

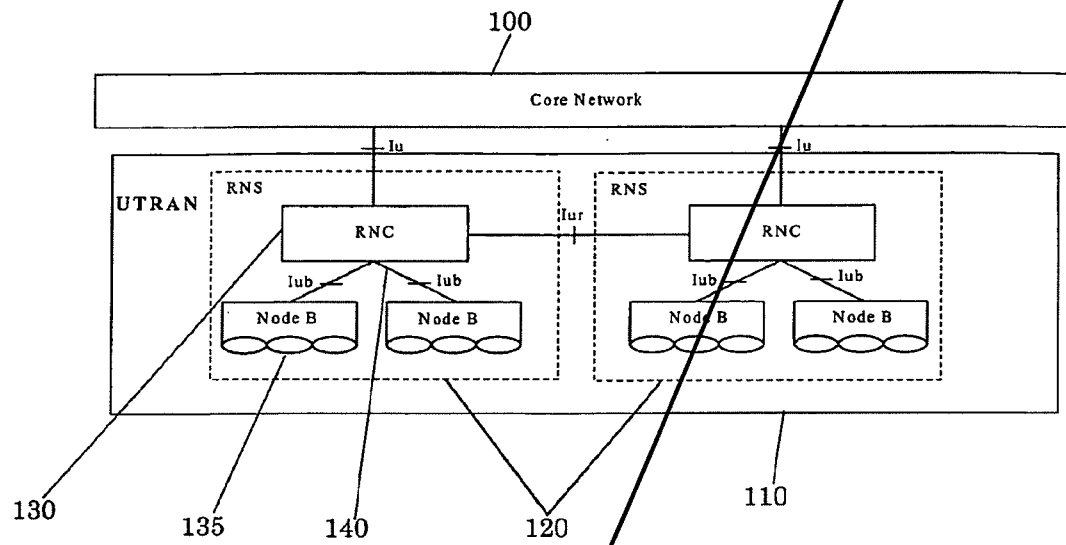


Fig. 1
(Prior Art)

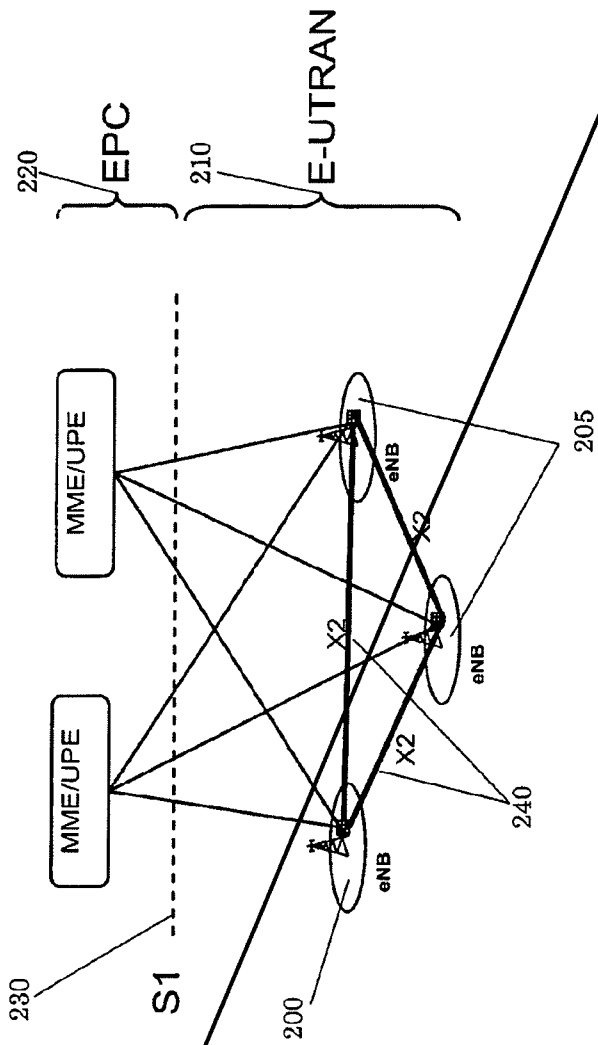


Fig. 2
(Prior art)

