第8章 网络安全协议

罗文坚

主要内容

- 8.1 概述
- 8.2 IPSec
- 8.3 SSL
- 8.4 安全电子交易协议

概述

- 许多网络攻击都是由网络协议（如TCP/IP）的固有漏洞引起的，因此，为了保证网络传输和应用的安全，各种类型的网络安全协议不断涌现。

- 安全协议是以密码学为基础的消息交换协议，也称作密码协议，其目的是在网络环境中提供各种安全服务。

- 安全协议是网络安全的一个重要组成部分，通过安全协议可以实现实体认证、数据完整性校验、密钥分配、收发确认以及不可否认性验证等安全功能。

网络安全协议层次

- 网络安全协议基本上与TCP/IP协议族相似，分为四层，即网络接口层、网络层、传输层和应用层。
  - 应用层：种类繁多（SSH、PGP和SET）；
  - 传输层：SSL、TLS和SOCKS v5等；
  - 网络层：IPSec协议（IP Security）；
  - 网络接口层：L2TP 、L2F、PPTP。

- 网络安全协议建立在密码体制基础上，运用密码算法和协议逻辑来实现加密和认证。
  - 密钥管理主要分为人工管理和协商管理两种形式。
  - 密钥管理都需要通过应用层服务来实现。
  - 网络安全协议所处的网络层次不同，存在包含关系，但存在特殊应用的情况除外。

主要内容

- 8.1 概述
- 8.2 IPSec
  - 8.2.1 IPSec协议族的体系机构
  - 8.2.2 IPSec协议的工作方式
  - 8.2.3 Internet秘钥交换协议
- 8.3 SSL
- 8.4 安全电子交易协议

IPSec

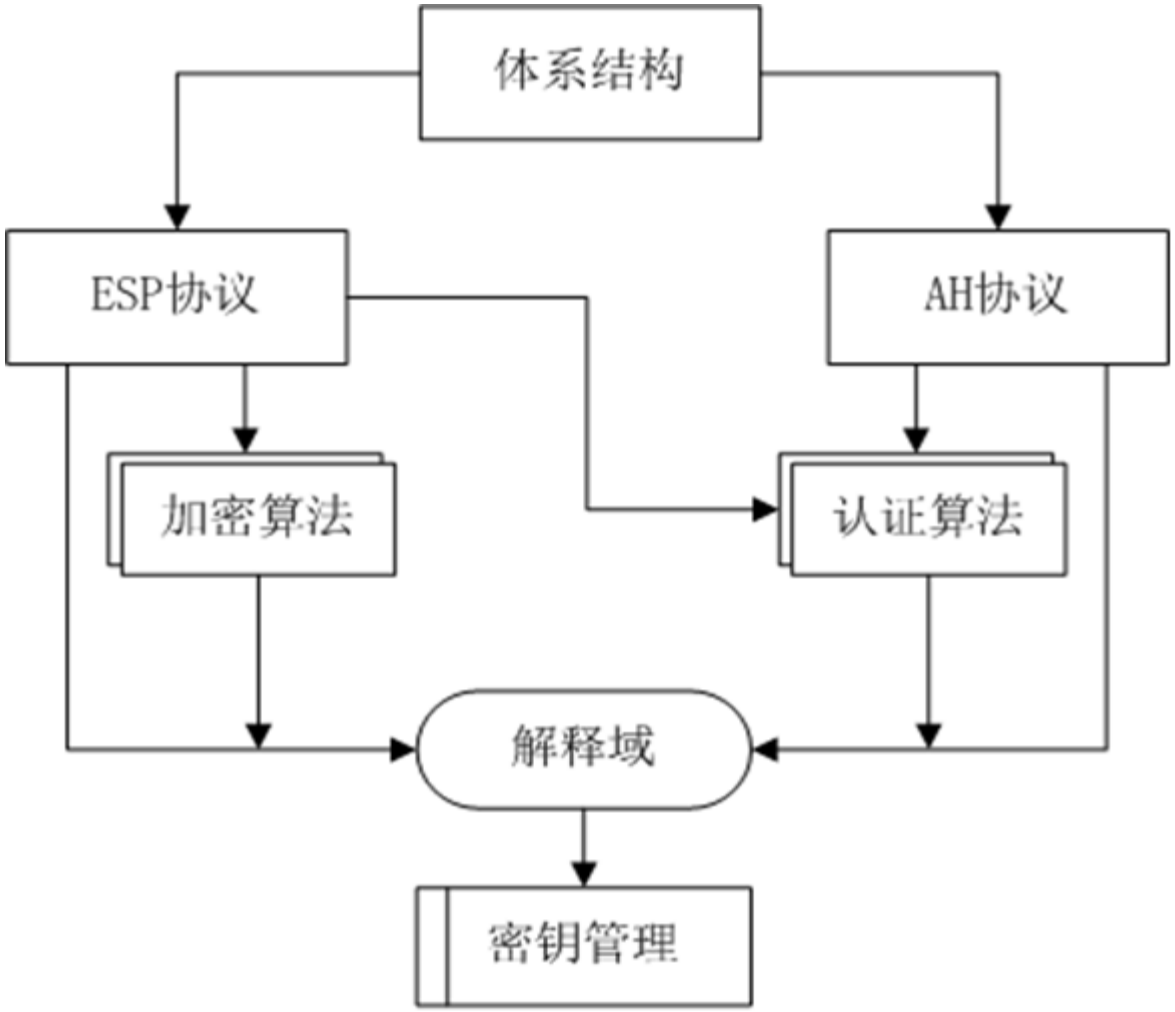
- 1994年，IAB（Internet Architecture Board），发表《互联网体系结构中的安全问题》报告。
- 1994年，IETF专门成立IP安全协议工作组。
- 1995年，IPSec细则在互联网标准草案中颁布。
- 1998年11月，被提议为IP安全标准。

- IPSec是一个标准的第三层安全协议族；不是一个协议，而是一个协议簇。
- IETF为IPSec一共定义了12个标准文档RFC（Request For Comments）。
- IPSec对于IPv4是可选的，对于IPv6是强制性的。
- IPSec提供了一种标准的、健壮的以及包容广泛的机制，可用它为IP及上层协议（如UDP和TCP）提供安全保证。

