物联网网络层安全实验	文档编号	版本	页数
	AWS-WSN-01	1.0	3

网关广播源认证实验

一、实验目的

了解 merkle 树基本原理，认识基于 merkle 树的广播源认证方式，及网络密钥如何保证广播源认证的安全性

二、实验原理

1.1 Merkle 树定义及作用

Merkle 树是一种树，可以是二叉树，也可以多叉树，无论是几叉树，它都具有树结构的所有特点。Merkle 树的叶子节点上的 value 可以由用户自主设定，非叶子节点的 value 是根据它下面所有的叶子节点值，然后按照一定的算法计算而得出的。如 Merkle Tree 的非叶子节点 value 的计算方法是可以是将该节点的所有子节点进行串联，然后对组合结果进行 hash 计算所得出的 hash value。

Merkle 树在计算机领域中，大多用来进行比对及验证处理等场景中。例如，在无线传感器的广播源认证场景中，传感器节点需要验证网关的身份，就可以使用 Merkle 树来实现。

1.2 Merkle 树原理

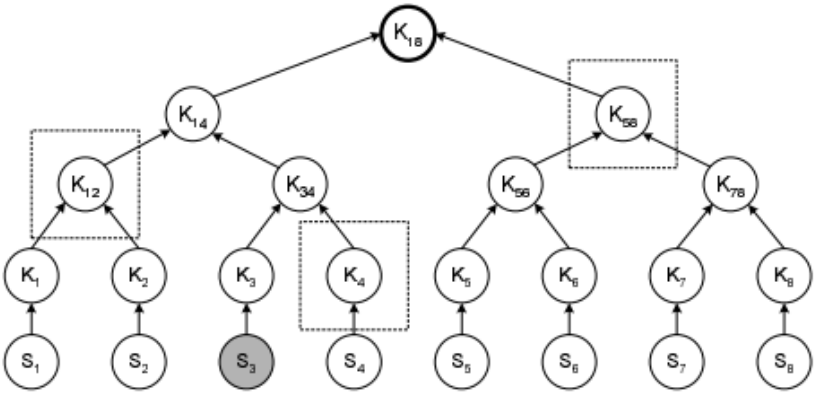


图 1 merkle 树构造

1.2.1 merkle 树构造

离线服务器生成一系列 Si（i=1,2,…,8）和深度为 3 的完全二叉 merkle 树，该树有 15 个节点，为每个节点 i 编号，满足如 i 为父亲节点，则其左孩子结点为 2i，右孩子节点为 2i+1，树的根节点编号为 1。图 1 merkle 树是一颗完全二叉树，$S_i, i = 1,2, \ldots, m$ 为第 i 个 uTESLA 实例；

1.2.2 参数证书实例化

为每个 uTESLA 实例 i 构造一参数证书 ParaCert_i。比如，第 i 个uTESLA 实例的参数证书包含S_i和从 i 个叶子K_i到根的路径上相关旁侧节点值，在图 1 中，第 3 个 uTESLA 实例的证书为$ParaCert_3=\{S_3, K_4, K_{12}, K_{58}\}$；

1.2.3 证书分配

将 uTESLA key 链和相关证书预分配给发送者（网关），而将 merkle 树的根节点预分配给潜在接受广播消息的节点。当网关需要广播控制命令时，随机选取 uTESLA 实例的广播通道。广播消息中包含参数证书$ParaCert_i$，考虑到数据包长度及可行性，采用数据包拆分，来将比较大的广播数据包拆分成多个小数据包，也即将参数证书分割，使得传感器节点可以立即对每个分割包进行认证；

1.2.4 网关下发广播源认证命令

网关下发广播源认证命令。网关选择第 i-th uTESLA 通道 Si，调用过程 ParaCertCompute 得到证书参数 ParaCerti（其中包含 4 个 hash 值）并将该证书用广播源认证命令数据包发送出去。广播命令中 ParaCerti 参数的顺序是从 Si 开始依次向上层排列。

1.2.5 节点进行网关源认证

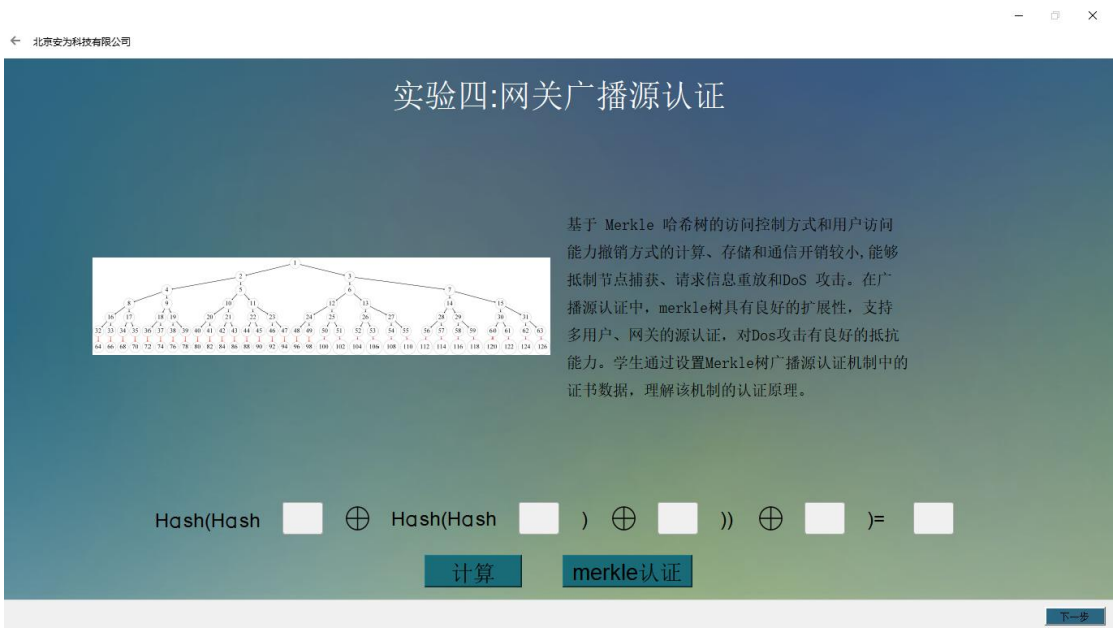
节点对网关进行源认证。节点依次收到和命令数据和证书参数 ParaCerti，i=0,1,2。进行如下认证流程：

计算

Hash(Hash(Hash(Hash(ParaPacket[0]) ⊕ ParaPacket[1]) ⊕ ParaPacket[2]) ⊕ ParaPacket[3])

验证其结果与节点自身存储的 K1 是否相等；若相等，认证成功。

2 实验内容


北京安为科技有限公司
实验四:网关广播源认证
基于 Merkle 哈希树的访问控制方式和用户访问能力撤销方式的计算、存储和通信开销较小,能够抵制节点捕获、请求信息重放和DoS 攻击。在广播源认证中，merkle树具有良好的扩展性，支持多用户、网关的源认证，对Dos攻击有良好的抵抗能力。学生通过设置Merkle树广播源认证机制中的证书数据，理解该机制的认证原理。
Hash(Hash
Hash(Hash
))
)=
计算
merkle认证
下一步