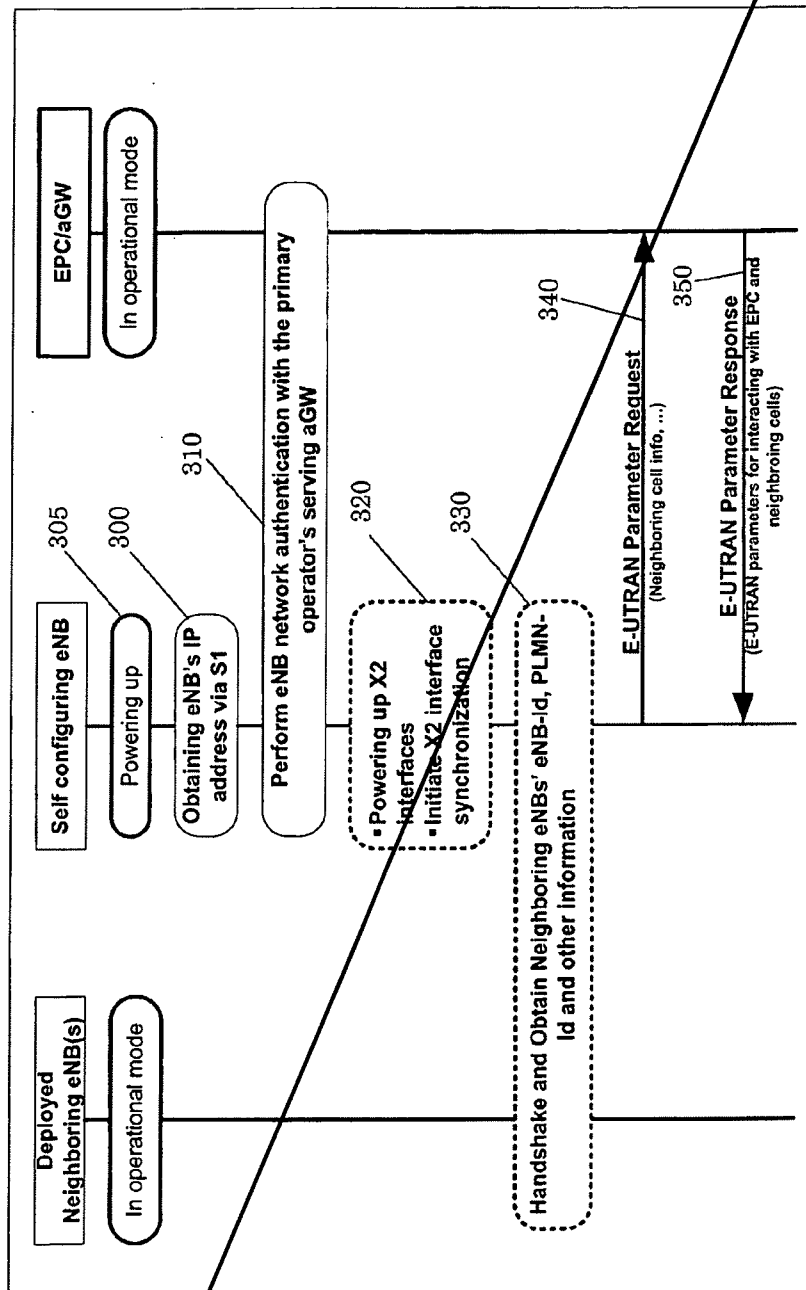


Fig. 3

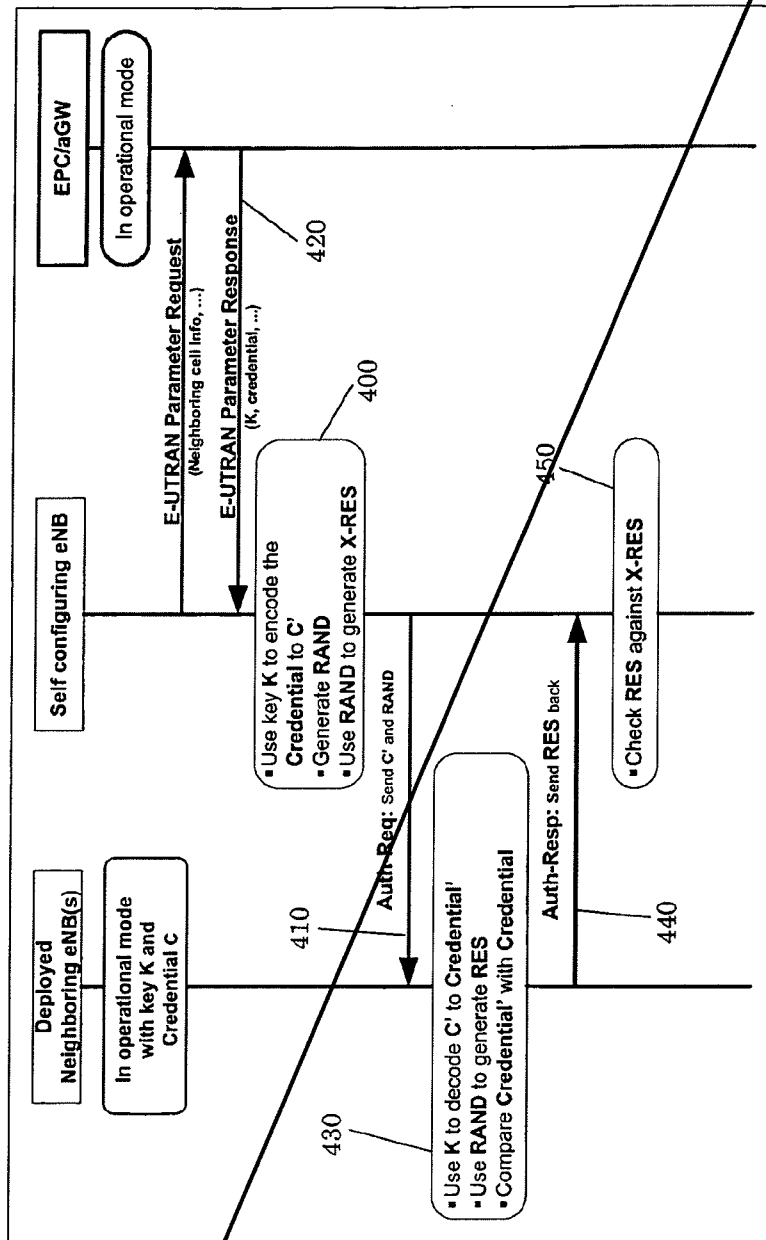


Fig. 4

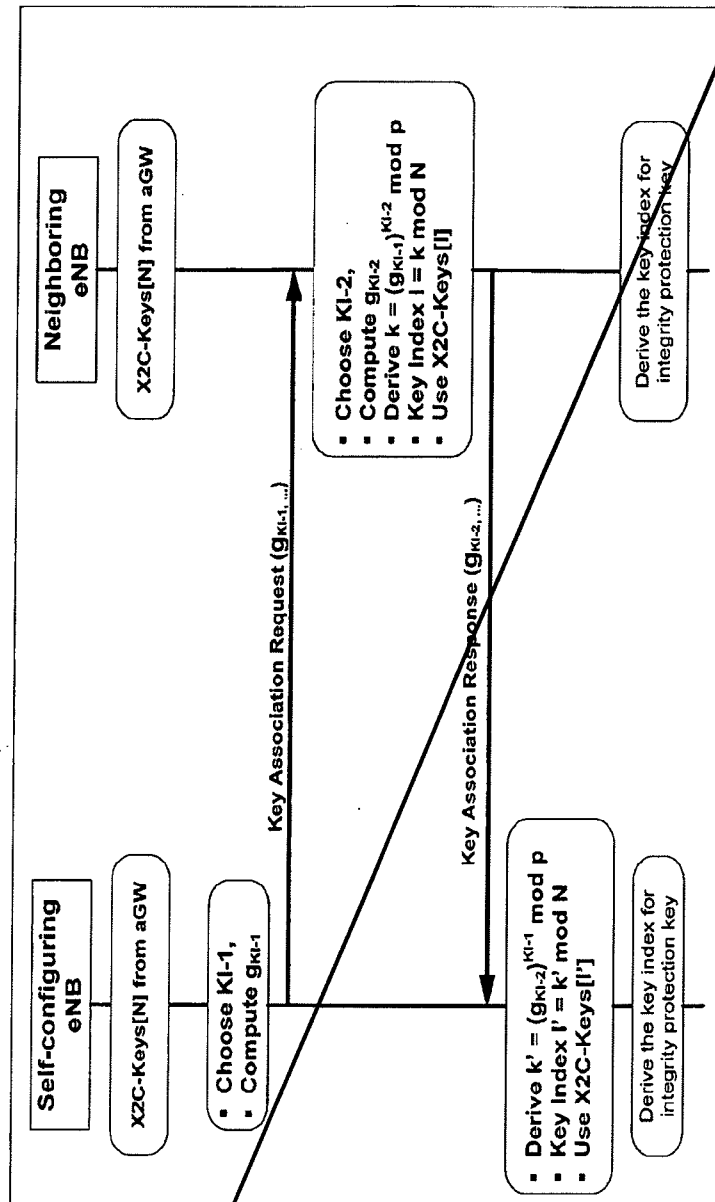


Fig. 5

I: Initiator

R: Responder

A: Attacker

Let p be a large prime number and g a generator of the multiplicative group F_p^* .

Initially I picks x , A picks m , and R picks y , all integers uniformly selected from the interval $[1, p-1]$

1. $I \rightarrow A(R)$: HDR_I, SA_I, g_I^x, N_I (Note: $A(R)$ denotes A receiving message intended for R)
2. $A(I) \rightarrow R$: HDR_I, SA_I, g_I^m, N_I (Note: $A(I)$ denotes a message from A but is assumed by the recipient R to be from I)
3. $R \rightarrow A(I)$: HDR_R, SA_R, g_R^y, N_R
4. $A(R) \rightarrow I$: HDR_R, SA_R, g_R^m, N_R
5. $I \rightarrow A(R)$: $HDR_I, SK\{ID_I, Cert_I, AUTH, SA2_I, \dots, \text{other fields to create child SAs}\}$
6. $A(I) \rightarrow R$: $HDR_I, SK\{ID_I, Cert_I, AUTH, SA2_I, \dots, \text{other fields to create child SAs}\}$
7. $R \rightarrow A(I)$: $HDR_R, SK\{ID_R, Cert_R, Sig_R, AUTH, SA2_R, \dots, \text{other fields to create child SAs}\}$
8. $A(R) \rightarrow I$: $HDR_R, SK\{ID_R, Cert_R, Sig_R, AUTH, SA2_R, \dots, \text{other fields to create child SAs}\}$