IPSec协议的优点

- IPSec在传输层之下，对于应用程序是透明的。
- IPSec对终端用户是透明的，因此不必对用户进行安全机制的培训。
- IPSec可以为个体用户提供安全保障，可以保护企业内部的敏感信息。

IPSec协议族的体系结构



- **Encapsulating Security Payload（ESP，封装安全有效负载协议）**
- **Authentication Header（AH，认证头协议）**

基本协议

- **ESP（Encapsulating Security Payload）协议**
  - 对IP数据报文实施加密和可选认证双重服务
  - 提供了数据保密性、有限的数据流保密性、数据源认证、无连接的完整性以及抗重放攻击等服务。

- **AH（Authentication Header）协议**
  - 对IP数据报文实施认证服务，提供数据源认证、无连接的完整性以及一个可选的抗重放服务。
  - AH协议通过对IP数据包进行签名以确保其完整性，虽然数据包的内容没有加密，但是可以向接收者保证数据包的内容未被更改，还可以向接收者保证包是由发送者发送的。

基本协议

- AH协议和ESP协议都支持认证功能，但二者的保护范围存在着一定的差异。
  - AH的作用域是整个IP数据包，包括IP头和承载数据。
  - ESP认证功能的作用域只是承载数据，不包括IP头。

- 从理论上讲，AH所提供的认证的安全性高于ESP的认证服务。

- ESP和AH的有效工作依赖于四个要件。
  - 加密算法、认证算法、解释域DOI（Domain of Interpretation）以及密钥管理。
  - 实际应用中，这些要件都是以程序或程序包的形式出现。

IPSec基本要件

①加密算法

- 描述各种能用于ESP的加密算法。
- IPSec要求任何实现都必须支持DES（数据加密标准），也可使用3DES、IDEA(国际加密算法)、AES(高级加密算法)等其他算法。

②认证算法

- 用于AH和ESP，以保证数据完整性及进行数据源身份认证。
- IPSec用HMAC-MD5和HMAC-SHA-1作为默认认证算法，同时也支持其他认证算法，以提高安全强度。

IPSec基本要件

③ 解释域DOI(Domain of Interpretation)

- DOI是一个描述IPSec所涉及到的各种安全参数及相关信息的集合。
- 通过对DOI的访问，可以得到相关协议中各字段含义的解释，可以被与IPSec服务相关的系统参考调用。

④ 密钥管理

- 密钥管理主要负责确定和分配AH和ESP中加密和认证使用的密钥，有手工和自动两种方式。
- IPSec默认的自动密钥管理协议是IKE(Internet Key Exchange)。

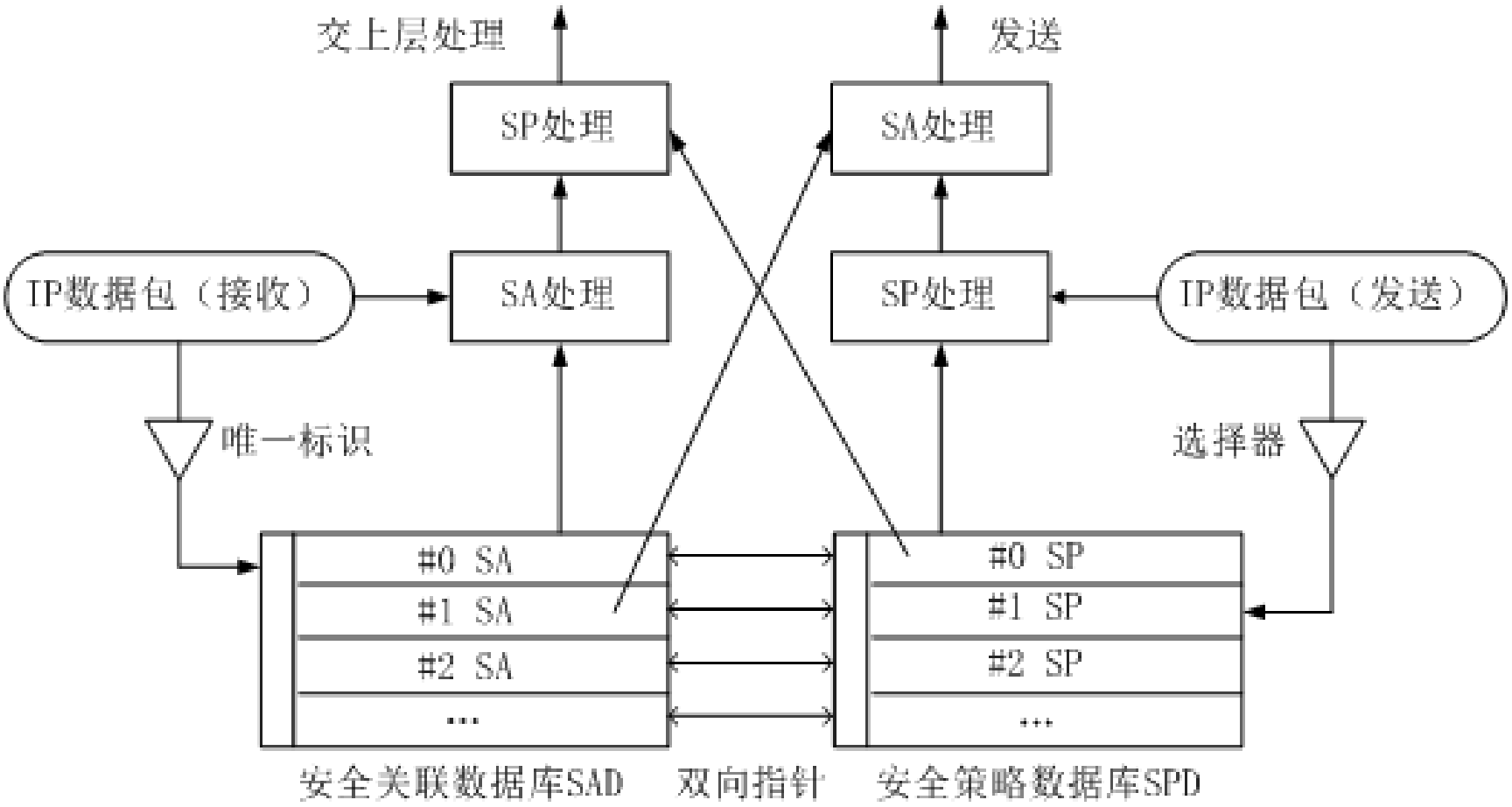
安全关联

- 安全关联SA（Security Association）是一个IPSec单向连接所涉及的安全参数和策略的集合。
  - 决定了保护什么、如何保护以及谁来保护通信数据；
  - 规定了用来保护数据包安全的IPSec协议类型、协议的操作模式、加密算法、认证方式、加密和认证密钥、密钥的有效存在时间以及防重放攻击的序列号等。
  - AH和ESP均使用SA，而且IKE协议的一个主要功能就是建立和维护SA；
  - 一个SA定义了两个应用实体（主机或网关）间的一个单向连接；如果需要双向通讯，则需要建立两个SA。

