A0 = MACKA( N || ACK )

A12 = A0  \oplus C0

Root commitment = A20 \oplus E11

E11

A20 = A11  \oplus A12

A20

A12

A11

A12 = A0  \oplus C0

Root commitment = A20 \oplus E11

E11

A20 = A11  \oplus A12

A20

A12

A11

A0 = MACKA( N || NACK )

Aggregation tree

Fan-out = n1

Fan-out = n2

Fan-out = nn

Fan-out = n4

Fan-out = n3

BS

**C2 = < C.id, 4, C2.value, H [ N || C.id || 4 || C2.value ] >**

**B1 = < B.id, 2, B1.value, H [ N || B.id || 2 || B1.value ] >**

**A0 = < A.id, 1, A.value, H [ N || A.id || 1 || A.value ] >**

**D0 = < D.id, 1, D.value, H [ N || D.id || 1 || D.value ] >**

**H0 = < H.id, 1, H.value, H [ N || H.id || 1 || H.value ] >**

A’s: (001)*2*

From D: (001)*2*

From B:

(010, 001)*2*

From C:

(100)*2*

D

BS

BS

**A1 = < A.id, 2, A1.value, H [ N || A.id || 2 || A1.value || A0 || D0] >**

**A1.value= A0.value + D0.value**

BS

A1

B1 C1

H1

B

C

D

B1

C0

B0

A0

A