Fig. 6

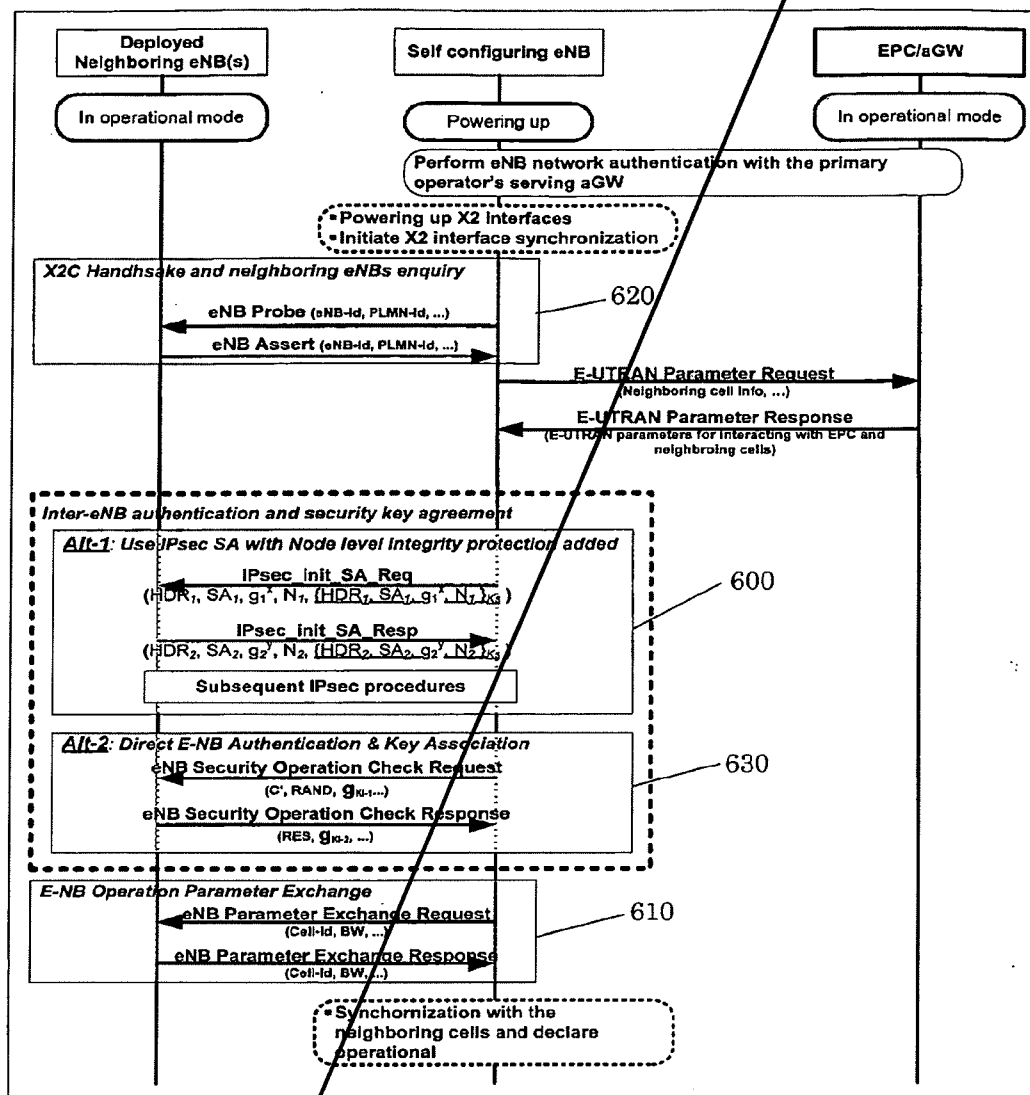


Fig. 7

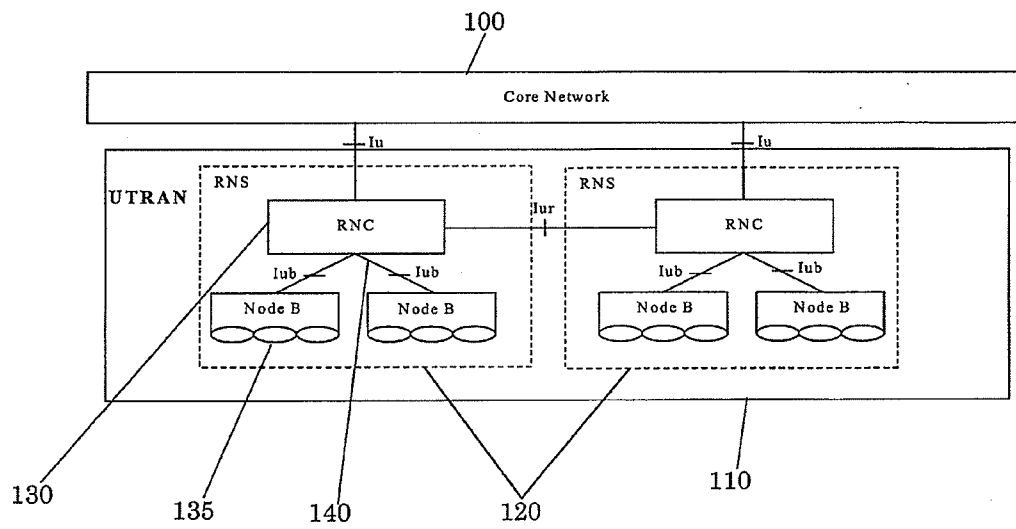


Fig. 1
(Prior Art)