安全关联SA的工作原理

- 在SA对IP数据包处理的过程中，有两个重要的数据库起到了关键作用。
  - 安全策略数据库（SPD，Security Policy Database）：保存着定义的处理策略，每条策略指出以何种方式对IP数据报文提供何种服务。
  - 安全关联数据库（SAD，Security Association Database）：保存应用实体中所有的SA。

安全关联SA的工作原理



安全关联SA的工作原理

- SAD中的SA是通过三元组<安全参数索引，IP目的地址，安全协议标识>来标识。
  - SPI（Security Parameter Index）：是一个与SA相关联的位串。一般在IKE 确立一个SA时，产生一个伪随机导数作为该SA的SPI。SPI 也可以人为设定。
  - IP目的地址：目前IPSec仅支持使用单播地址来表示SA的目的地址。
  - 安全协议标识：标识该SA是一个AH或ESP协议的安全关联。

- SPD中的SP是通过选择因子来确定的。
  - 选择因子是从网络层和传送头内提取出来的，主要包括：目的地址、源地址、名字、协议、上层端口等。

SPD

- 安全策略数据库SPD 是SA处理的核心之一，每个IPSec实现必须具有管理接口，允许用户或系统管理员管理SPD。

- SPD有一个排序的策略列表，针对接收数据和发送数据有不同的处理策略。

- SPD的处理方式主要有三种：
  - Discard；
  - Bypass IPSec；
  - Apply IPSec。

SAD

- SAD中的任意SA都被定义了以下参数（即SAD的字段）：
  - 目的IP地址：目前的SA管理机制只支持单播地址的SA。
  - IPSec协议：标识SA用的是AH还是ESP。
  - SPI：32比特的安全参数索引，标识同一个目的地的不同的SA。
  - 序号计数器：32比特，用于产生AH或ESP头的序号，仅用于发送数据包。
  - 序号计数器溢出标志：标识序号计数器是否溢出。
    - 如溢出，产生审计事件，禁止用SA继续发送数据包。
  - 抗重放窗口：32比特计数器，用于决定进入的AH或ESP数据包是否为重发，仅用于接收数据包。
  - AH信息：指明认证算法、密钥、密钥生存期等与AH相关的参数。

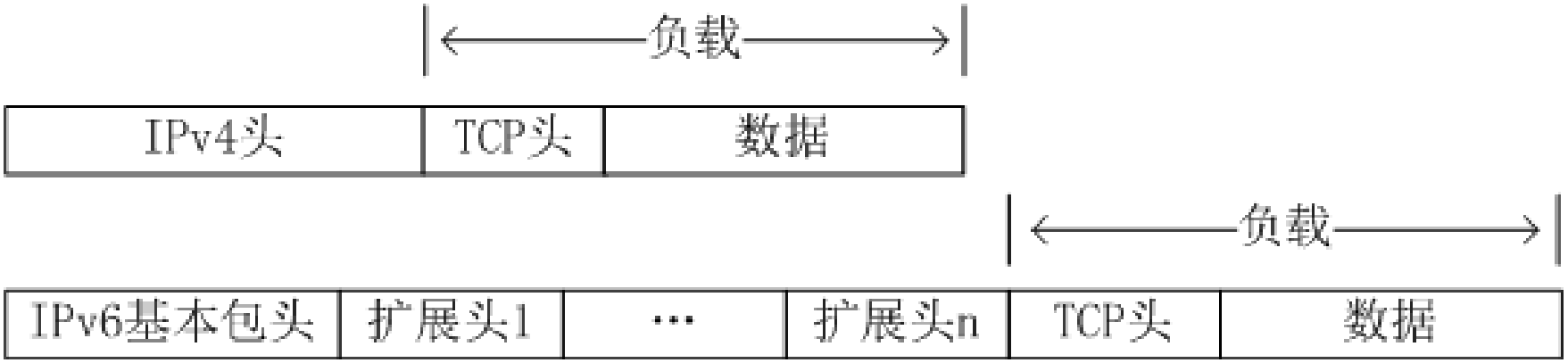
SAD

- SAD中的任意SA都被定义了以下参数（即SAD的字段）：
  - ……
  - ESP信息：指明加密和认证算法、密钥、初始值、密钥生存期等与ESP相关的参数。
  - SA的生存期：一个特定的时间间隔或字节计数。
  - IPSec协议模式：指明是隧道、传输或混合方式（通配符），这些内容后面讨论。
  - Path MTU（路径最大传输单元）：指明预计经过路径的MTU及延迟变量。

主要内容

- 8.1 概述
- 8.2 IPSec
  - 8.2.1 IPSec协议族的体系机构
  - 8.2.2 IPSec协议的工作方式
  - 8.2.3 Internet秘钥交换协议
- 8.3 SSL
- 8.4 安全电子交易协议

IPv4与IPv6数据包结构



- IPv6增加了扩展头，其原理为：大多数IP包只需要简单的处理，因此有基本报头的信息就足够了。当网络层存在需要额外信息的信息包时，就可以把这些信息编码到扩展报头上。

