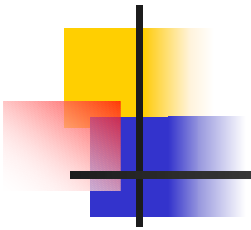
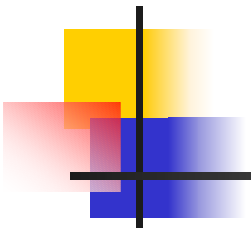


Computer Network Intrusion Detection Via Neural Networks Methods

Vu Dao
phongvu_98@yahoo.com
July 18, 2002

Outline

- Goals
- Background on Intrusion Detection Systems (IDS)
- Types of IDS
- Why Applying Neural Networks Techniques?
- User Profiling in the UNIX OS Environment
- Study of the Proposed Methods
  - Implementation of the Proposed IDS
  - Results
  - Trade-Offs of the Proposed Methods
- Summary
- Future Work



Goals

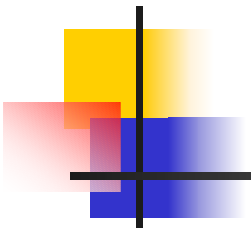
- Design and implement new intrusion detection systems that deal with changes in user profile (i.e. user behavior)
- Compare the proposed methods with other statistical methods to the intrusion detection problem, explain the trade-offs and the potential advantages of the proposed methods

Background on Intrusion Detection Systems

- 1999 DARPA Study [1]
  - Types of Evaluation
    - U2R - User Illegally Became Root (eject, fdformat, ps, …)
    - DoS - Denial of Service (selfping, smurf, tcpreset, …)
    - R2L - Remote User Illegally Accessed a Local Host (guest, ftpwrite, xsnoop, …)
  - Results of Detecting Intruders
    - 80% Success for Old Attacks
    - 25% Success for New and Novel Attacks

DARPA: Defense Advanced Research Project Agency

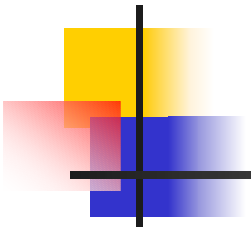
[1] R. Lippmann, et. al., The 1999 DARPA off-line intrusion detection evaluation, Computer Networks, 2000



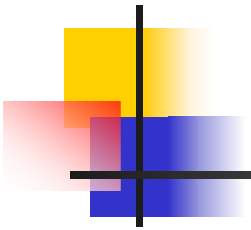
Types of IDS

- Audit-Trail IDS
- Network Monitoring IDS
- Others

Audit-Trail Methods



- Audit-Trail Methods
  - Classical Artificial Intelligence (AI)
    - Statistical or Anomaly
    - Rule-Based, Signature or Misuse
  - Soft-Computing Artificial Intelligence
    - Back Propagation (BP)
    - Radial Basis Function (RBF)
    - Genetic Algorithm (GA)



Research Concentration

- Previous Works Concentrate on System or Network
  - System Traffic or System Log
  - Goal is to Detect Intrusion on System or Network
- This Research Concentrates on User Account
  - Account Traffic or Account Log
  - Goal is to Detect Intrusion on a Specified Account

Why Applying Neural Network?

- Statistical Method
  - Used in Detecting New Attacks
  - Inaccurate
    - 75% Success Rate [2] for currently best research system
- Neural Network Has Self Learning Capability
  - Supervised Learning for Input-Output Mapping
  - Adapt Synaptic Weights to Changes in the Surrounding Environment

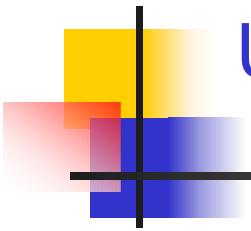
[2] Pete Lindstrom, IDS at the Crossroads, Information Security, June 2002

User Profiling in the UNIX OS Environment (1/2)

- Events Used in User Profiling[3]
  - Activities of the System as a Whole
  - Activities of Users
  - Activities of Particular Terminals
  - Transactions Involving Particularly Sensitive Files or Programs
  - Transactions Involving Particular Sensitive System Files or Programs

[3] Dorothy Denning, “An Intrusion Detection Model,” IEEE Transactions on Software Engineering, 1987

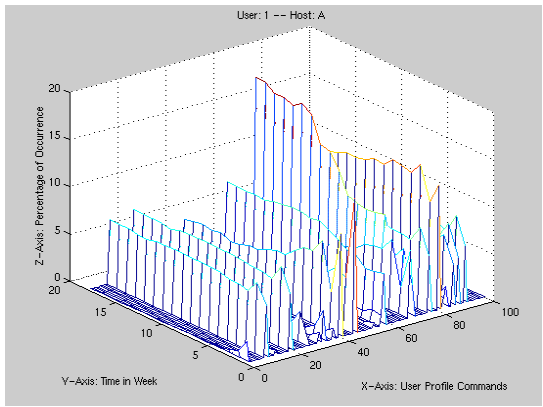
User Profiling in the UNIX OS Environment (2/2)

