物联网网络层安全实验	文档编号	版本	页数
	AWS-WSN-01	1.0	2

密钥更新

一、实验目的

认识密钥协商的过程，其中网络密钥的预置依赖于相应节点的对密钥

二、实验原理

2.1 密钥更新原理

无线传感器网络中的所有节点需要周期性的更新自己与网关间的对密钥。网关向所管辖的节点网络下发更新密钥命令数据包，该数据包中包含有一个新的随机数(8B，网关中预置了每个节点的随机数标识符都为 8B，为了和网关中预置的每个节点的随机数标识符格式保持一致，特将此时的随机数字段规定为 8B)，收到该命令数据包的所有节点将网关此时下发的随机数(8B)和与节点自己相对应的随机数标识符(8B)异或后，利用单向散列函数生成新的感知节点和网关之间的对密钥。网关也按照此方式来计算更新与每一个节点间的对密钥。

在网关的发起下，每个节点更新自己与网关间的对密钥的操作方式为：

感知节点 i 与网关间的对密钥 $K_{i\text{-}update}$（16B）=MD5(N_i（8B）$\oplus$ N_{update}（8B））

其中：

$K_{i\text{-}update}$ -------16B，节点向网关上报温湿度光照值的数据包时用此密钥加密数据，生成和验证消息认证码 MAC(需要密钥)时也使用此密钥。

N_i-------8B，每个感知节点预置与自己的 ID 号相对应的随机数标识符。

N_{update}-------8B，在生成或更新对密钥时网关所下发的一个随机数。

3 实验内容