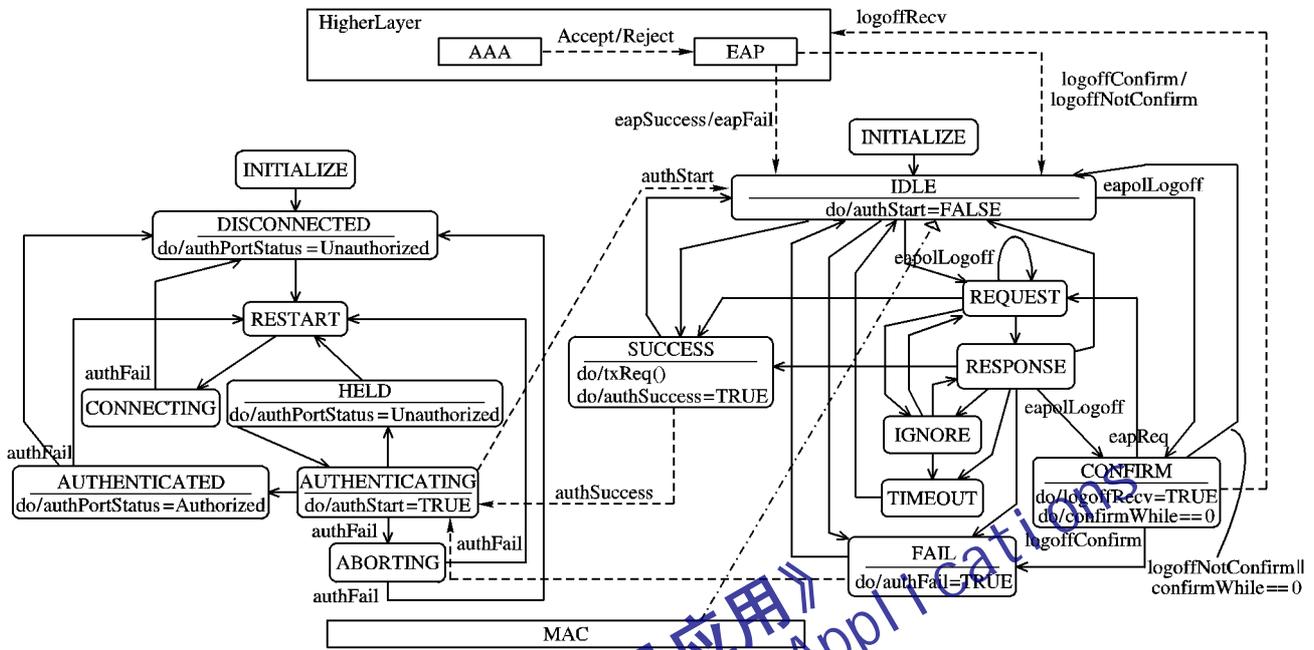


图6 改进的认证状态机

3.2 BAN 逻辑验证

3.2.1 协议描述

对协议进行理想化处理,此过程包括两个阶段。首先应用 N-u 协议理想化规则,确定可在协议形式化描述中使用 $A \xrightarrow{K} B$ 替代 A, B 之间的共享密钥 Key (简记为 K);其次用语法分析器“*”分析协议中 A, B, S 三方发送和接受的消息,确定这些用不同密钥加密的消息中没有结构相同的加密块,依此保证 A, B 相信接收到的消息是可识别的,完成后在每个消息加密块之前标上“*”。

经过上述处理,协议消息序列的形式化描述如下:

$$A \rightarrow B: * \{A, N_a\}_{K_{as}} \quad (1)$$

$$B \rightarrow S: * \{A, N_b, \{A, N_a\}_{K_{as}}\}_{K_{bs}} \quad (2)$$

$$S \rightarrow B: * \{A, S, N_b, A \xrightarrow{K} B, \{N_a, N_b, N_s, B, A \xrightarrow{K} B\}_{K_{as}}\}_{K_{bs}} \quad (3)$$

$$B \rightarrow A: * \{N_a, N_b, N_s, B, A \xrightarrow{K} B\}_{K_{as}}, * \{B, N_b\}_K \quad (4)$$

$$A \rightarrow B: * \{A, N_a, N_b\}_K, HMAC_K(A, N_s) \quad (5)$$

$$B \rightarrow S: * \{A, B, HMAC_K(A, N_s)\}_{K_{bs}} \quad (6)$$

$$B \rightarrow A: * \{B, F, N_a\}_K \quad (7)$$

$$A \rightarrow B: * \{A, F, N_b\}_K \quad (8)$$

消息(1)~(6)是认证过程,消息(7)~(8)是下线验证过程。这里省略了图4中的部分 EAPOR、EAP、EAPOL 消息以及少量明文。

3.2.2 逻辑推理

略过初始化假设。认证的目标为:一级信仰 $A \models A \xrightarrow{K} B, B \models A \xrightarrow{K} B$; 二级信仰 $A \models B \models A \xrightarrow{K} B, B \models A \models A \xrightarrow{K} B$ 。本文以 $A \models A \xrightarrow{K} B$ 和 $A \models B \models A \xrightarrow{K} B$ 为例进行证明,其余两者的证明与之类似。