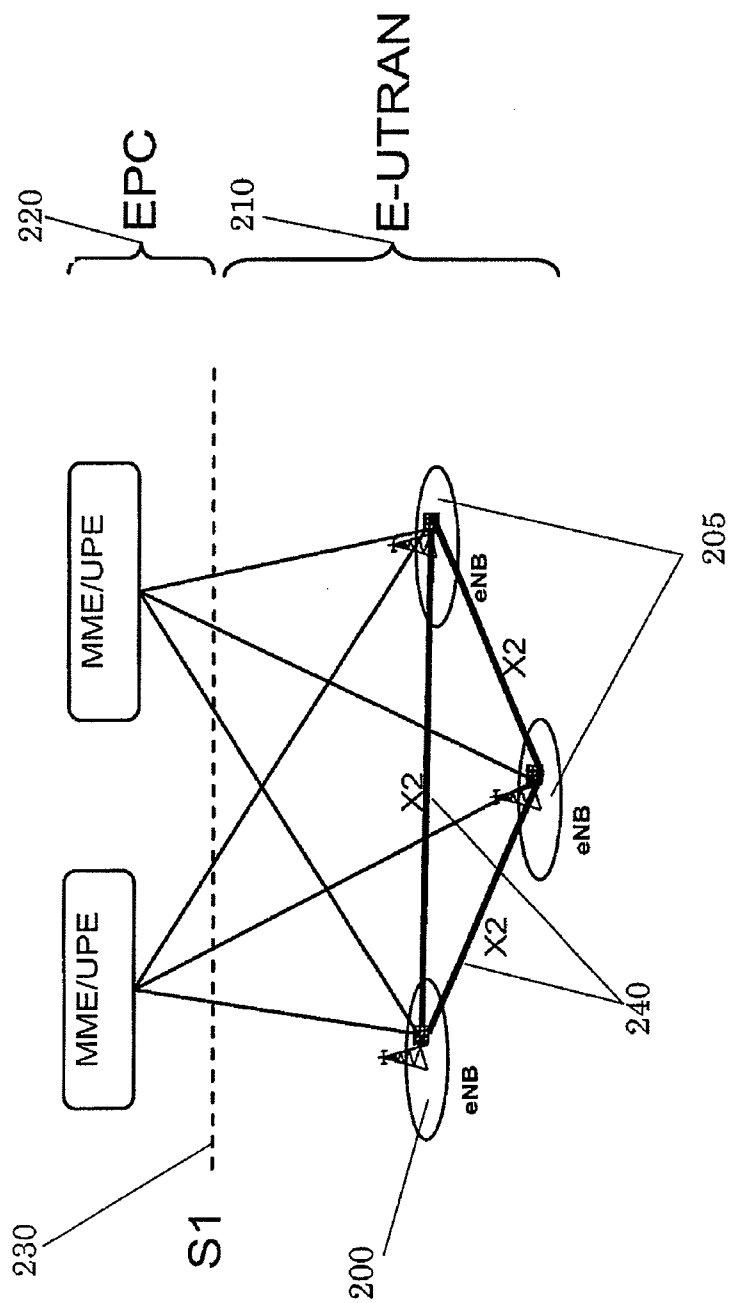


Fig. 2

(Prior art)

