Modeling Insider User Behavior Using Multi-Entity Bayesian Network **

Ghazi A. AlGhamdi [1]

Kathryn B. Laskey [1]

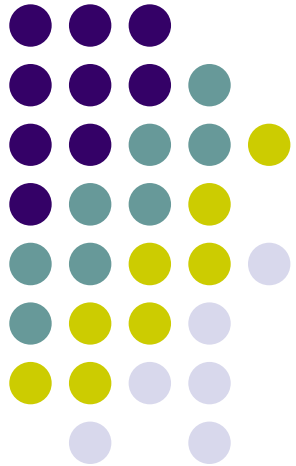
Edward J. Wright [2]

Daniel Barbará [1]

KC Chang [1]

[1] George Mason University

[2] IET



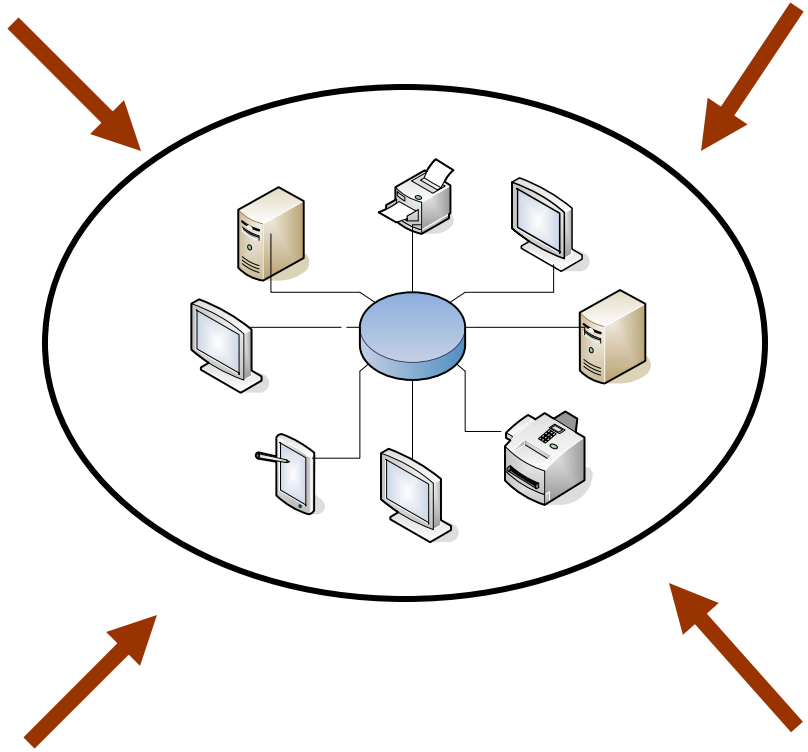
** Work for this paper was performed under funding provided by the Advanced Research and Development Activity (ARDA), under contract NBCHC030059, issued by the Department of the Interior. Additional support was provided by the US Navy

Presentation Outline

- Introduction
- Research Methodology
- Insider Bayesian Network Model (IBN)
- Operational Concept
- Model Evaluation
- Conclusion & Future Work

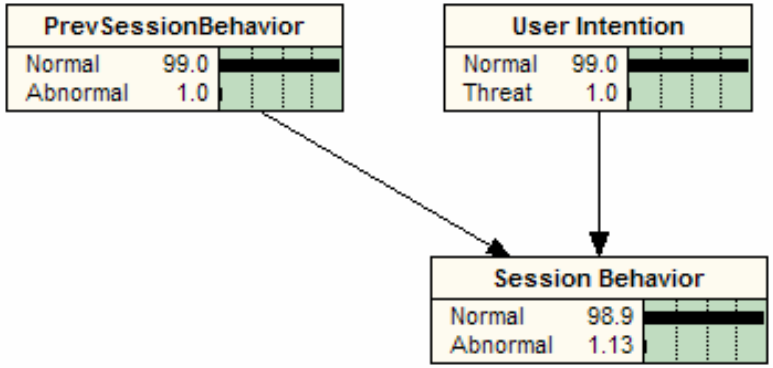
Insider Threat
Statement of the Problem

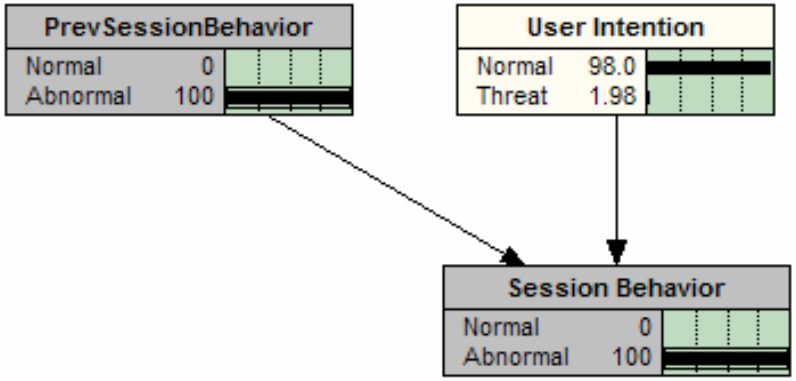
- Insider Domain Knowledge
- Malicious Insider
  - Confidentiality
  - Integrity
  - Availability
- Existing IDS
- CSI/FBI report 2003: “Computer Crime and Security Survey” :
  - Insider abuse of network access was the most cited form of attack or abuse (80%)
  - 92% of the respondents organizations employ some form of access control mechanisms

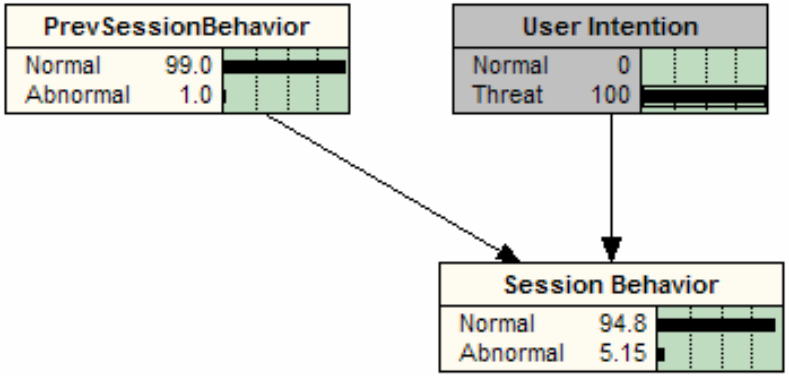


Research Methodology
Bayesian Networks

- *Each node in the network represents a variable of interest*
- *Each arc represents influence between the variables*