1) 证明 $A \models A \xrightarrow{K} B$ 。

由仲裁规则可证明,条件是:

<1> $A \models S \models A \xrightarrow{K} B$, 初始化假设。

<2> $A \models S \models A \xrightarrow{K} B$, 临时值验证规则。

<2.1> $A \models \#A \xrightarrow{K} B$, 易证。

<2.2> $A \models S \sim A \xrightarrow{K} B$, 发送规则。

<2.2.1> $A \models S \sim (N_a, N_b, N_s, B, A \xrightarrow{K} B)$, 简记括号内消息为 X , 消息含义规则。

<2.2.1.1> $A \triangleleft * \{X\}_{K_{as}}$, 消息(4)。

<2.2.1.2> $A \models A \xrightarrow{K_{as}} S$, 初始化假设。

<2.2.1.3> $A \models \otimes(X)$, 消息可识别规则。

<2.2.1.3.1> $A \triangleleft * \{X\}_{K_{as}}$, 消息(4)。

<2.2.1.3.2> $A \ni K_{as}$, 初始化假设。

<2.2.1.3.3> $X \supseteq [N_a, B]$, 易证。

2) 证明 $A \models B \models A \xrightarrow{K} B$ 。

由临时值验证规则可证明,条件是:

<1> $A \models \#A \xrightarrow{K} B$, 上文已证。

<2> $A \models B \sim A \xrightarrow{K} B$ 。

消息(4)可以表示为 $A \triangleleft * \{N_a, N_b, N_s, B, A \xrightarrow{K} B\}_{K_{as}}, * \{B, N_b, A \xrightarrow{K} B\}_K$ 。在这条消息中,通过 K 和 K_{as} 绑定了 N_a, N_b, B, K ;此外利用可信第三方证实了发送者 B 的身份,并分配了 A, B 的共享密钥 K 和共享秘密 N_b ,且保证了它们的新鲜性、保密性和真实性。故可将消息(4)表示为 $A \triangleleft * \{N_a, N_b, N_s, B, A \xrightarrow{K} B\}_{K, K_{as}}$ 。由发送规则和消息含义规则可证 <2>,如下。

<2.1> $A \triangleleft * \{N_a, N_b, N_s, B, A \xrightarrow{K} B\}_{K, K_{as}}$, 消息(4)。

<2.2> $A \models A \xrightarrow{K} B, A \models A \xrightarrow{K_{as}} S$, 已证。

<2.3> $A \models \otimes \{N_a, N_b, N_s, B, A \xrightarrow{K} B\}_{K, K_{as}}$, 消息可识

别规则。

<2.3.1> $A \triangleleft * \{N_a, N_b, N_s, B, A \xleftarrow{K} B\}_{K, K_{as}}$, 消息(4)。

<2.3.2> $A \ni K, K_{as}$, 初始化假设。

<2.3.3> $(N_a, N_b, N_s, B, A \xleftarrow{K} B) \supseteq [N_a, B]$, 易证。

经逻辑推理,成功证得了一级信仰和二级信仰,因而改进方案的安全性得到验证。由此得出结论:本方案是安全的。

4 结语

本文对当前广泛应用的 802.1X 协议进行了深入分析,从状态机出发揭示其存在安全缺陷及产生这些问题的根源。在不改变原协议报文格式的基础上,提出一种改进方案,重点针对客户端下线过程进行改进,提出在认证过程中协商共享密钥,并用其进行下线验证。随后运用一种改进的 BAN 逻辑对方案进行了形式化验证。经验证,该方案可完善协议状态机系统,保护消息完整性和源真实性,抵御多种安全威胁。由于引入了新的状态,是否会对系统性能及安全性产生较大影响,尚待进一步研究。

参考文献:

[1] JEFFREE T, CONGDON P, SALA D, *et al.* 802.1X-2004: IEEE standard for local and metropolitan area networks-port-based network access control [S]. Piscataway, NJ: LAN/MAN Standards Committee of the IEEE Computer Society, 2004.

[2] MISHRA A, ARBAUGH W A. An initial security analysis of the IEEE 802.1X standard, collection CS-TR-4328[R]. Maryland: University of Maryland, Computer Science Department, 2002: 7-10.

[3] HE C H. Analysis of security protocols for wireless networks [D]. California: Stanford University, Department of Electrical Engineering, 2005: 14-45.

[4] 李永强,汪海航. 针对 802.1X-EAP 安全认证协议的中间人攻击[J]. 计算机工程, 2008, 34(22): 192-197.