- 在实施IPSec时，IPv4和IPv6存在着一些区别，主要集中在对两种协议数据包的封装上。

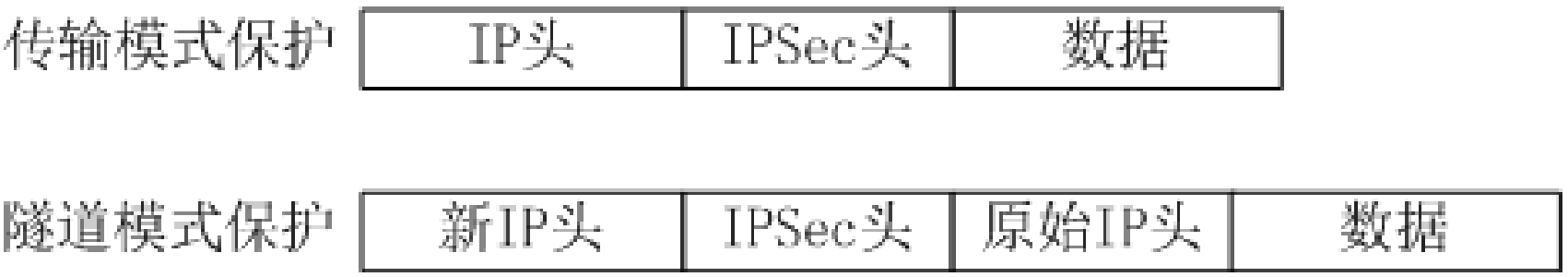
IPv4与IPv6数据包结构

a、IPv4报头

b、IPv6报头

IPSec的工作模式

- IPSec 标准定义了 IPSec 操作的两种不同模式：
  - 传输模式（Transport Mode）和隧道模式（Tunnel Mode）；
  - 安全协议AH和ESP，都可以以这两种模式工作。

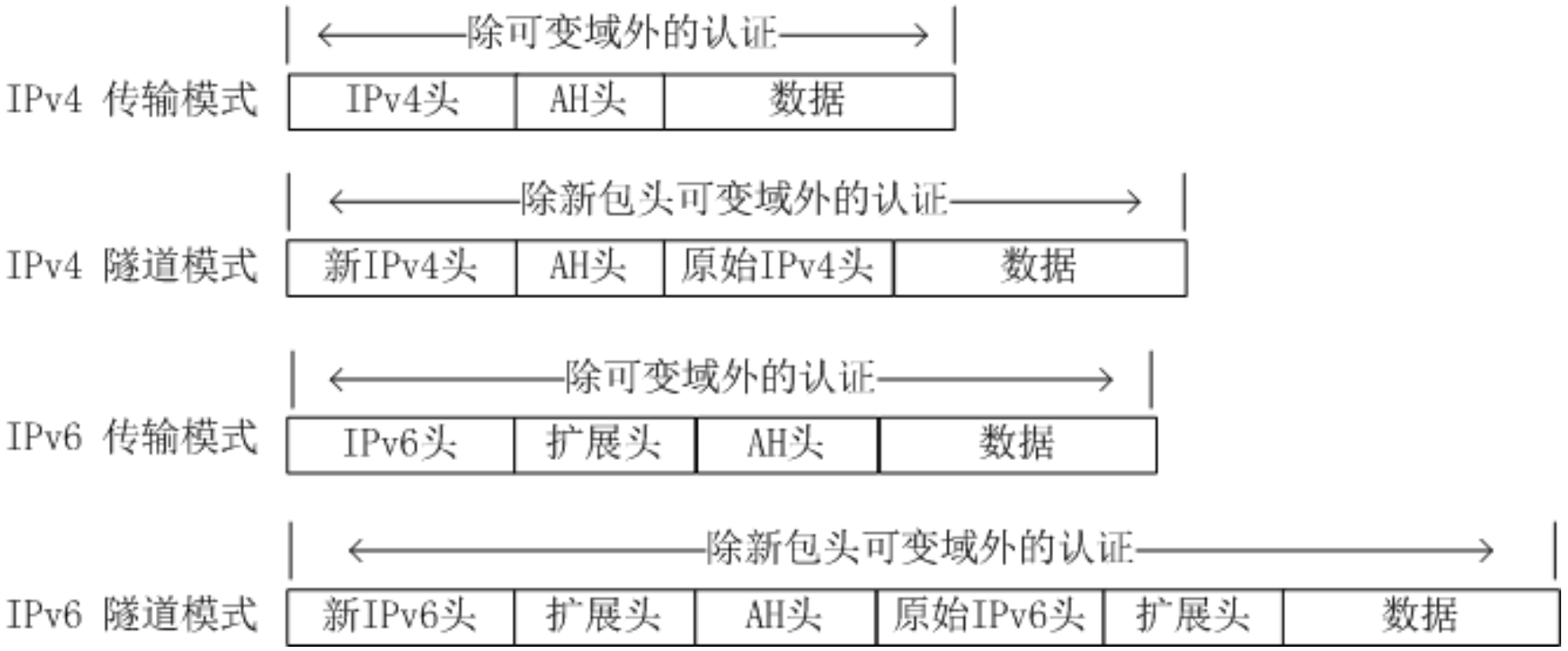


- 传输模式：只对IP数据包的有效负载进行加密或认证；继续使用以前的IP头部，只对IP头部的部分域进行修改。

- 隧道模式：对整个IP数据包进行加密或认证；需要新产生一个IP头部，IPSec头部放在新产生的IP头部和以前的IP数据包之间。

认证头AH

- AH的工作原理：可变内容一般被填充“0”后参与计算。
- 目前计算认证数据的算法主要有MD5算法和SHA-1算法等。



AH头格式

- 下一个头（8位）：用来标记下一个扩展头的类型；
- 载荷长度（8位）：表示认证头数据的长度减2，以字（字长32位）来计；
- 保留（16位）：备用；
- SPI（32位）：用来标识安全关联；
- 序列号（32位）：收发双方同时保留一个序列号计数器，每收发一个IP包，序列号将递增1，当递增到2^{32}后复位；
- 认证数据（32N位）：认证数据域的长度可变，但必须是32的整数倍，默认为3个字（96位）。

