## 簇头与控制中心之间的相互认证与密钥协商



1. AS(控制中心)首先发起认证请求，包含新生成的时间戳T1以及随机数r1;
2. 簇头收到消息后，如果确认T1是新鲜的，返回响应消息，即IDL,IDAS, T2, r2,MACL，其中MACL=hash(K，IDL,IDAS, T2, r2,r1),其中T2为新生成的时间戳，r2为随机数,K为控制中心与簇头之间的预置密钥；
3. AS检查T2的新鲜性与MACL是否正确。检查通过则返回认证确认消息IDAS, IDL,T3, r3,MACAS，其中MACAS=hash(K，IDAS,IDL, T3, r3,r2),其中T3为新生成的时间戳，r3为随机数。
4. 簇头检查T3的新鲜性与MACAS是否正确。检查通过返回认证结果，并开始衍生密钥。
5. AS根据认证结果决定是否衍生密钥。如果认证成功，AS（或者簇头）及时广播簇头的ID。（括号主要取决于设定里究竟是否节点能与AS之间信号强度是否支撑通信，是则簇头的主要目的是减少信令数目，否则兼具中继功能）12345678 CK=1234 IK=5678

## 节点与控制中心之间的相互认证与密钥协商



1. 节点i依据控制中心广播的簇头ID,发送认证请求消息IDL,IDi,ti,ri,MACi，其中MACi=hash(Ki, IDL,IDi,ti,ri), 其中ti为新生成的时间戳，ri为随机数,K为节点i与AS之间的预置密钥；
2. 收到多个节点的认证请求后，簇头检查新鲜性后，按照MAC=MAC1⊕MAC2⊕…⊕MACn的方式聚合消息中的MAC值，并发送聚合认证请求IDAS, IDL,{(ID1,t1, r1),(ID2,t2, r2),…,(IDn,tn, rn)},MAC,MACL,其中MACL=hash(IK, IDAS, IDL,{(ID1,t1, r1),(ID2,t2, r2),…,(IDn,tn, rn)},MAC)，其中IK为上一阶段簇头与控制中心衍生的密钥;
3. 控制中心核验MAC，如果检查通过，则返回IDL, IDAS,{(ID1,T1, R1,MACAS\_1),(ID2,T2, R2,MACAS\_2),…,(IDn,Tn,Rn,MACAS\_n)},MACAS-L，其中MACAS\_i=hash(Ki, IDi,Ti, Ri,ri)，MACAS\_L=hash(IK,IDL, IDAS,{(ID1,T1, R1,MACAS\_1),(ID2,T2, R2,MACAS\_2),…,(IDn,Tn,Rn,MACAS\_n)}),T1T2……Tn为新生成的时间戳,R1R2……Rn为随机数。
4. 簇头收到消息后核验MACAS\_L，核验通过后将认证回应分发给相应的节点；
5. 节点i核验MACAS\_i,核验通过后开始衍生密钥。

* 依靠簇头(簇头的选取依靠广播消息)，但不与簇头进行身份认证与密钥协商
* 聚合认证请求MAC=MAC1⊕MAC2⊕…⊕MACn
* MACAS\_i=hash(Ki, IDi,Ti, Ri,ri),
* MACAS\_L=hash(IKAS\_L,IDL, IDAS,{(ID1,T1, R1,MACAS\_1),(ID2,T2, R2,MACAS\_2),…,(IDn,Tn,Rn,MACAS\_n)})(没加随机数不知道会不会安全性分析出问题)
* 簇头在这里的作用为转发消息
* 簇头的更新依靠AS的广播（或者加密）消息

对簇头的一些合理设定：1.减少认证的信令开销；2.减少AS处控制信令的信令开销2.减少数据传输的信令开销（某些节点采集的数据数据不一定要连续发送，可以采集一段时间集中发送（而节点存储空间不够，所以先加密簇头，可能是与AS的密钥，也可能是与簇头的密钥））

## 节点与簇头之间的相互认证与密钥协商（按需选择）



1. Nodei首先发起认证请求，包含新生成的时间戳T1以及随机数r1;
2. 簇头收到消息后，如果确认T1是新鲜的，返回响应消息，即IDL,IDi, T2, r2,MACL，其中MACL=hash(K，IDL,IDi, T2, r2,r1),其中T2为新生成的时间戳，r2为随机数,K为节点i与簇头之间的预置密钥；
3. Node i检查T2的新鲜性与MACL是否正确。检查通过则返回认证确认消息IDi, IDL,T3, r3,MACi，其中MACi=hash(K，IDi,IDL, T3, r3,r2),其中T3为新生成的时间戳，r3为随机数。
4. 簇头检查T3的新鲜性与MACAS是否正确。检查通过返回认证结果，并开始衍生密钥。
5. Node i根据认证结果决定是否衍生密钥

## 节点之间的相互认证与密钥协商



Node A与Leader之间已经建立了加密和完整性保护

1. Node A首先发起认证请求，将会话请求消息（IDA,Enc(IDB,RA),MACA）发送给Leader。其中MACA=hash(IKA，IDA,Enc(IDB,RA))，IKA为NodeA和Leader两者之间的完整性保护密钥
2. Leader核验MACA和检验随机数的新鲜性，检查通过生成随机数RS，将会话通知消息(IDL,Enc(IDB, IDA, RS⊕RA),MACL\_B)发送给Node B，其中MACL\_B=hash(IKB,IDL,Enc(IDB, IDA, RS⊕RA))，IKB为NodeB和Leader两者之间的完整性保护密钥。
3. Node B核验MACL\_B和检验RS⊕RA的新鲜性，检查通过生成随机数RB，计算密钥CK||IK=hash(IDA,IDB,RA⊕RB⊕RS)，将会话通知回复（IDB,Enc(IDA, RB),MACB）返回给Leader。其中MACB=hash(IKB，IDB,Enc(IDA, RB))，IKB为NodeB和Leader两者之间的完整性保护密钥。
4. Leader核验MACB和检验随机数的新鲜性, 检查通过后将会话请求回复（IDL,Enc（IDA,IDB,RB⊕RS)MACL\_A）发送给Node A，其中MACL\_A=hash(IKA,IDL, Enc(IDB, IDA, RS⊕RB))，IKA为Node A和Leader两者之间的完整性保护密钥。

## 群组节点更新

正常情况由AS通过旧簇头将加密的新簇头的ID发送给各个节点，簇头节点损坏的情况重新执行流程

## 子节点与节点之间的相互认证与密钥协商

同（三）

## 用户设备与节点之间相互认证与密钥协商

我们这个是要考虑AKA吗？石小平论文

不考虑AKA 普通群组认证