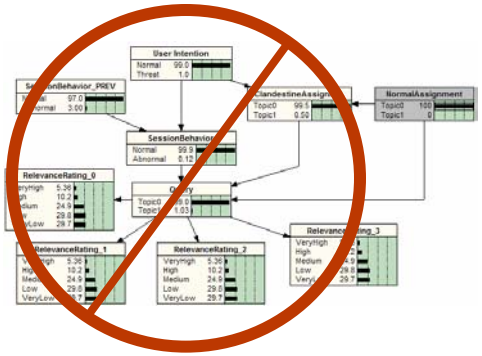


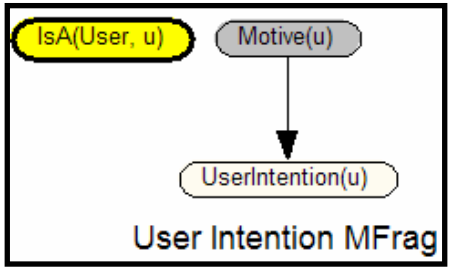


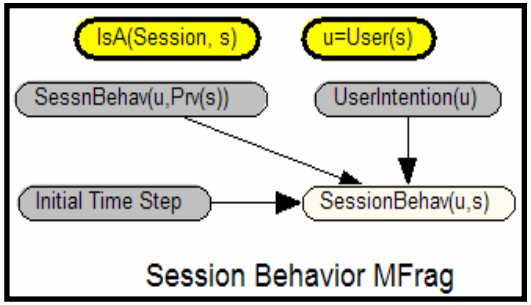
[Jensen, 2001]

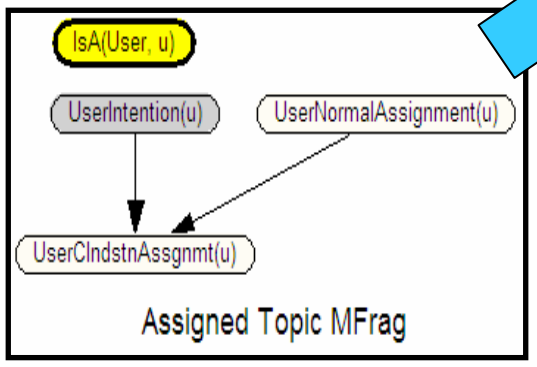
[Screen shots are taken from Netica® package]

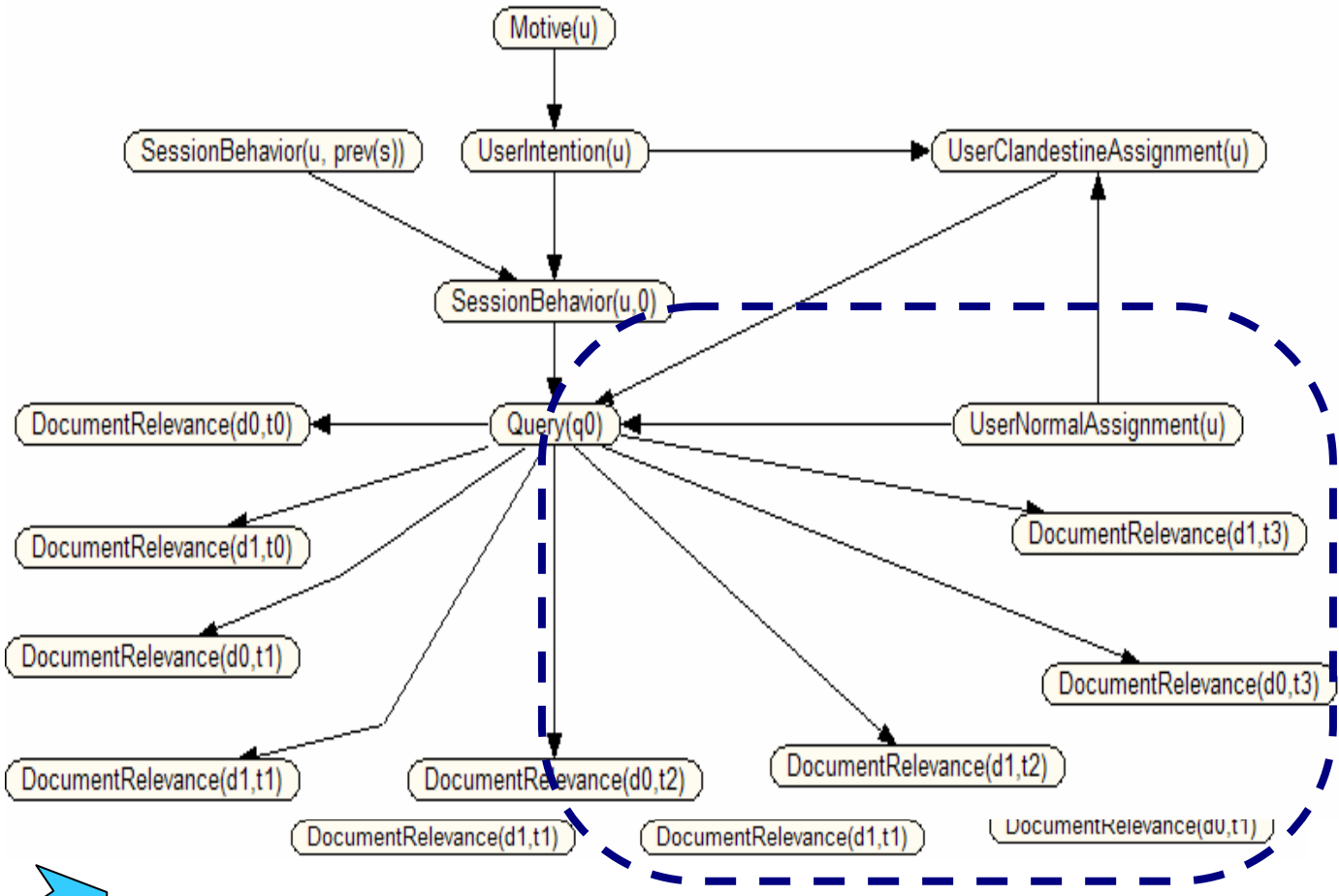
Multi Entity Bayesian Networks (MEBN)