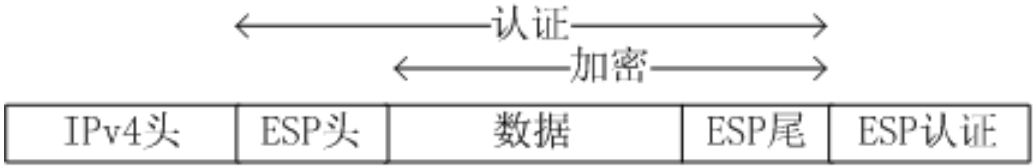
AH头格式

- 认证数据也称为完整性校验值（Integrity Check Value，ICV），是一种报文认证编码MAC或MAC算法生成的截断码。

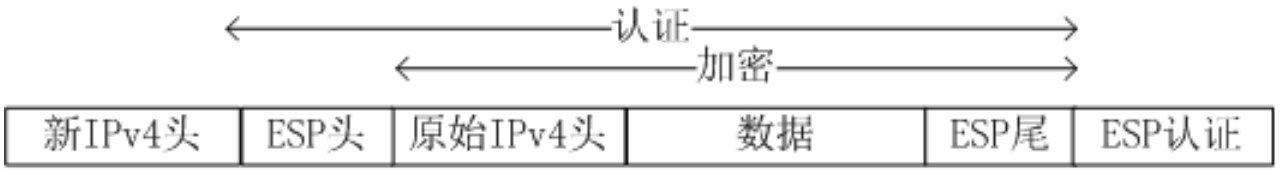
- 认证数据的计算主要使用基于秘钥的Hash算法的认证协议（Hash Message Authentication Code，HMAC），常用的包括HMAC-MD5-96和HMAC-SHA-1-96。
  - 这两种算法是先进行散列计算，然后截取前96位作为ICV。
  - 参与散列计算的数据包括IP包头（可变部分被置为0）、AH头（认证数据被置为0）和整个上层协议数据。