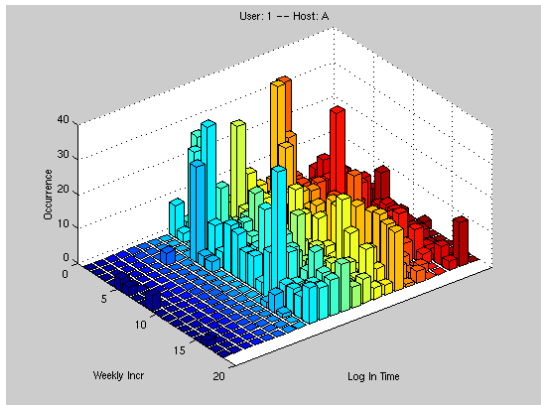


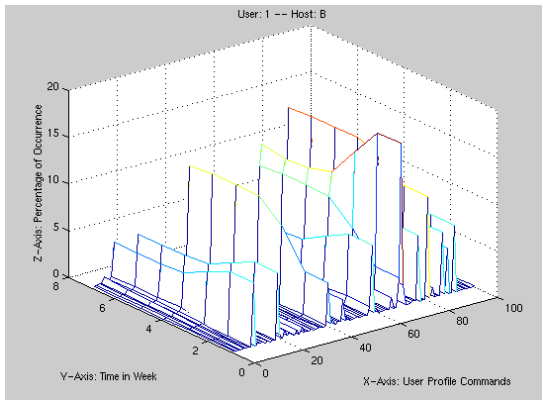
- Attributes of Users in Profiling
  - Command Sets, Time of Login, Host, CPU Time
- Issues in User Profiling [4]
  - Short-Term
    - Constant Profile
  - Long Term
    - Profile Drift
- Case Study

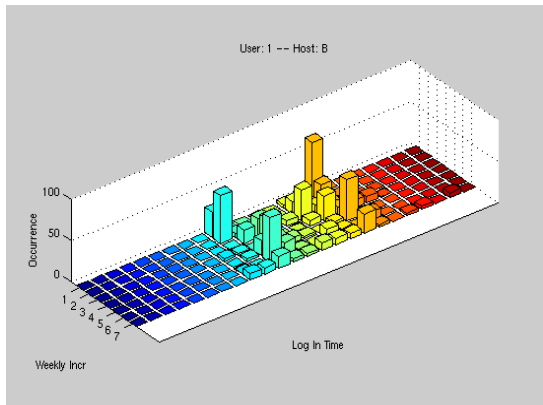
[4] Vu Dao, et. al. “Profiling Users in the UNIX OS Environment”, International Computer Science Conventions Conference, Dec. 2000

User Profiling -- Case Study (1/2)

