Analysis and Verification of Concurrent Systems

UFCFYN-15-M

Course Work Assignment

By Michael Onileowo

**Task 1:**

Design and draw a state transition diagram of the system considering four agents.

The state transition diagram for AgentA, ServerB, AuthenticationS and IntruderI is as below

Application Request A

Application Request A

Authentication Request

Application Response B

Eavesdropped message Application Request B

Authentication Response

This is also represented as below to help in writing the NuSMV code

AgentA:

WAIT SEND1 RECEIVE2 SEND3a RECEIVE4a

AuthenticationSB:

WAIT RECEIVE1 SEND2

ServerB:

RECEIVE3a SEND4b

WAIT

RECEIVE3b SEND4b

IntruderI:

ACTIVE RECEIVE3b SEND3b RECEIVE4b

**Task 2:**

In your NuSMV model (code using the SMV language) all the agents should work concurrently, and in an asynchronous manner.



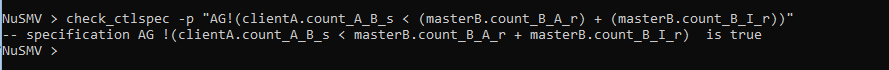
**Task 3 and 4:**

Identify and express five authentication and secrecy properties using both LTL and CTL

and Verify all the properties identified above

1. SPEC AG!(clientA.count\_A\_B\_s < (masterB.count\_B\_A\_r) + (masterB.countB\_B\_I\_r))

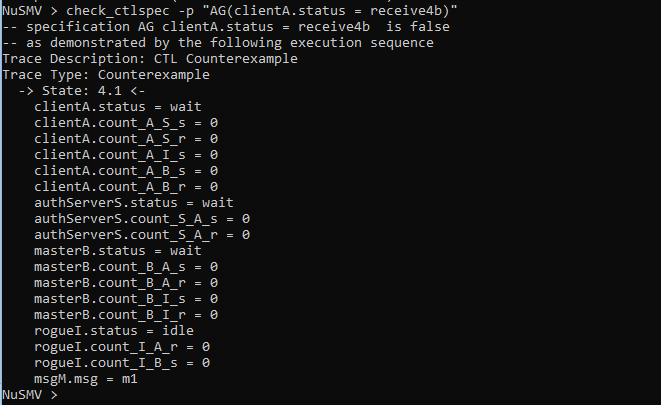
This is to specify that the count of messages received by ServerB can be more than the count of messages sent by AgentA because IntruderI is also able to send messages to ServerB.



1. SPEC AG!(clientA.status = receive4b)

This is to specify that Always Globally, AgentA status will not get to the status of receive4b. This is the message that has been eavesdropped by IntruderI.





1. SPEC AG(clientA. count\_A\_S\_s >= authServerS. count\_S\_A\_r)

This verify that Always Globally, number of messages sent from AgentA to AuthenticationS must greater or equal to the count messages sent from AuthenticationS to AgentA.



1. SPEC AG(clientA.count\_A\_B\_s >= masterB.count\_B\_A\_r)

This will verify that the count of messages sent from ServerB to AgentA will always be equal or greater than the count of the messages received by AgentA from ServerB.



1. SPEC AG(rogueI.count\_I\_A\_r = clientA.count\_A\_I\_s)

This verifies that IntruderI cannot have more messages than the number of messages sent by AgentA.