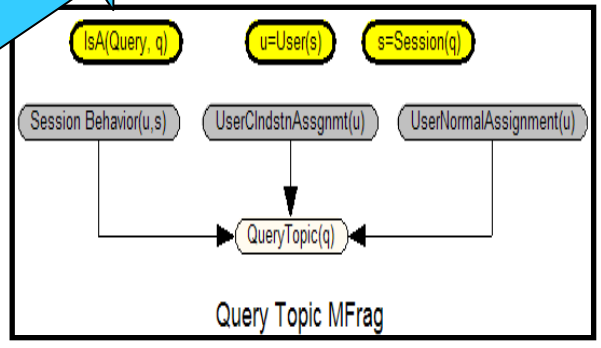


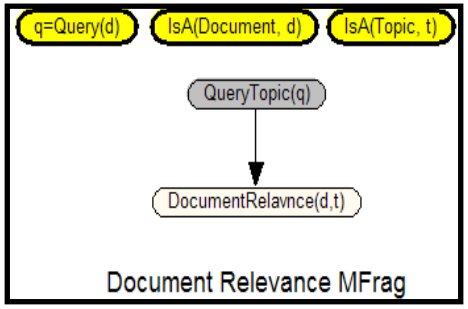






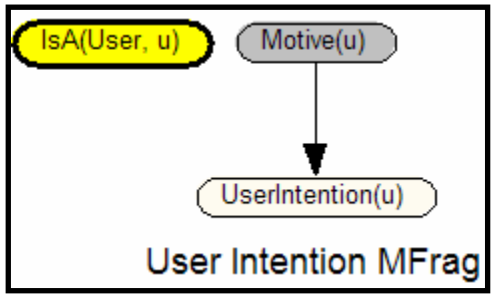
Situation-Specific BN for Document Access Model

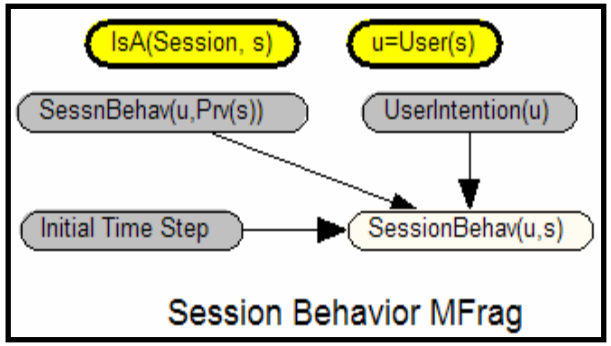


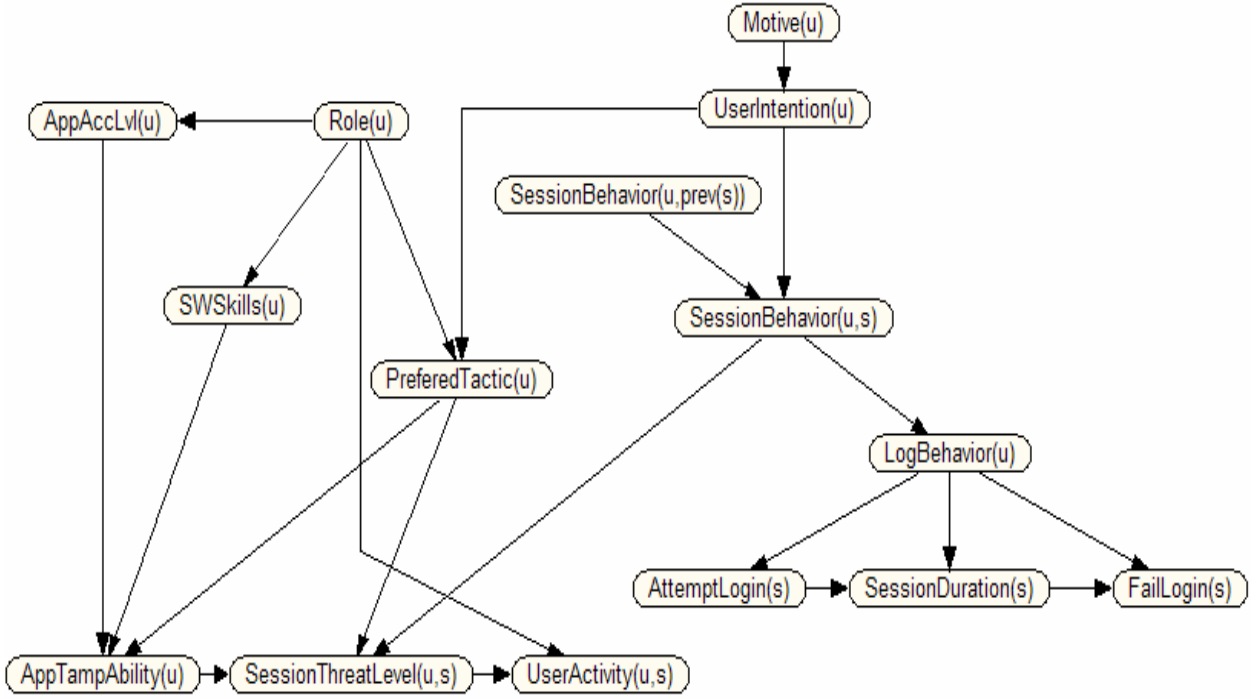


"MEBN is to BN as algebra is to arithmetic"

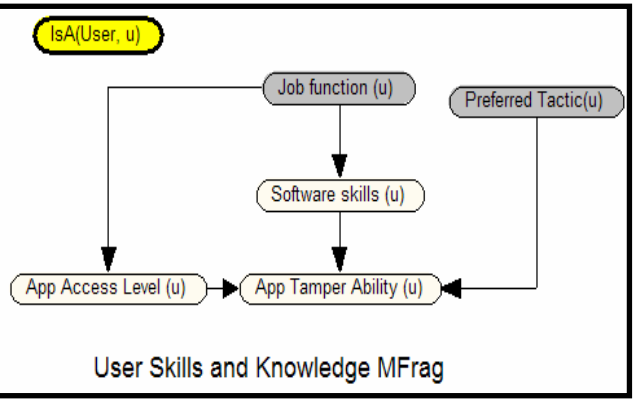
Multi Entity Bayesian Networks (MEBN)