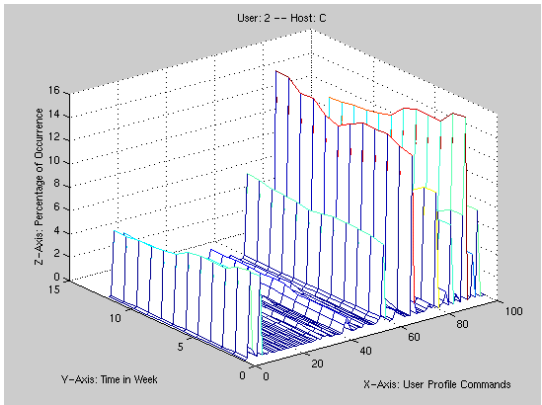


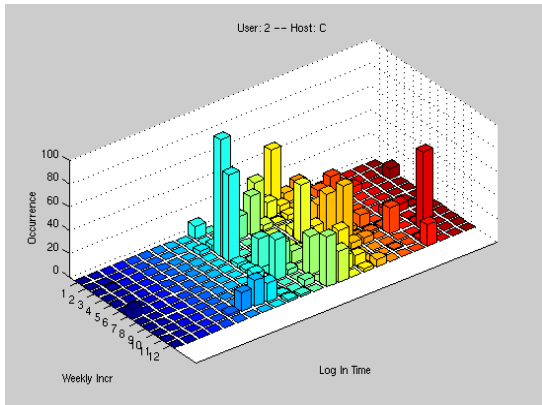


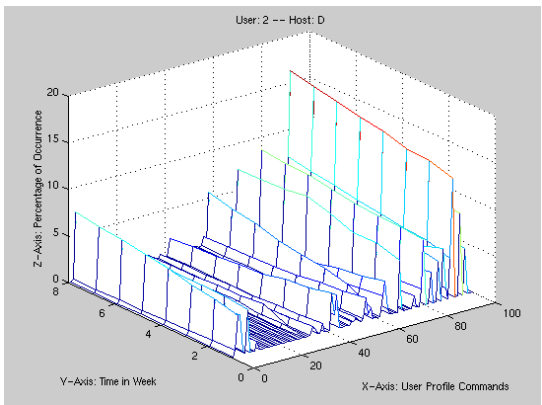


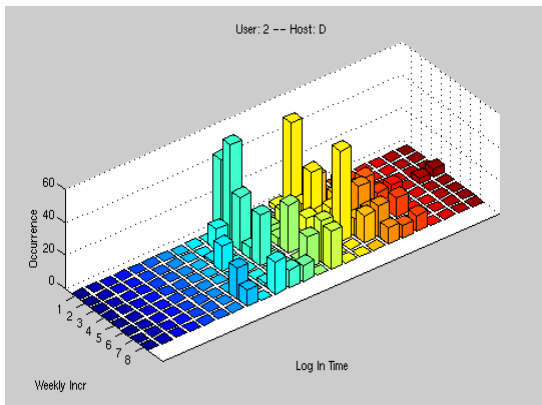


User Profiling -- Case Study (2/2)





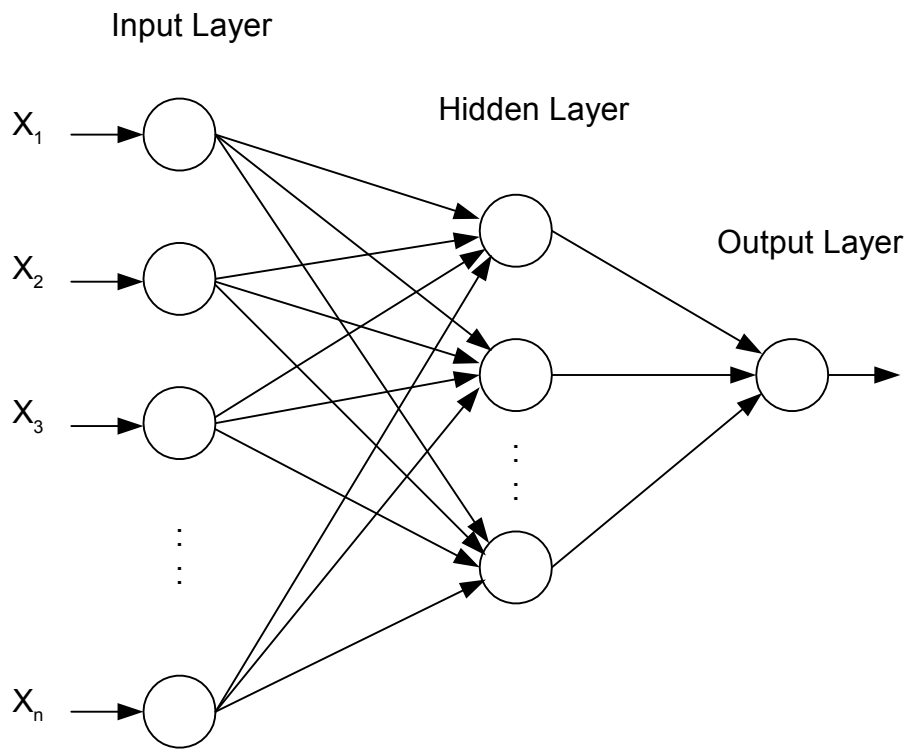




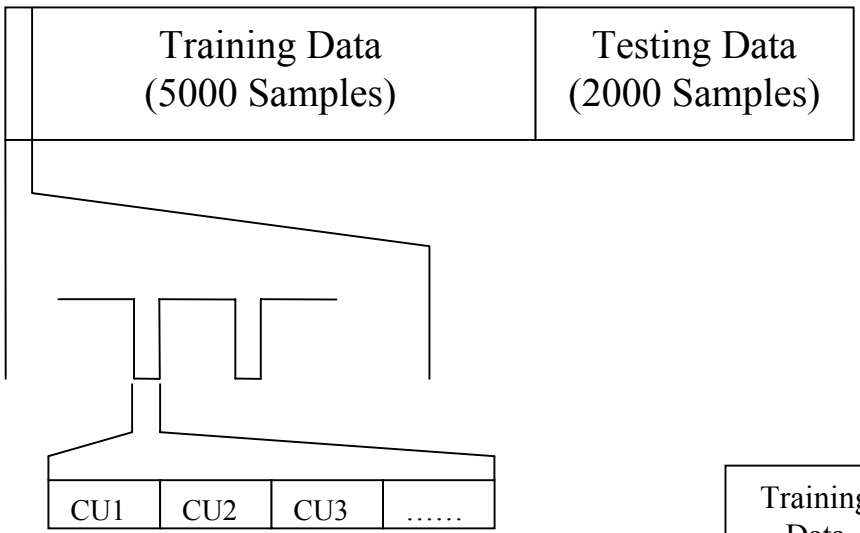
Study of the Proposed Methods

- Neural Network Methods
  - Back Propagation
    - Gradient Descent (GD)
    - Gradient Descent with Momentum
    - Variable Learning Rate GD with Momentum
    - Conjugate Gradient
    - Quasi Newton