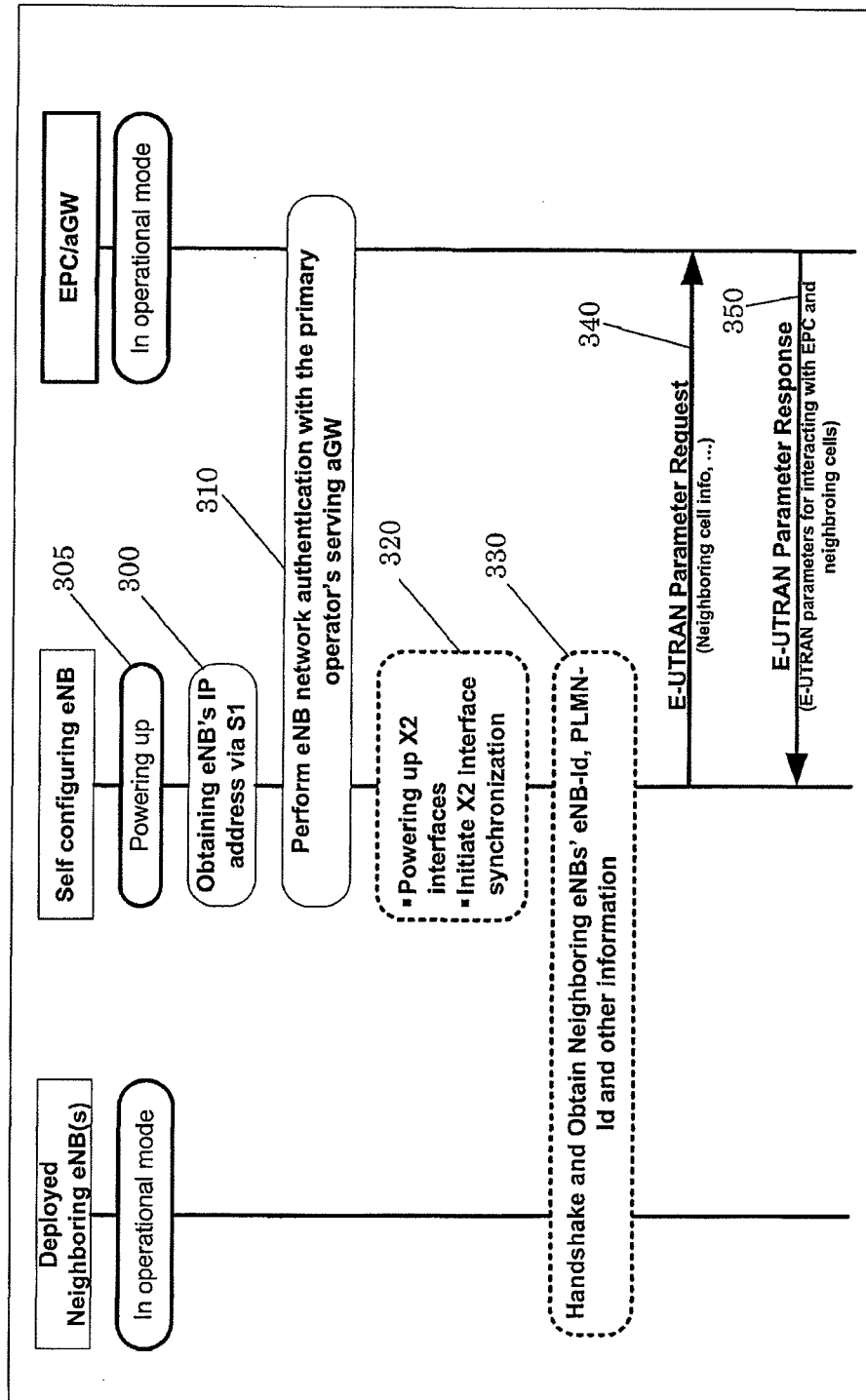


Fig. 3

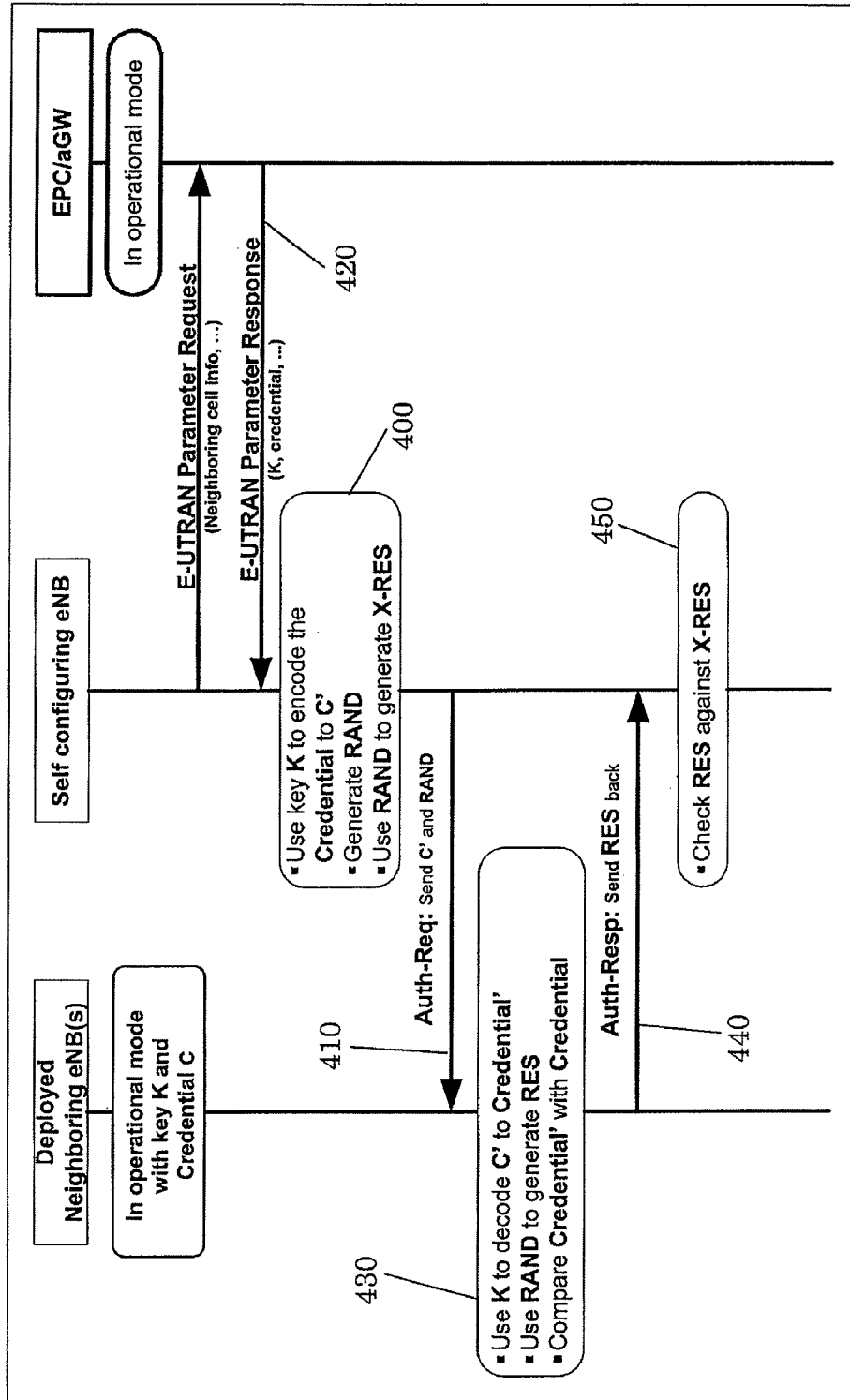


Fig. 4

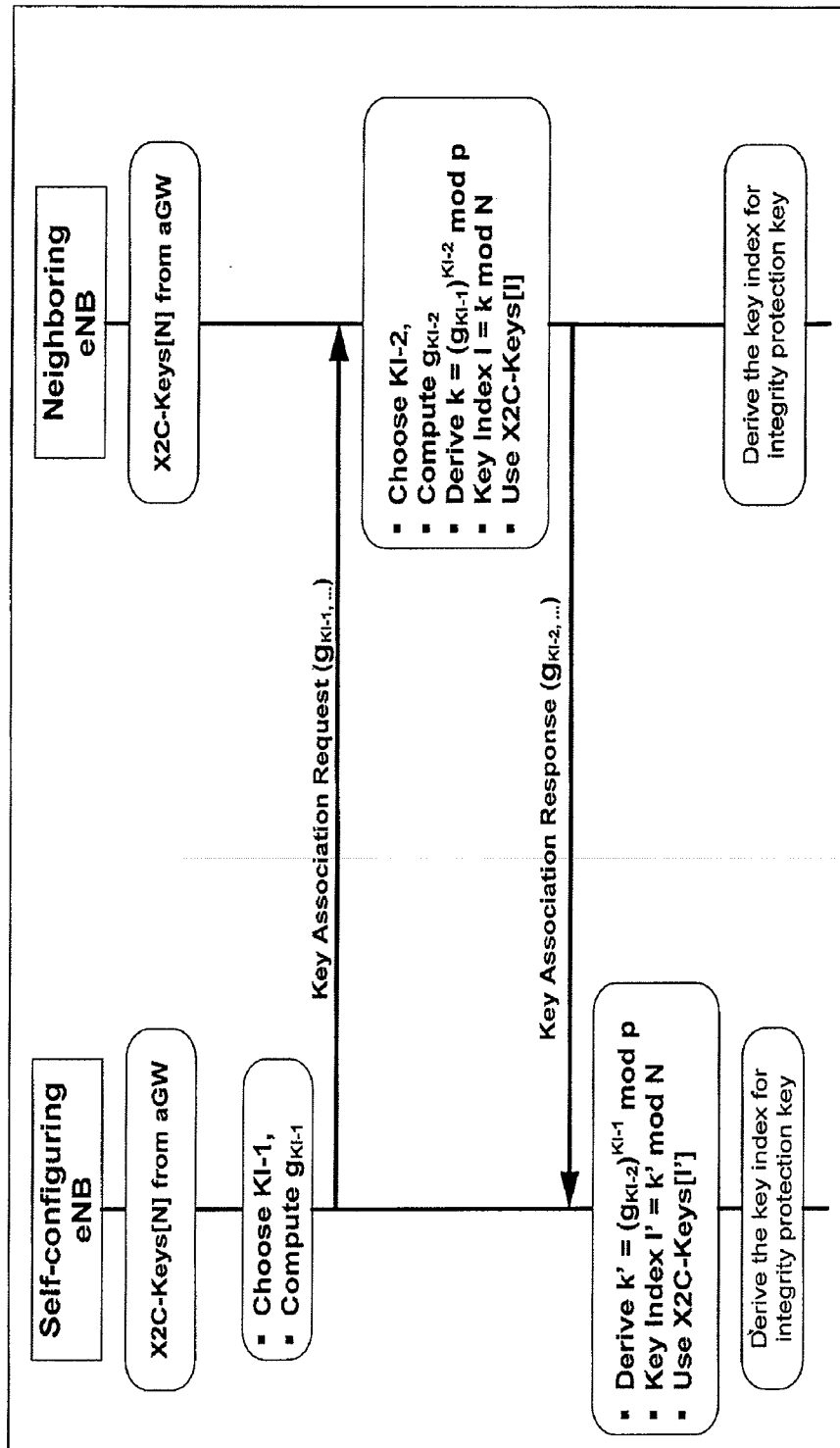


Fig. 5

I: Initiator

R: Responder

A: Attacker

Let p be a large prime number and g a generator of the multiplicative group F_p^* .