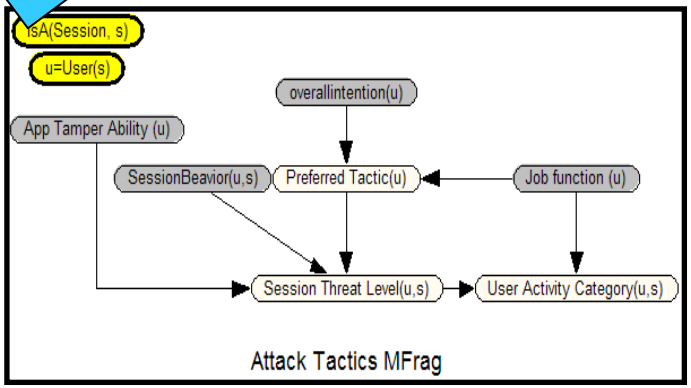


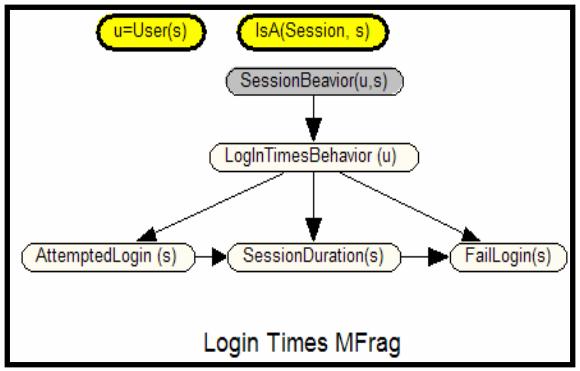




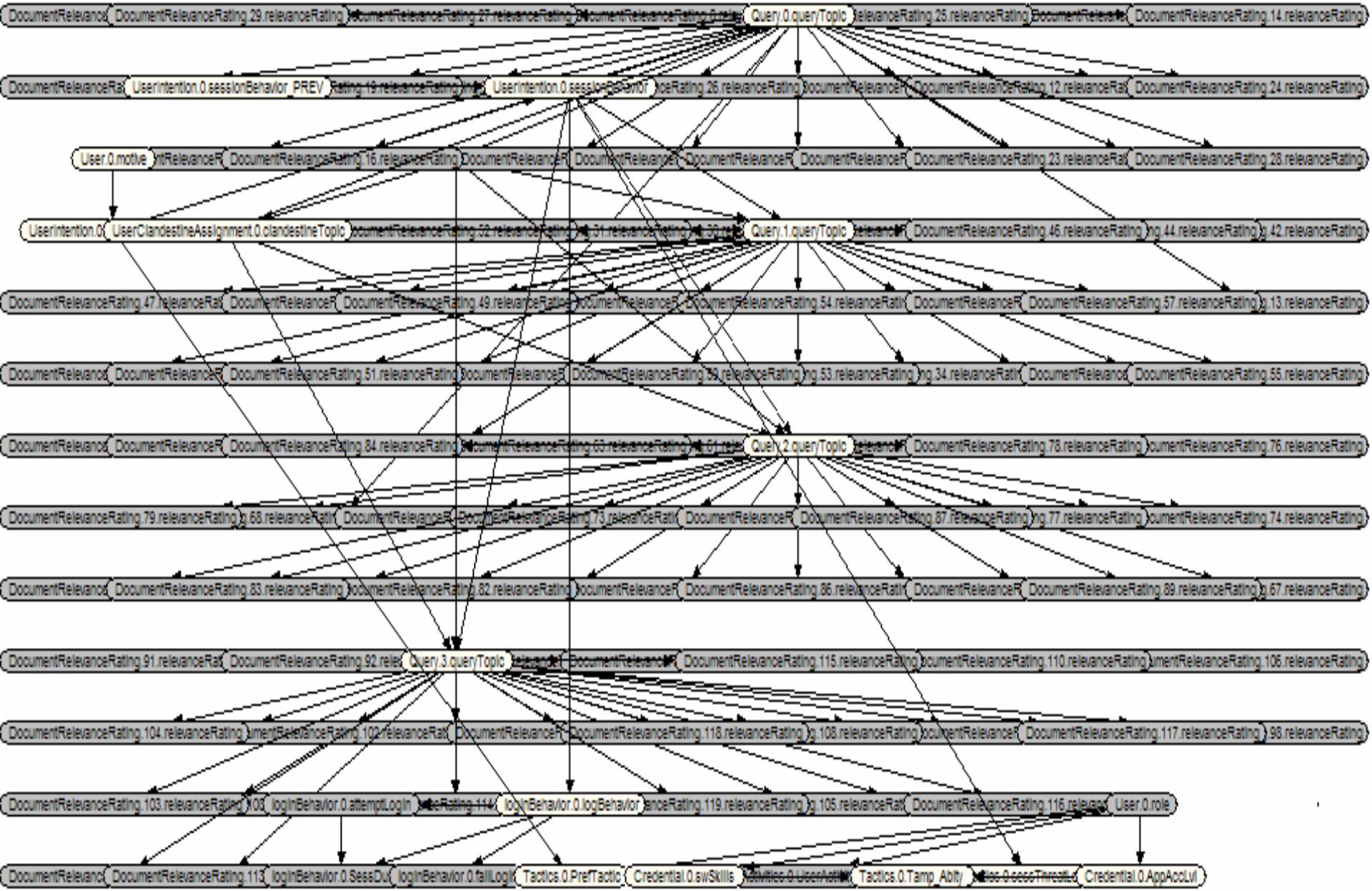
Situation-Specific BN for Login Behavior Model