Feed Forward Neural Networks

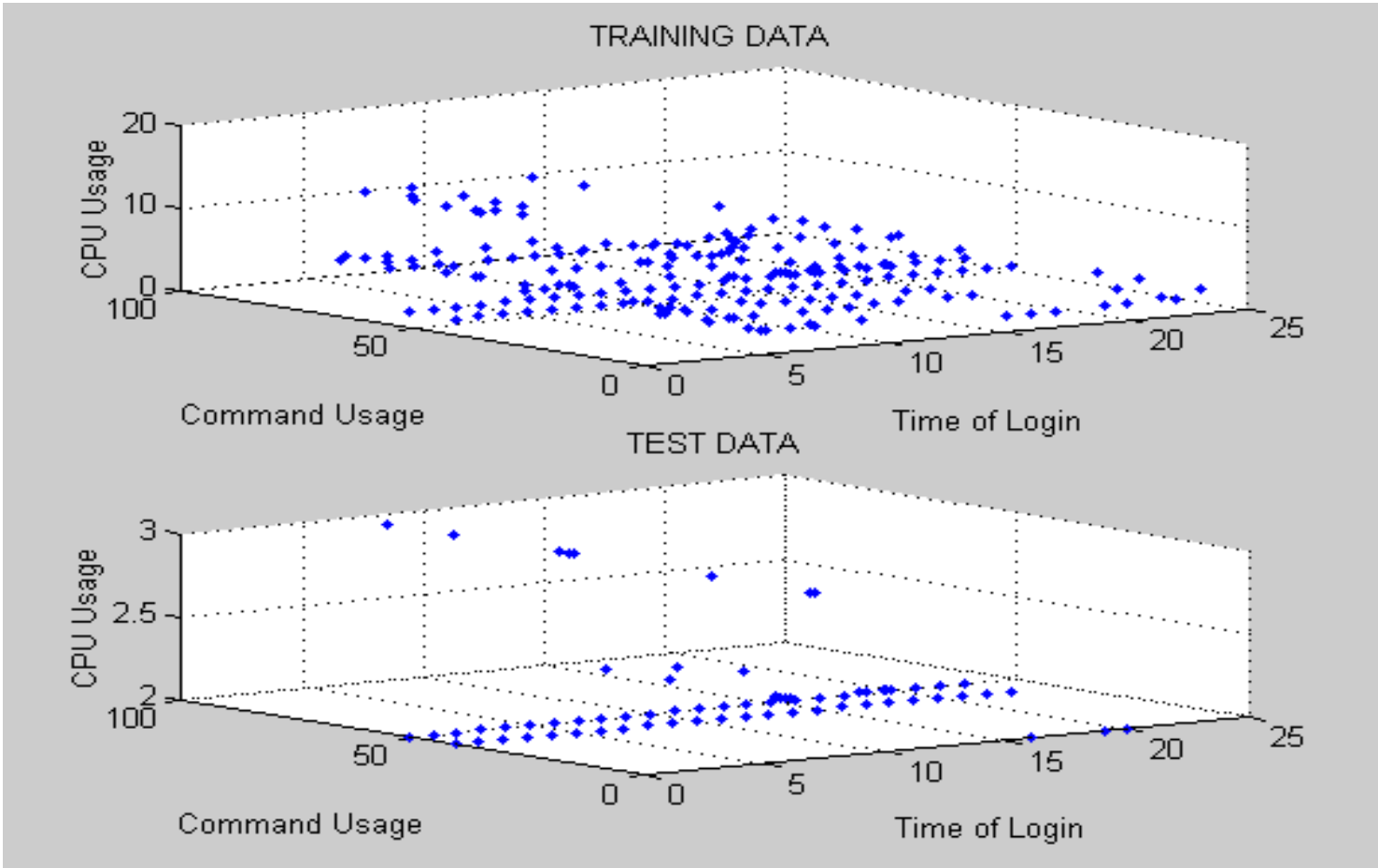


Generated Data File

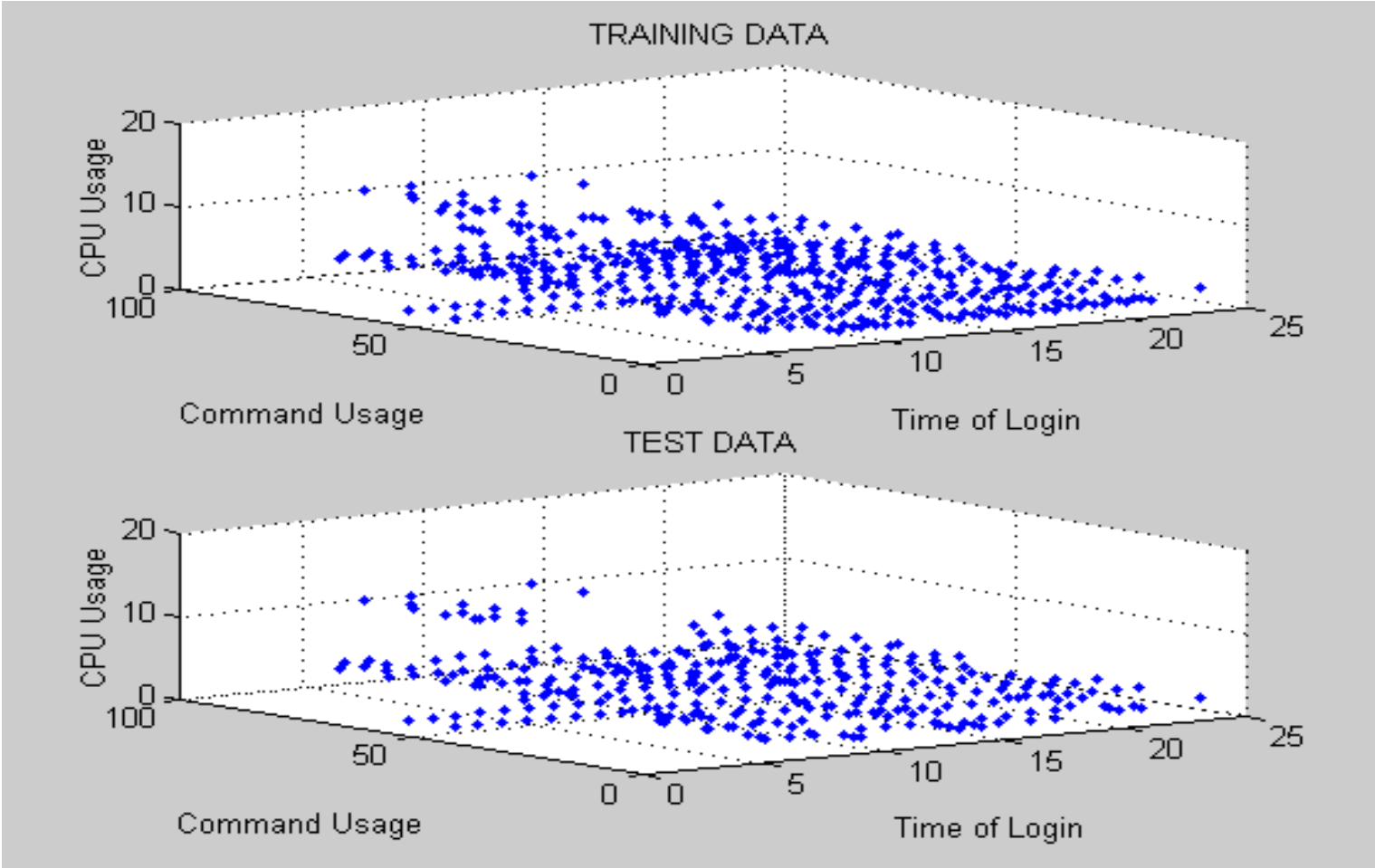


	File 1 CU = 5	File 2 CU = 6	File 3 CU = 7
Training Data	25000	30000	35000
Testing Data	10000	12000	14000
Total	35000	42000	49000