封装安全有效负荷ESP

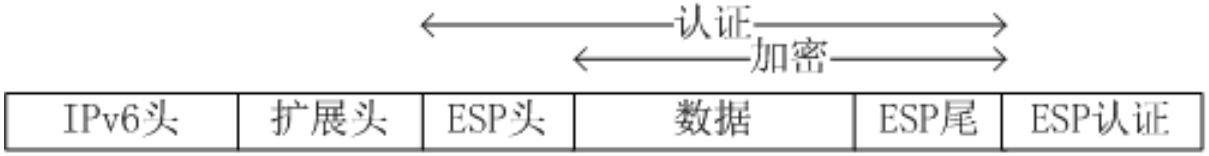
- 工作方式分传输模式和隧道模式。



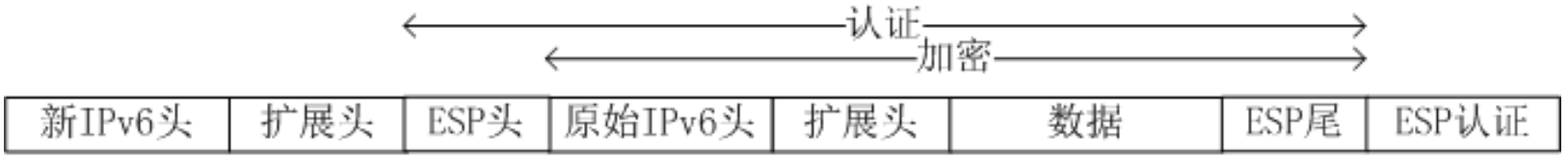
（a）IPv4 传输模式



（b）IPv4 隧道模式

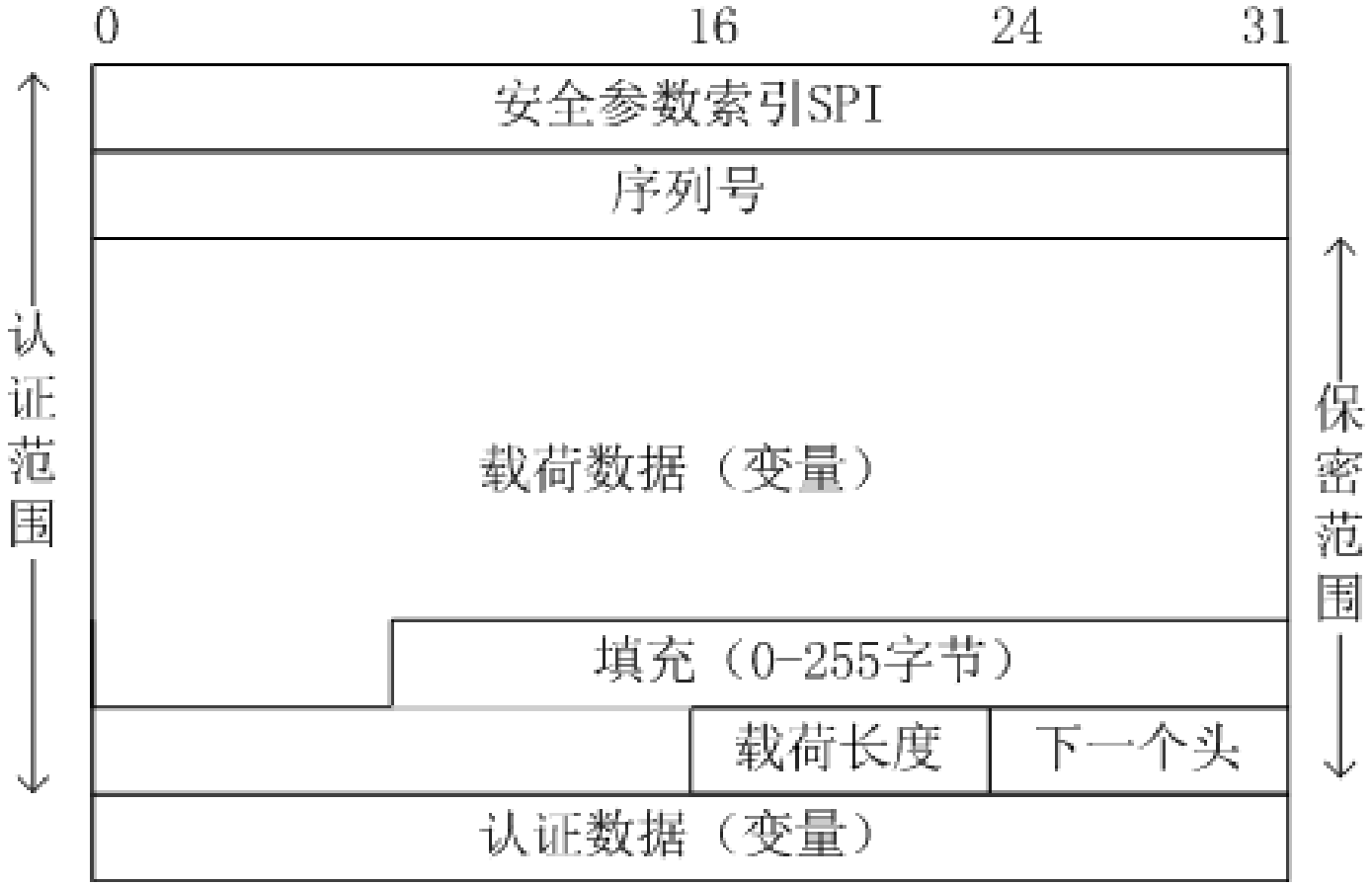


（c）IPv6 传输模式



（d）IPv6 隧道模式

ESP的封装格式



- 传输模式：需对IP数据包的负载部分进行有效填充，并添加ESP尾，构造成长度为字长整数倍的规整数据块。
- 隧道模式：需对整个原始IP数据包进行有效填充。

ESP的封装格式

- ESP封装包主要包括七个部分：
  - 安全关联索引：用来标识安全关联；
  - 序列号：与AH相同，用来防范IP包的重放攻击；
  - 载荷数据：被加密的传输层数据（传输模式）或整个原始IP包（隧道模式）；
  - 填充域：提供规整化载荷数据，并隐藏载荷数据的实际长度；
  - 填充长度：填充数据的长度；
  - 下一个头：用来标记载荷中第一个包头的类型，具体值与AH相同；
  - 认证数据：针对ESP包中除认证数据域外的内容进行完整性计算，得到的完整性校验值，具体计算方法与AH相同。

重放攻击

- 重放攻击是指攻击者发送一个目的主机已接收过的包，对目标系统进行欺骗，主要用于身份认证过程。

- 重放攻击主要分为：
  - 简单重放攻击：攻击者简单地复制一条消息，以后再重新发送它；
  - 反向重放攻击：攻击者复制一条消息，只修改源/目的地址，然后反向发送给消息源（消息发送者）。

- 除了提供加密和认证服务，IPSec安全体制还考虑了反重放攻击问题。

重放攻击

- 由于IP是无连接、不可靠的服务，协议本身不能保证数据包按顺序传输，也不能保证所有数据包均被传输，这就为重放攻击提供了条件。

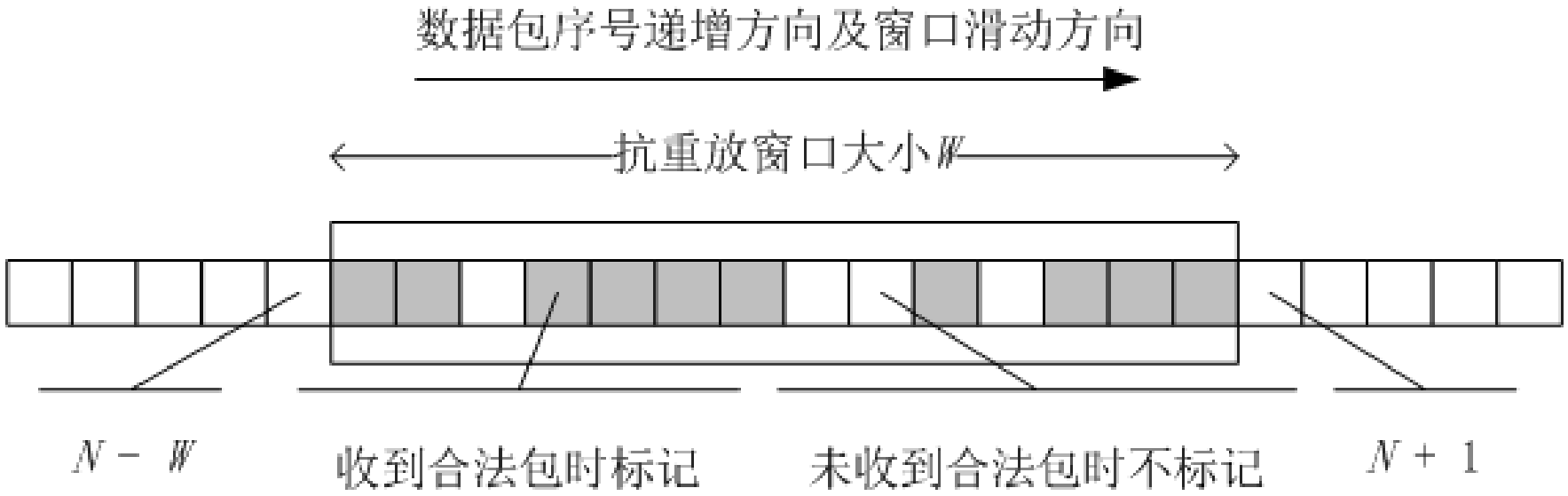
- 抵御重放攻击主要方法包括：
  - 序列号：使用一个序列号来给每一个消息报文编号，仅当收到的消息序数顺序合法时才接受；
  - 时间戳（Timestamp）：A接受一个消息，仅当该消息包含一个时间戳，该时间戳足够接近当前时间时才接受；
  - 盘问/应答方式（Challenge/Response）： A期望从B获得一个新消息，首先发给B一个临时值（Challenge），并要求后续从B收到的消息（Response）包含正确的临时值或对其正确的变换值。

反重放攻击服务

- IPSec使如何防范重放攻击的？
  - 在安全关联SA中定义了序号计数器和抗重放窗口。
- 序号计数器提供了设置IPSec包中序列号域的值。
- 当新SA建立后，发送方将序号计数器的初值置为0，每发送一个包，计数器的值加1并并置于序列号域中，直至$2^{32}-1$。
- 如需提供抗重放服务，则发送方不允许重复计数。当序列号达到2^{32}时，原SA必须终止，并产生新的SA继续工作。

抗重放窗口

- 抗重放窗口W实际上就是某个特定时间接收到的数据包序号是否合法的上、下界，同时窗口具有滑动功能。



主要内容

- 8.1 概述
- 8.2 IPSec
  - 8.2.1 IPSec协议族的体系机构
  - 8.2.2 IPSec协议的工作方式
  - 8.2.3 Internet秘钥交换协议
- 8.3 SSL
- 8.4 安全电子交易协议

Internet密钥交换协议

- IPsec在提供认证或加密服务之前，必须针对安全协议、加密算法和密钥等内容进行协商，并建立SA，这个过程可以手工进行和自动完成。

- IPSec默认的自动密钥管理协议是Internet密钥交换协议IKE（Internet Key Exchange）。

- IKE是一个多用途的安全信息交换管理协议，被定义为应用层协议，主要用于安全策略协商以及加密认证基础材料的确定。
  - SNMPv3、OSPFv2及IPSec等都采用IKE进行密钥交换。
  - IKE是3个协议的混合体，这三个协议分别是ISAKMP、Oakley和SKEME。