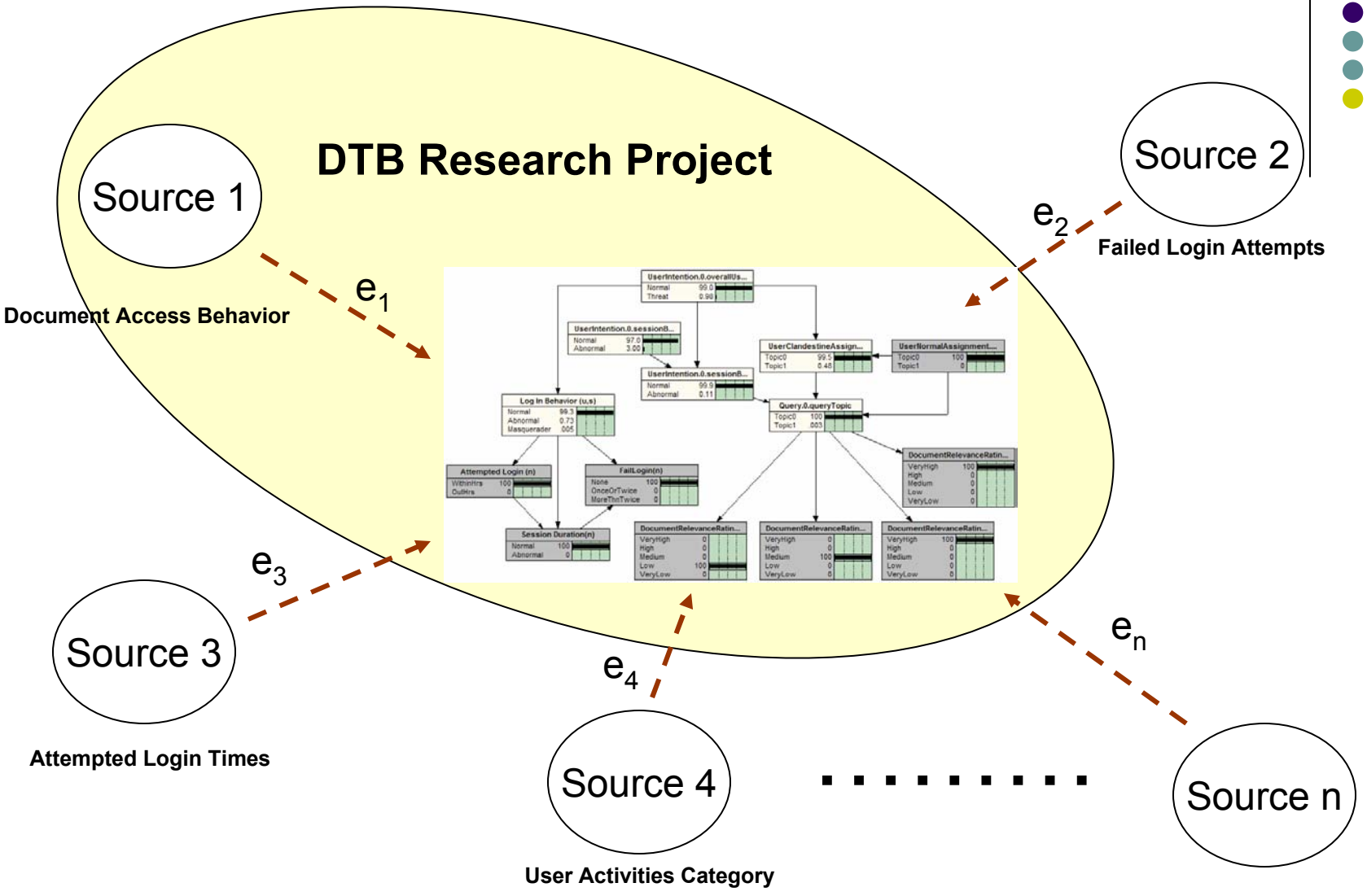


How Complex can we go?



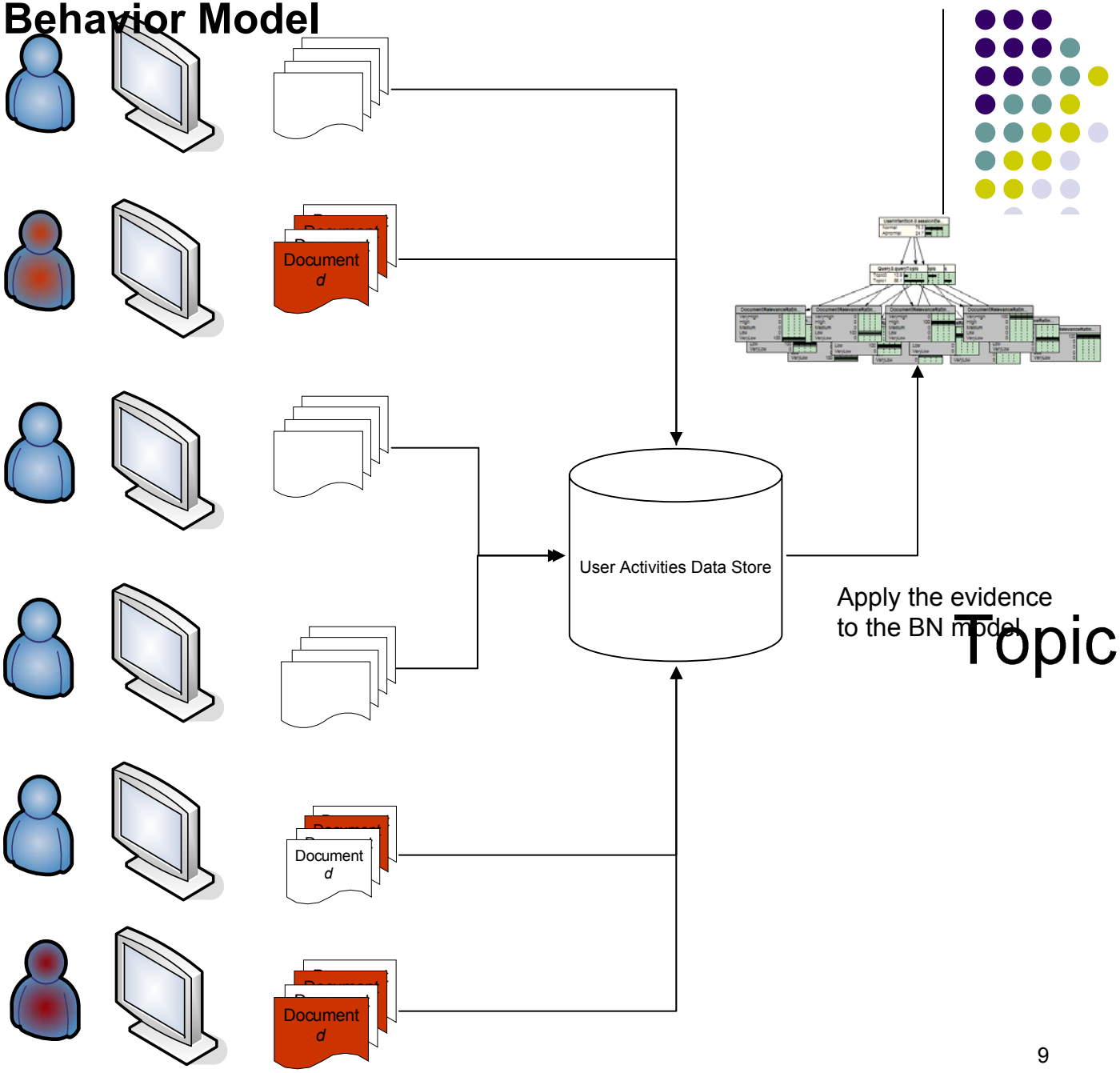
Situation-Specific BN for the Combined Model