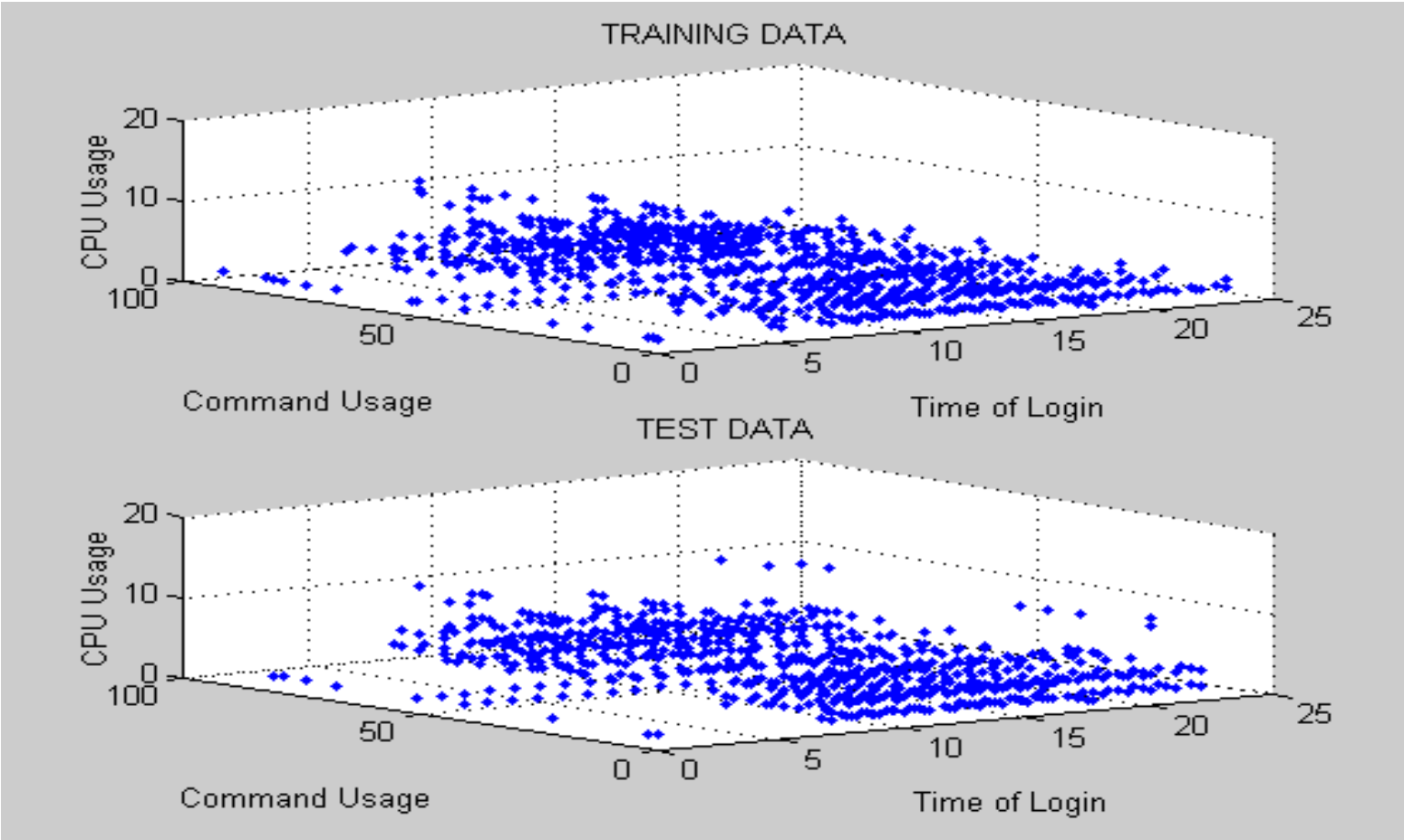
Data set 1, CU = 5



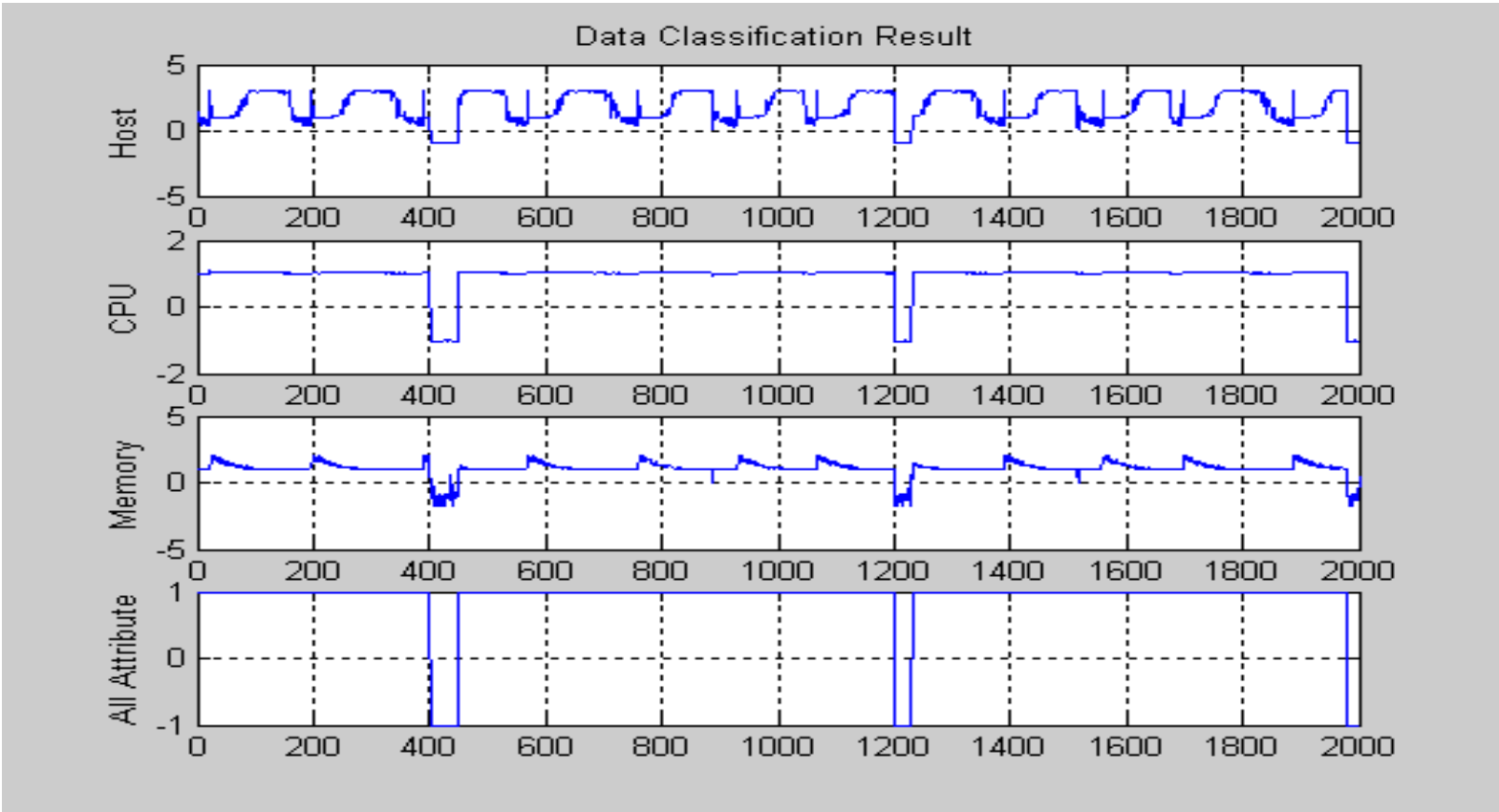
Data set 2, CU = 5