[5] 朱加伟,周颖,赵保华. 基于状态机的 802.1X 协议攻击检测方法[J]. 西安交通大学学报, 2010, 44(4): 52-56.

[6] 周贤伟,刘宁,覃伯平. IEEE 802.1X 协议的认证机制及其改进[J]. 计算机应用, 2006, 26(12): 2894-2896.

[7] ABOBA B, BLUNK L, VOLLBRECHT J, *et al.* RFC 3748-2004, Extensible Authentication Protocol (EAP) [S]. Piscataway, NJ, USA: IETF, 2004.

[8] SANKAR K, SUNDARALINGAM S, BALINSKY A, *et al.* Cisco wireless LAN security [M]. Indianapolis: Cisco Press, 2004: 170-192.

[9] CHEN J C, WANG Y P. Extensible Authentication Protocol (EAP) and IEEE 802.1X: tutorial and empirical experience [J]. IEEE Communications Magazine, 2005, 43(12): 27-31.

[10] 王亚弟,束妮娜,韩继红,等. 密码协议形式化分析[M]. 北京:机械工业出版社, 2006: 38-58.

(上接第 1229 页)

是最低的,说明此时损失了源图中很多的有用信息。而本文的方法却具有很好的稳定性,在去云的同时更好地保留了原始图像的细节信息。

系数和近似系数分别进行适度地加权,这样既有效地去除了云层又有效地保留了图像的细节,合理地突出了景物信息。通过与同态滤波和文献[4]中的方法做对比实验发现,本文提出的方法无论从视觉效果还是客观评价指标上都是最优的。

表 1 去云效果的客观评价

算法	图像均值 (源图为 112.1)	对比度 (源图为 32.381)	梯度 (源图为 9.688)	信息熵 (源图为 3.63)
云区阈值法	90.961	30.626	12.134	3.5000
同态滤波算法	103.550	20.701	9.355	3.0100
本文算法	100.850	24.262	11.766	6.9806

表 2 去云效果的客观评价

算法	图像均值 (源图为 139.9)	对比度 (源图为 31.338)	梯度 (源图为 5.466)	信息熵 (源图为 3.51)
云区阈值法	116.73	28.668	6.80	5.79
同态滤波算法	103.30	20.501	5.47	2.94
本文算法	131.54	20.758	6.84	6.36

参考文献:

[1] 李刚. 卫星遥感图像薄云去除技术研究[D]. 成都: 成都理工大学, 2007.

[2] 王恒进. 基于小波的遥感图像薄云去除的研究与实现[D]. 西安: 西北工业大学, 2002.

[3] 李刚, 杨武年, 翁韬. 一种基于同态滤波的遥感图像薄云去除算法[J]. 测绘科学, 2007, 32(3): 47-48.

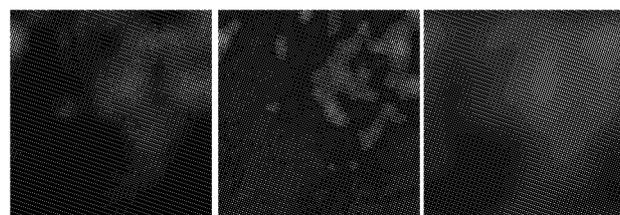


图 7 Spot 5 图像去云后的残差图像比较

3 结语

分析小波变换各层系数频率的关系,通过选择合理的分界层数将云信息和图像背景信息以及图像细节信息较好地分离,使得云噪声主要存在于高层细节系数中。然后再利用同态滤波的方法去除高层细节系数中的云噪声。同时对高、低层细节

[4] 朱锡芳,吴峰,陶纯堪. 基于小波阈值理论的光学图像去云处理新算法[J]. 光子学报, 2009, 38(12): 3312-3317.

[5] 朱锡芳,吴峰,庄燕滨. 基于 Mallat 算法遥感图像去云雾处理的改进方法[J]. 遥感学报, 2007, 11(2): 241-246.

[6] 樊厚春. 遥感图像薄云去除研究[D]. 北京: 中国科学院研究生院, 2004.

[7] 朱锡芳,陶纯堪. 一种用于遥感图像去云雾处理的小波系数加权算法[J]. 微电子学与计算机, 2008, 25(11): 141-145.

[8] WANG Z, BOVIK A C, SHEIKH H R, *et al.* Image quality assessment: From error visibility to structural similarity[J]. IEEE Transactions on Image Processing, 2004, 13(4): 600-612.

[9] 王涛,高新波,张都应. 一种基于内容的图像质量评价测度[J]. 中国图象图形学报, 2007, 12(6): 1002-1007.

[10] MAALOUF A, CARRE P, AUGEREAU B, *et al.* A bandelet-based inpainting technique for clouds removal from remotely sensed images [J]. IEEE Transactions on Geoscience and Remote Sensing, 2009, 47(7): 2363-2371.