Internet密钥交换协议

- ISAKMP（Internet Security Association and Key Management Protocol）设计了一个用于通信双方完成认证和密钥交换的通用框架，在此框架下可以协商和确定各种安全属性、密码算法、安全参数、认证机制等，这些协商的结果统称为安全关联SA。

- Oakley算法是一种以Diffie-Hellman算法为基础的自由形态的协议，允许他人依据本身的需要来改进协议状态。
  - IKE在Oakley基础上，进行有效的规范化，形成了可供用户选择的多种密钥交换模式。

- SKEME（Secure Key Exchange Mechanism）采用公开密钥加密的手段来实现匿名性、防抵赖和密钥更新等服务，可以提供密码生成材料技术和协商共享策略。

IKE

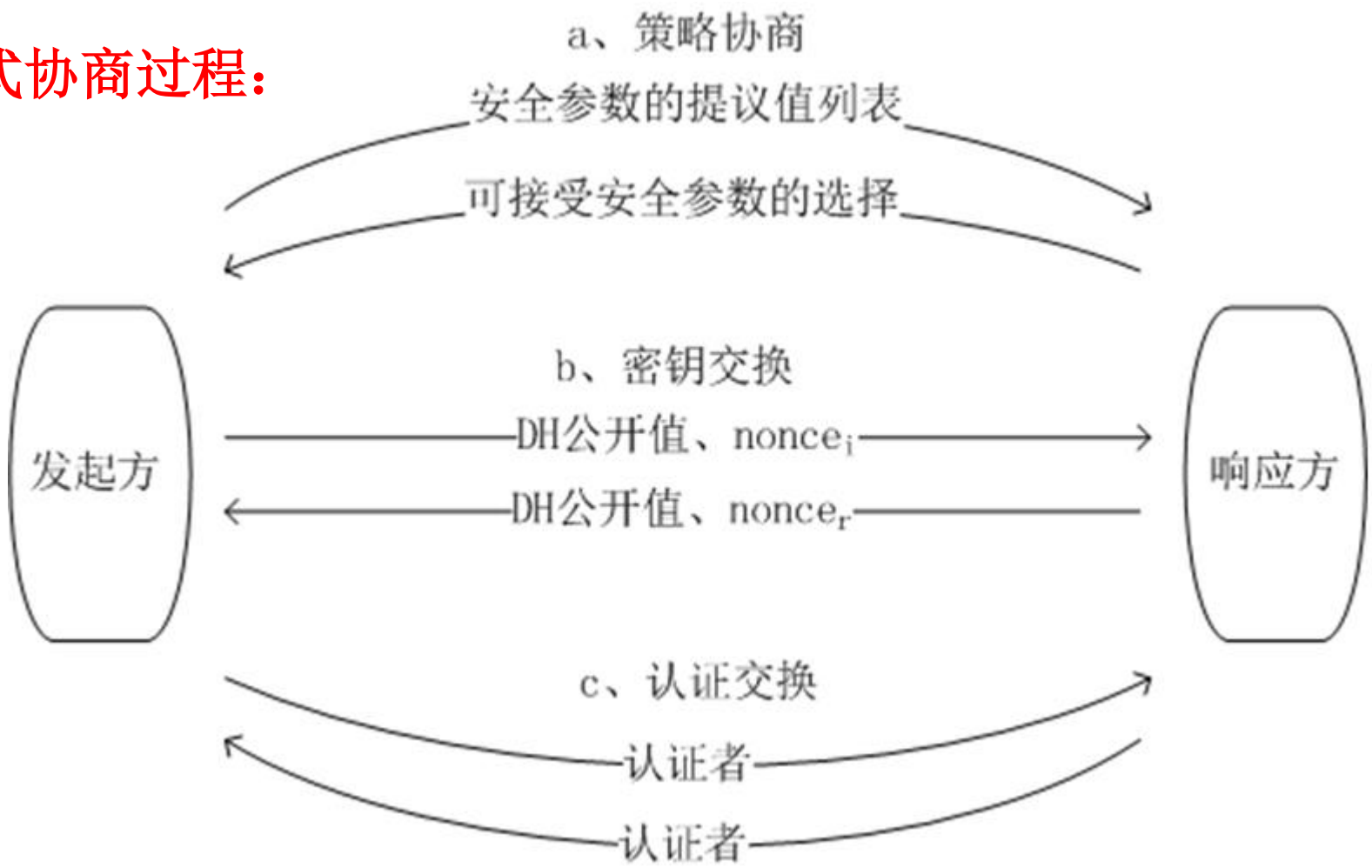
- IKE对IPSec的支持就是在通信双方之间，建立起共享安全参数及密钥（即安全关联SA）。

- IKE建立SA的过程分为两个阶段：
  - 第一阶段，协商创建一个通信信道（IKE SA），并对该信道进行验证，为双方进一步的IKE通信提供机密性、消息完整性以及消息源验证服务；
  - 第二阶段，使用已建立的IKE SA建立IPsec SA。

- 当两个实体间进行IPSec连接时：
  - 如果已经创建了IKE SA，就可以直接通过第二阶段，交换创建新的IPsec SA；
  - 如果还没有创建IKE SA，就要通过两个阶段交换创建新的IKE SA及IPsec SA。