IBN Operational Concept

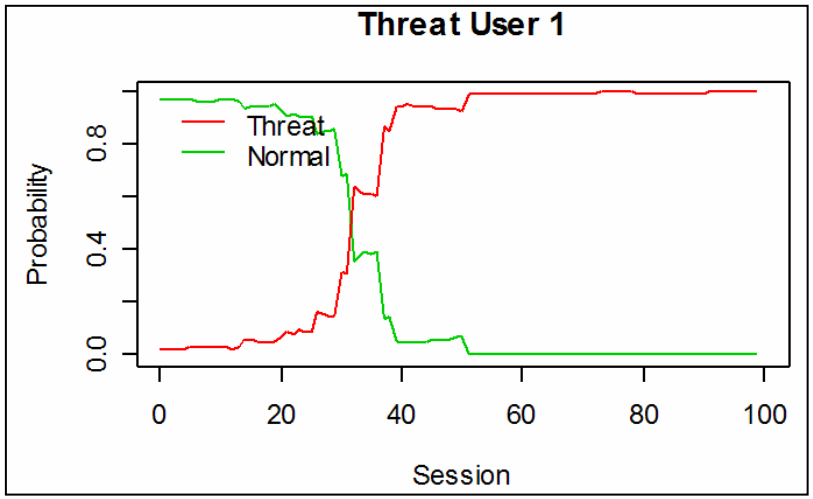


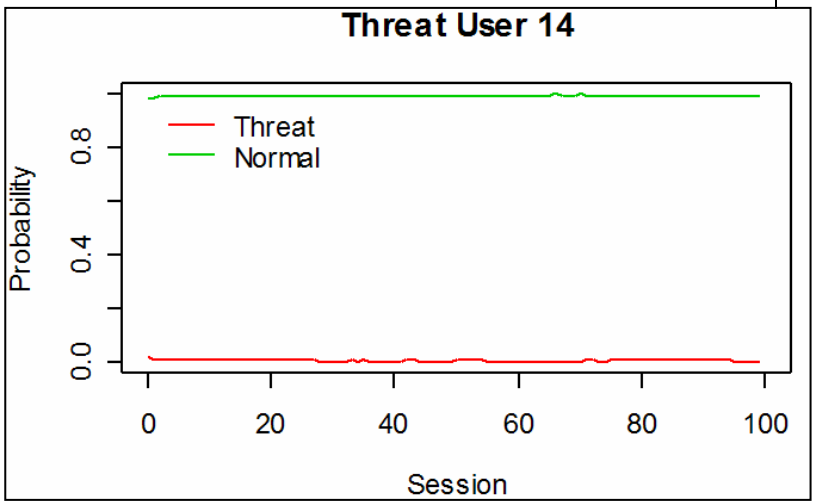
IBN Objective: ***Fuse and aggregate these evidence that are provided from different information sources to infer user intention!***

