物联网网络层安全实验	文档编号	版本	页数
	AWS-WSN-01	1.0	4

身份认证实验

一、实验目的

让学生理解身份认证原理，掌握基于对称加密的身份认证方法。

二、实验原理

1 身份认证原理

设备或用户的身份认证是指设备或用户能够提供一个声明的身份给系统。注意，身份认证和消息认证是不一样的。消息认证是指通信双方验证接收到的消息是否在传输过程中遭受了篡改，而身份认证则是验证通信双方的身份是否与宣称的身份一致。

认证一个设备或用户的身份大致有四个常用工具，这四个工具可以单独使用，也可以联合使用。

知道什么：如口令、个人身份号、或之前准备的问题的答案。

拥有什么：如加密密钥、电子密钥卡、智能卡等令牌。

静态生物特征：如指纹、视网膜和人脸。

动态生物特征：如声音模式、手写特征和打字节奏等。

所有这些方法通过适当的执行和应用都可以提供安全的身份认证。然而，每种方法都有缺陷。如攻击者可能伪造或窃取令牌，用户可能会忘记密码或丢失令牌。此外，管理系统的密钥和令牌信息并确保这些信息的安全将会增加不少的系统开销。关于生物计量的认证信息，存在各种各样的问题，如处理假阳性和假阴性、用户满意度、成本和便利性等。对于基于网络的身份认证，最重要的认证方法包括加密密钥和用户个人口令等。

1.1 双向认证

双向认证的一个重要应用领域是双向认证协议，双向认证协议能够使通信双方通过挑战/响应方法来互相认证彼此身份并交换会话密钥。

1.2 单向认证

单向认证则是指，通信中的一方 A 只对另一方 B 进行身份认证，然后 B 却不认证 A 的身份。

2 基于对称加密的身份认证

2.1 双向认证

利用对称加密算法的 CBC 工作模式可以实现数据机密性保护，还可以实现（身份）认证。

通信参与者只有拥有了正确的密钥才能利用 CBC-MAC 算法来生成正确的 CBC-MAC（消息认证码），因此，CBC-MAC 在实现消息完整性认证的同时，也就证明了通信参与者确实拥有正确的密钥。如果假设只要通信参与者拥有正确的密钥，那么就认为该通信参与者的身份就是合法的，那么 CBC-MAC 也就验证了通信参与者的身份。

本实验利用 CBC-MAC 对称加密工作模式来同时实现数据加密、消息完整性认证和身份认证。

三、实验内容

3 网关与节点之间的双向身份认证

3.1 攻击模型及安全攻击威胁

单个合法节点与合法网关之间的身份认证及通信过程中将面临攻击者的重放攻击、假冒攻击、窃听攻击。

在身份认证的过程中，攻击者利用重放截获的数据包来进行假冒攻击(伪装成合法节点)，即攻击者节点截获合法节点的认证数据，过段时间再将此数据发送给合法网关，声称自己是合法节点来欺骗合法网关，或者是以此操作来故意让合法网关进行身份认证来达到一种消耗合法网关的计算资源的 DoS 攻击。

此外，攻击者为了更好的隐藏自己不被合法节点和网关发现自己，可以只是截获数据包进行窃听分析，或者伪装成一个中继节点来中转数据包而不进行选择性转发攻击。(如关于选择性转发攻击的防范可通过基于可信机制的安全路由机制来检测，本实验暂不考虑此类攻击及安全防护方法)。

攻击者若不担心被合法节点和网关发现自己，则可以对收到的数据包进行篡改后再发送出去，即进行主动的篡改攻击。

3.2 安全假设

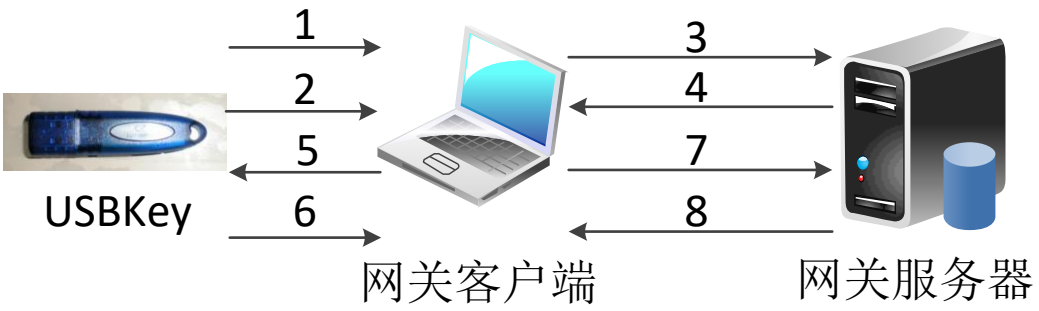
网络中每个合法节点在网络部署前烧写全网唯一的节点号 NodeID，NodeID 作为节点身份的唯一标识，合法节点和合法网关都成功共享了一个全网共享的网络密钥，每个节点也都成功共享了自己与网关之间的对密钥。

3.3 单个节点与网关间双向身份认证方案

1. 网关向节点发送认证初始化数据包，数据包中包含一个与节点号对应的随机数。
2. 节点收到与自己对应的随机数后返回给网关一个认证相应数据包，该数据包中包含一个消息认证码，该消息认证码是基于分组/流密码加密算法，利用节点与网关之间共享的对密钥生成的。网关接收到节点的认证相应数据包后，验证其中的消息认证码是否正确；若正确，则网关向节点发送一个注册成功的数据包，否则不作处理。
3. 网关给节点返回一个提示节点注册成功的数据包。

4 网关客户端用户与网关服务器之间的单向身份认证

网关客户端用户与网关服务器之间的单向身份认证过程采用基于随机数挑战响应和对称加密的身份认证工作方式。



1. USBKey 插入网关客户端(运行在笔记本)上，网关客户端读取到 USBKey 的 USBKeyID
2. 网关客户端弹出用户输入用户名(UserID)和口令(PIN)
3. 网关客户端将 USBKeyID、UserID、PIN 发送至网关服务器
4. 网关服务器验证 UserID、PIN 通过后发送随机数 N 给网关客户端
5. 网关客户端将随机数输入给 USBKey
6. USBKey 将加密后的密文(随机数加密后的密文)返还给网关客户端
7. 网关客户端将加密后的密文发送至网关服务器
8. 网关服务器解密密文得到恢复后的随机数，并与原随机数进行比对，若二者一致则认为网关客户端用户身份合法，网关服务器发送认证通过消息给网关客户端，或者打开网关客户端与网关的连接。