第一阶段

- IKE定义了两种信息交换模式：主模式（Main Mode）、野蛮模式（Aggressive Mode）。
- 主模式协商过程：



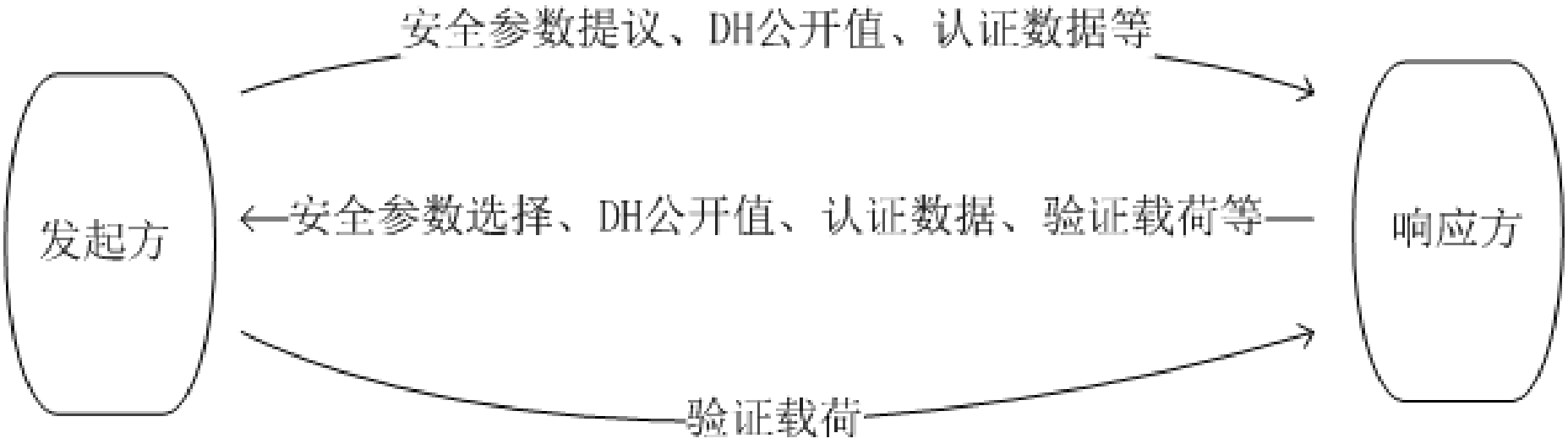
主模式协商过程

- 第一步：策略协商，即确定IKE SA中所必需的有关算法和参数，包括加密算法、散列算法、认证方法以及DH组的选择。

- 第二步，秘钥交换，即双方交换DH算法所需要的秘钥生成基本材料，即DH公开值g^x，还有用于防范重放攻击的一次性随机数nonce 。
  - 随后，各自计算主秘钥。

- 第三步，认证交换，即通信双方构造“认证者”并发给对方；验证通过，则成功建立IKE SA。
  - 认证者是通信双方使用前两步协商得到的秘钥对双方交换的信息进行散列计算得到的散列值（或经过数字签名）。
  - 双方交换的信息包括DH公开值、Nonce、SA内容以及身份标识符ID等。

野蛮协商过程



野蛮模式协商过程

- 验证载荷是使用协商得到的安全参数及秘钥对接收到的所有信息进行加密散列计算，得到的数据结果即为可验证信息，可作为发送方现场操作的证据。

第二阶段

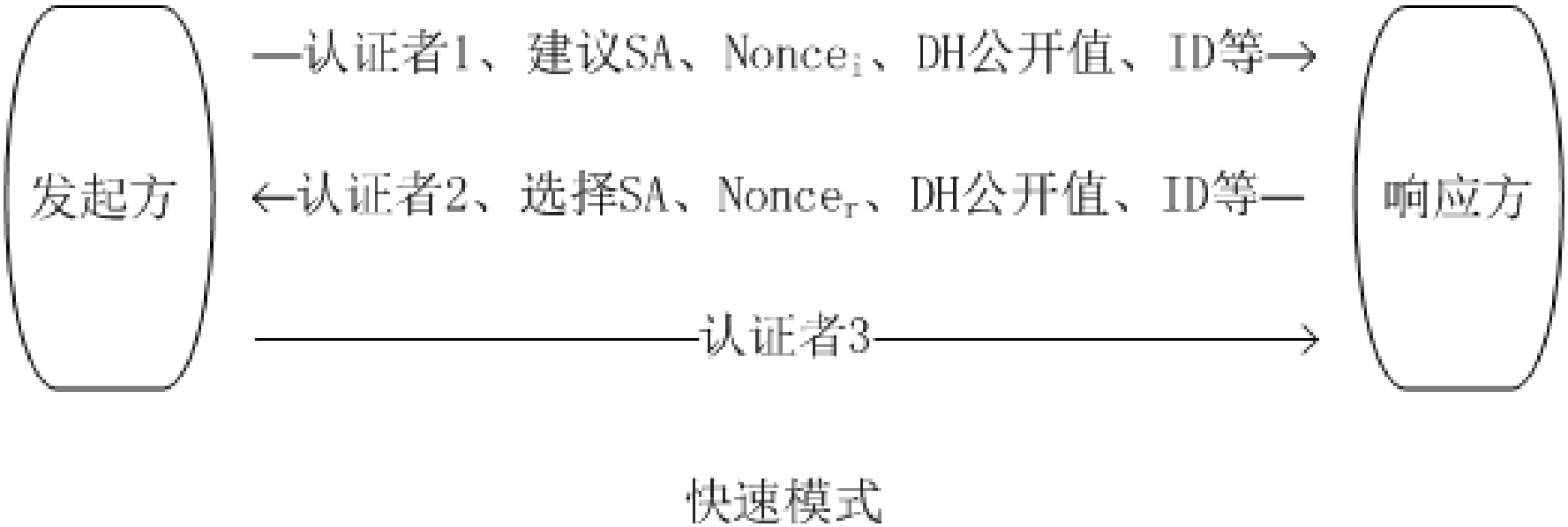
- IKE已经拥有了第一阶段建立起的IKE SA，通信双方的进一步协商采用SA保护，任何没有SA保护的消息将被拒收。

- 通常在第二阶段至少要建立两条SA，一条用于发送数据，一条用于接收数据。

- 此阶段IKE使用三种信息交换方式：
  - 快速模式（Quick Mode）；
  - 新组模式（New Group Mode）；
  - ISAKMP信息交换（ISAKMP Info Exchange）。

快速模式（Quick Mode）

- 快速模式主要用于交换IPSec SA信息。



快速模式

新组模式和ISAKMP信息交换

- 新组模式主要用于实现通信双方交换协商新的Diffie－Hellman组，属于一种请求/响应交换。
  - 发送方发送提议的DH组的标识符及其特征，如果响应方能够接收提议，就用完全一样的消息应答。

- ISAKMP信息交换主要功能是实现通信一方向对方发送错误及状态提示消息。
  - 这并非真正意义上的交换，而只是发送单独一条消息，不需要确认。

作业

- 习题2（1）：IPSec的两个主要协议有什么区别？
- 习题2（3）：IPSec是如何防范重放攻击的？