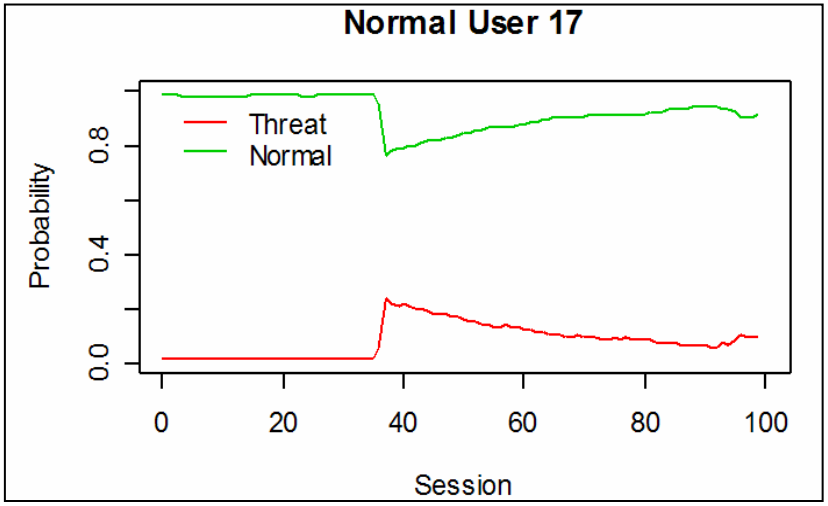
Document Access Behavior Model

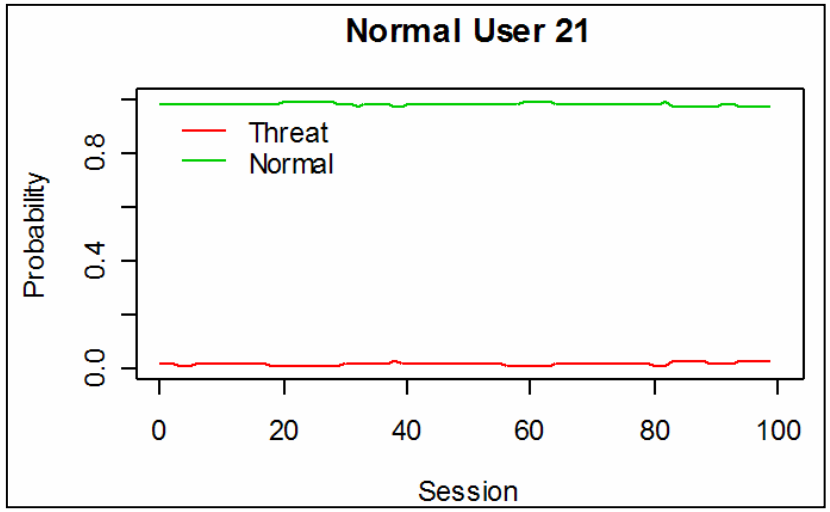


Sample Time Series Plots





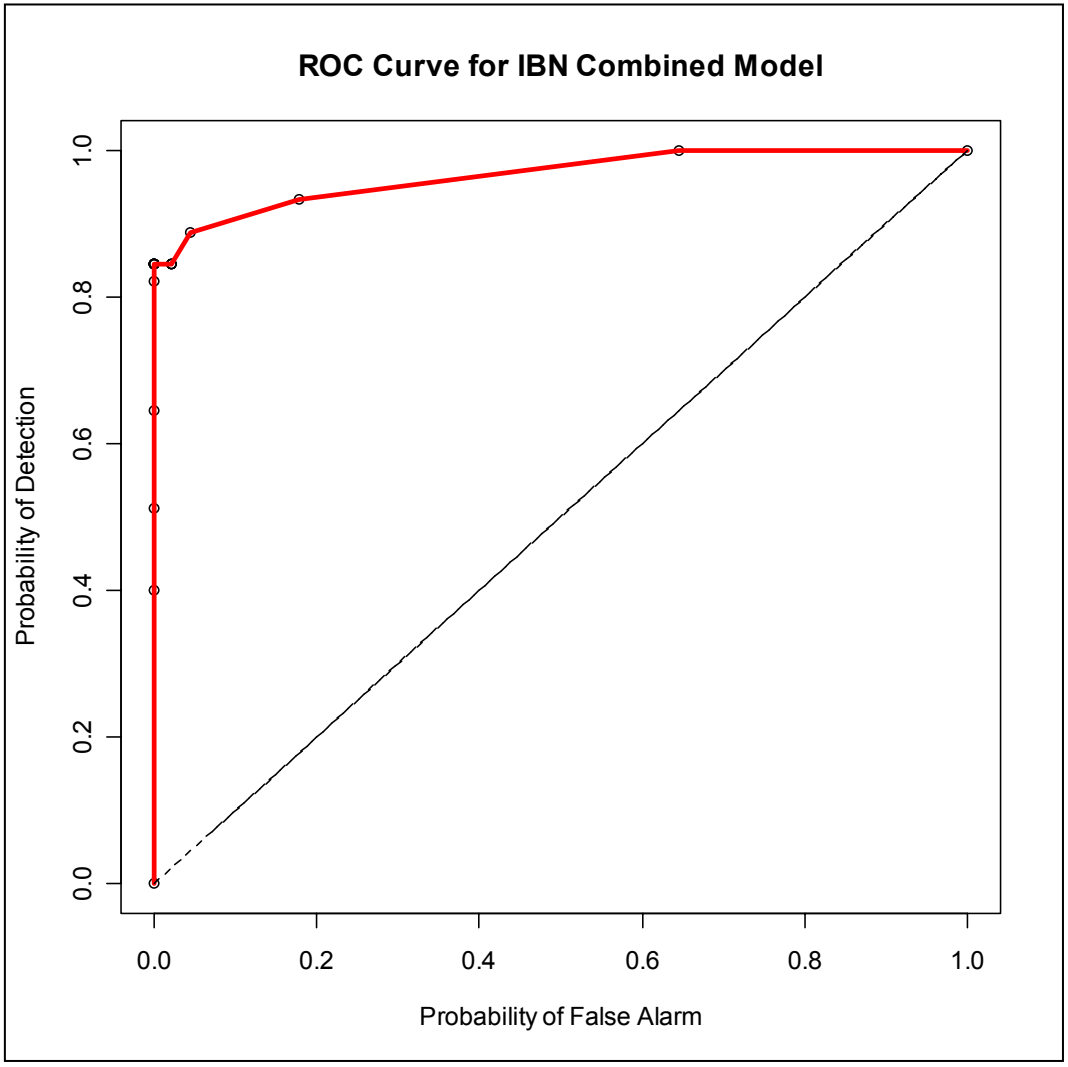




[Screen shots are taken from R Statistical package www.r-project.org]

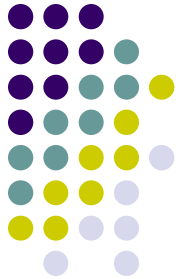
Simulation Results
ROC Curves

- **Document Relevance Model**
  - 2 Queries & 5 Documents:
    - AUC = 0.9121
  - 4 Queries & 6 Documents
    - AUC = 0.9217
  - 6 Queries & 10 Documents
    - AUC = 0.9358
- **Login Times and Attack Tactics Model**
  - AUC = 0.9022
- **Combined Model**
  - AUC = 0.9662



Threshold	0	.005	0.05	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	0.95	0.98	1
True Positive	1	1.0	0.93	0.89	0.84	0.84	0.84	0.84	0.84	0.84	0.82	0.64	0.51	0.4	0
False Positive	1	1	0.64	0.17	0.04	0.02	0.02	0.02	0	0	0	0	0	0	0

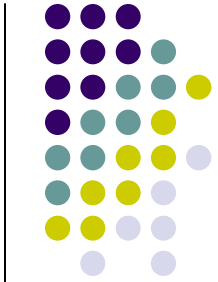
Conclusion



- Developed a novel approach to model insider user behavior using Multi Entity Bayesian network
- Demonstrated the potential of the model to detect insider threat behavior (*proof-of-concept models*)
- The IBN model was able to detect threats with reasonably high *true positive* and low *false positive* rates
- The different experiments produced qualitatively reasonable ROC curves and AUCs
- The performance improved