Initially I picks x , A picks m , and R picks y , all integers uniformly selected from the interval $[1, p-1)$

1. $I \rightarrow A(R)$: HDR_I, SA_I, g_I^x, N_I (Note: $A(R)$ denotes A receiving message intended for R)
2. $A(I) \rightarrow R$: HDR_I, SA_I, g_I^m, N_I (Note: $A(I)$ denotes a message from A but is assumed by the recipient R to be from I)
3. $R \rightarrow A(I)$: HDR_R, SA_R, g_R^y, N_R
4. $A(R) \rightarrow I$: HDR_R, SA_R, g_R^m, N_R
5. $I \rightarrow A(R)$: $HDR_I, SK\{ID_I, Cert_I, AUTH, SA2_I, \dots, \text{other fields to create child SAs}\}$
6. $A(I) \rightarrow R$: $HDR_I, SK\{ID_I, Cert_I, AUTH, SA2_I, \dots, \text{other fields to create child SAs}\}$
7. $R \rightarrow A(I)$: $HDR_R, SK\{ID_R, Cert_R, Sigr, AUTH, SA2_R, \dots, \text{other fields to create child SAs}\}$
8. $A(R) \rightarrow I$: $HDR_R, SK\{ID_R, Cert_R, Sigr, AUTH, SA2_R, \dots, \text{other fields to create child SAs}\}$

Fig. 6

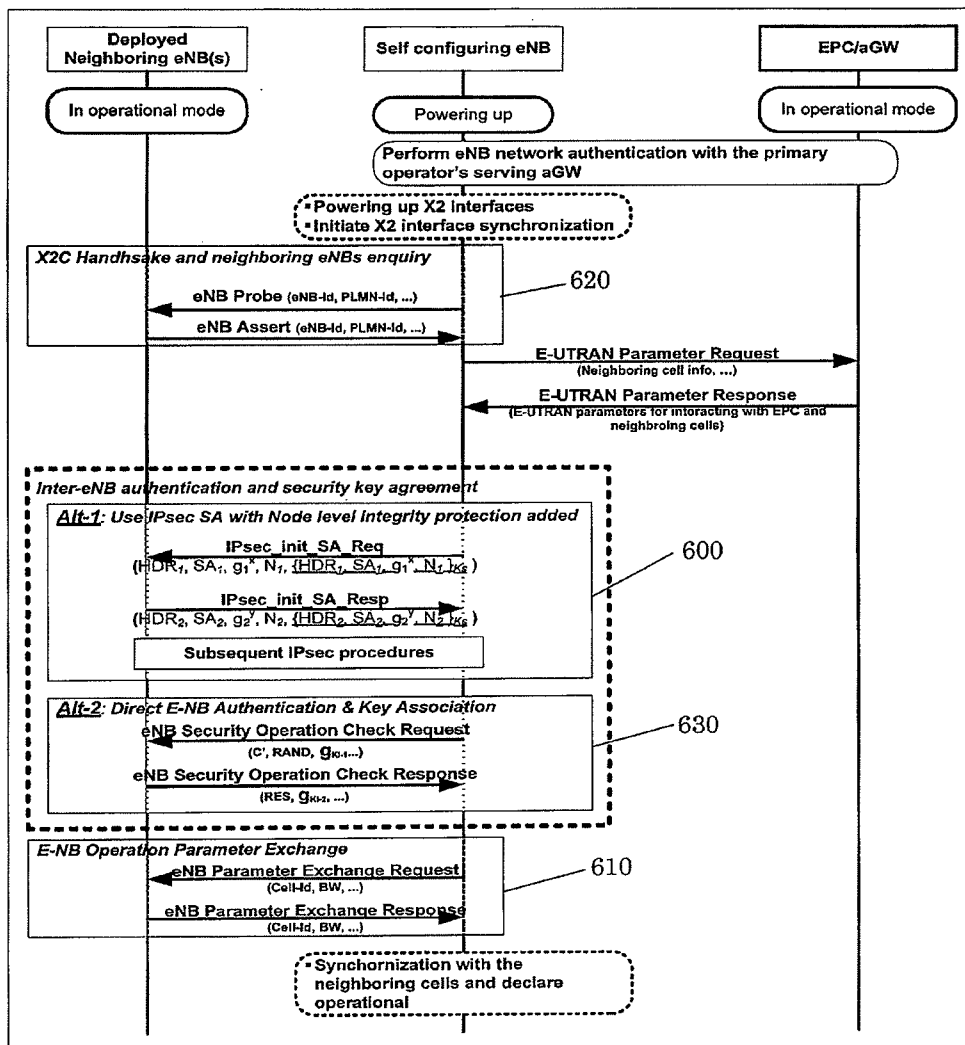


Fig. 7