Future Work

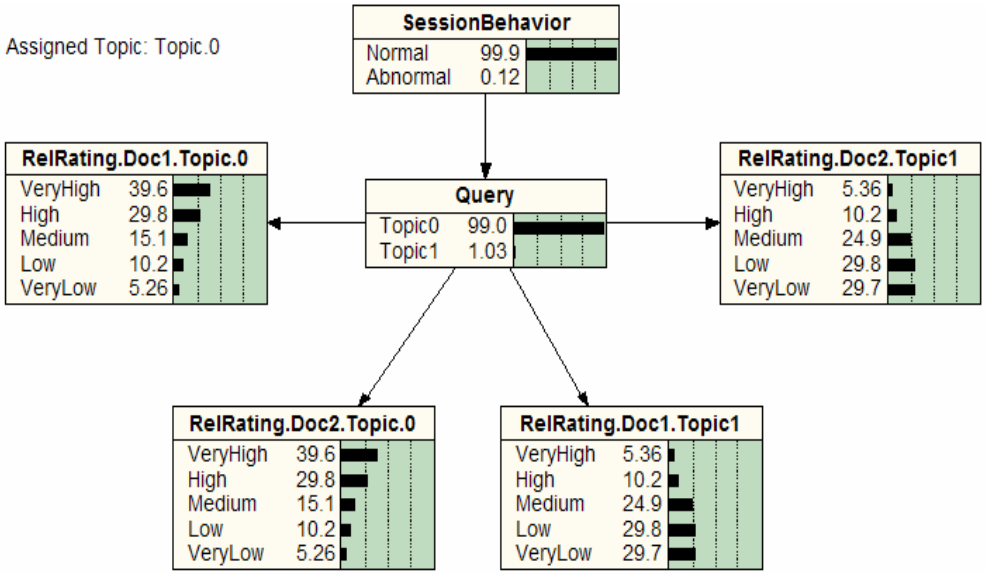
- Learning
- Field testing
- Collaboration between users
- Additional types of threat behavior



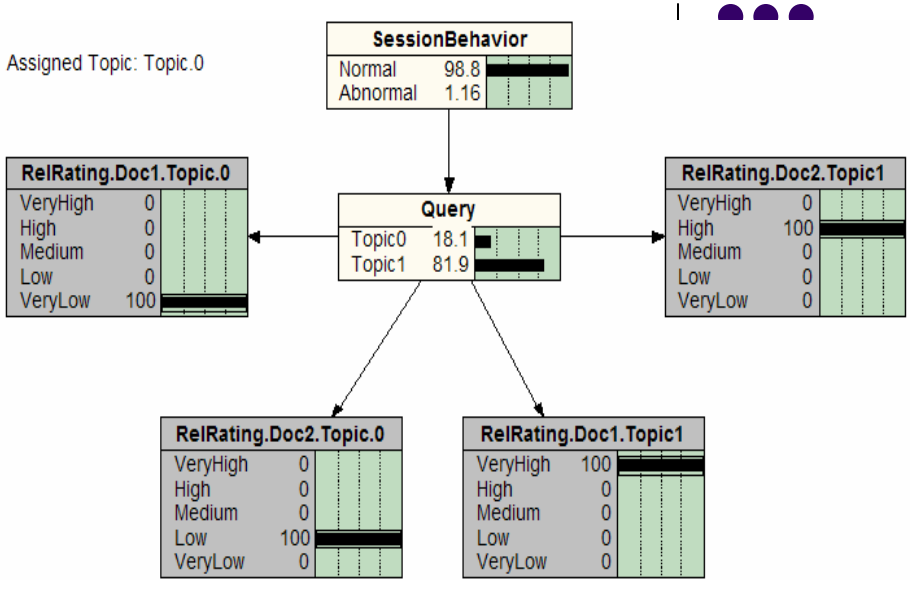
Thank You!

George Mason University

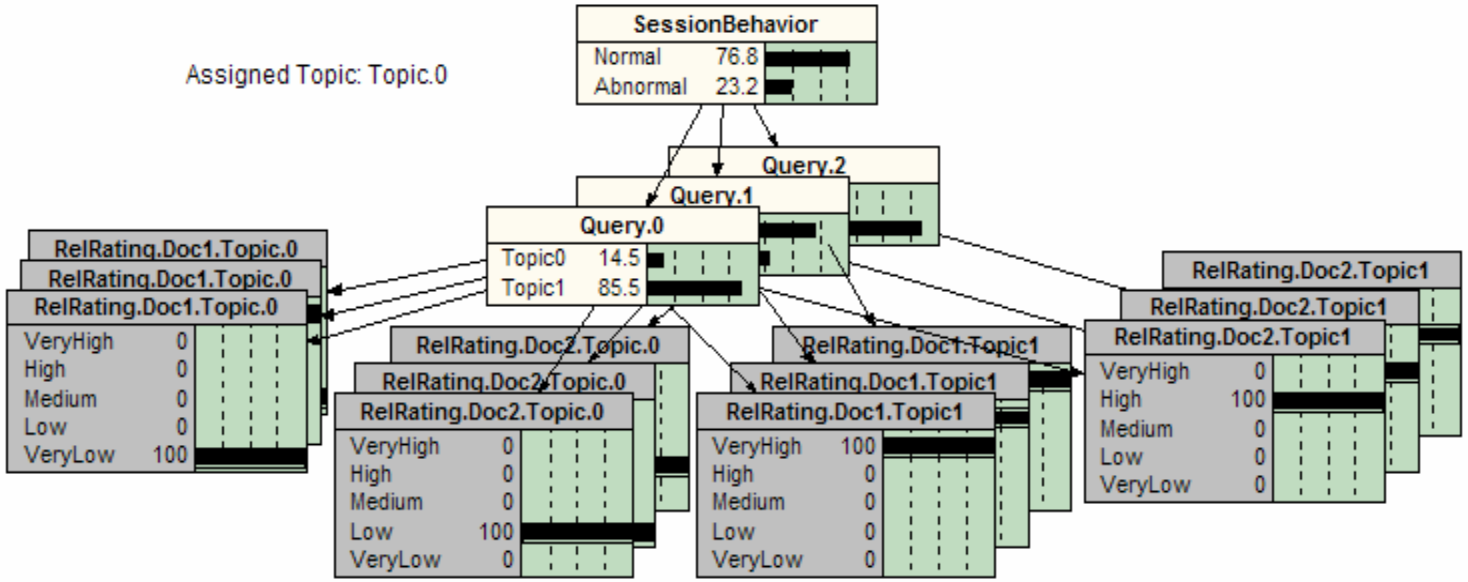
IET



A priori



After one suspicious access event



After multiple suspicious access events