Data set 3, CU = 5

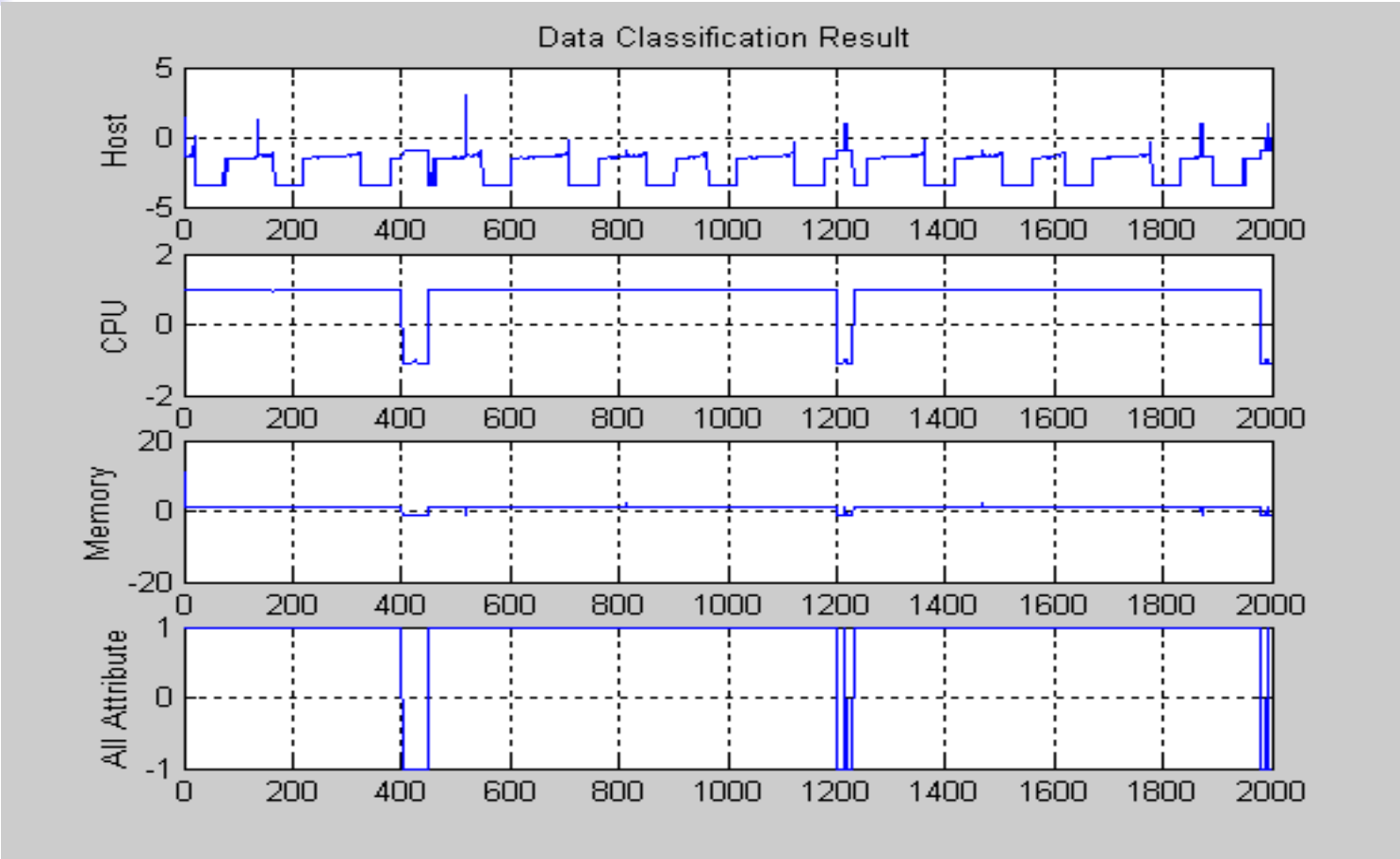


Results (BFGS - 5 Samples) Test Data 1

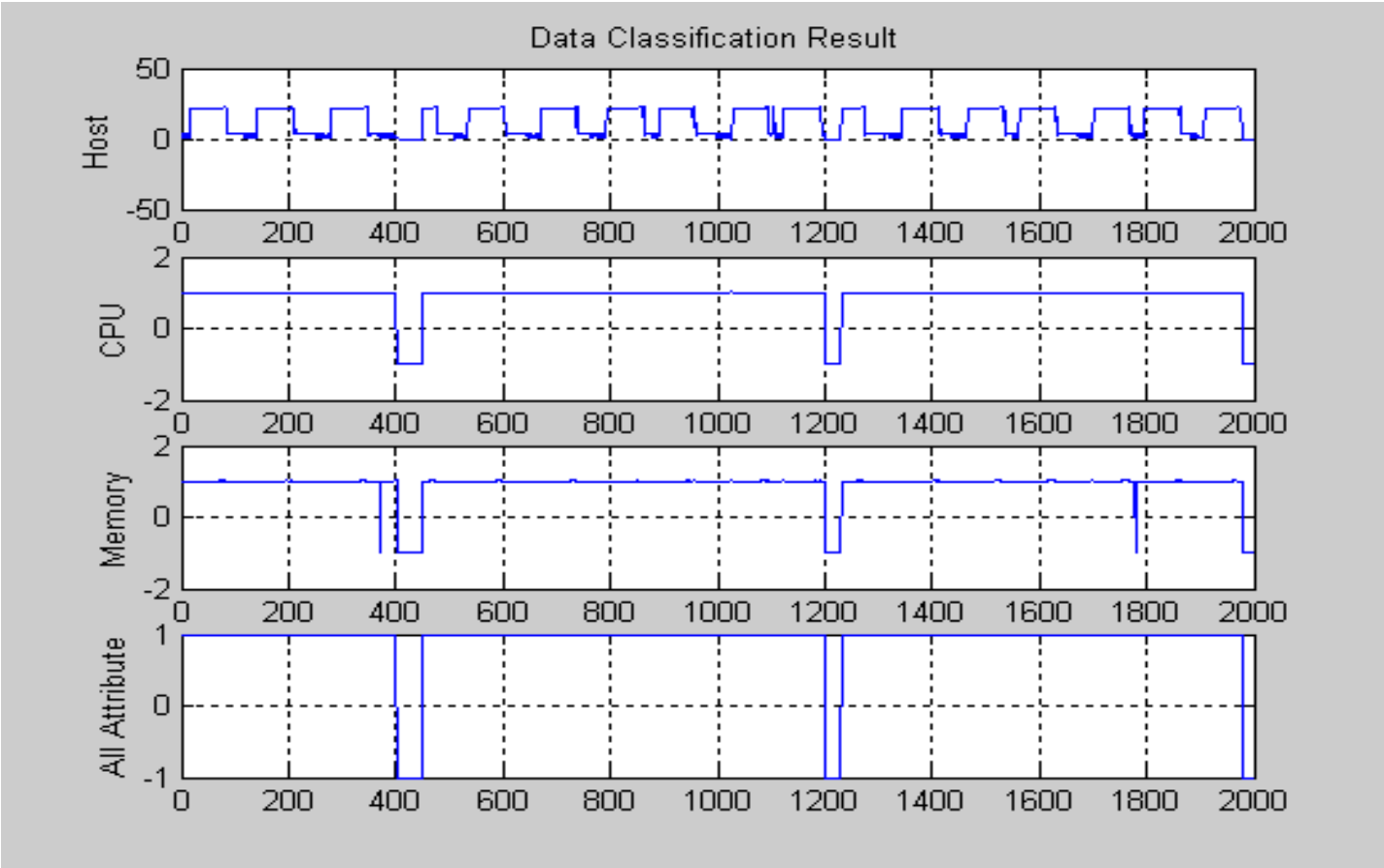


BFGS = Broyden, Fletcher, Goldfarb, Shanno

Results (BFGS - 6 Samples) Test Data 1



Results (BFGS - 7 Samples) Test Data 1



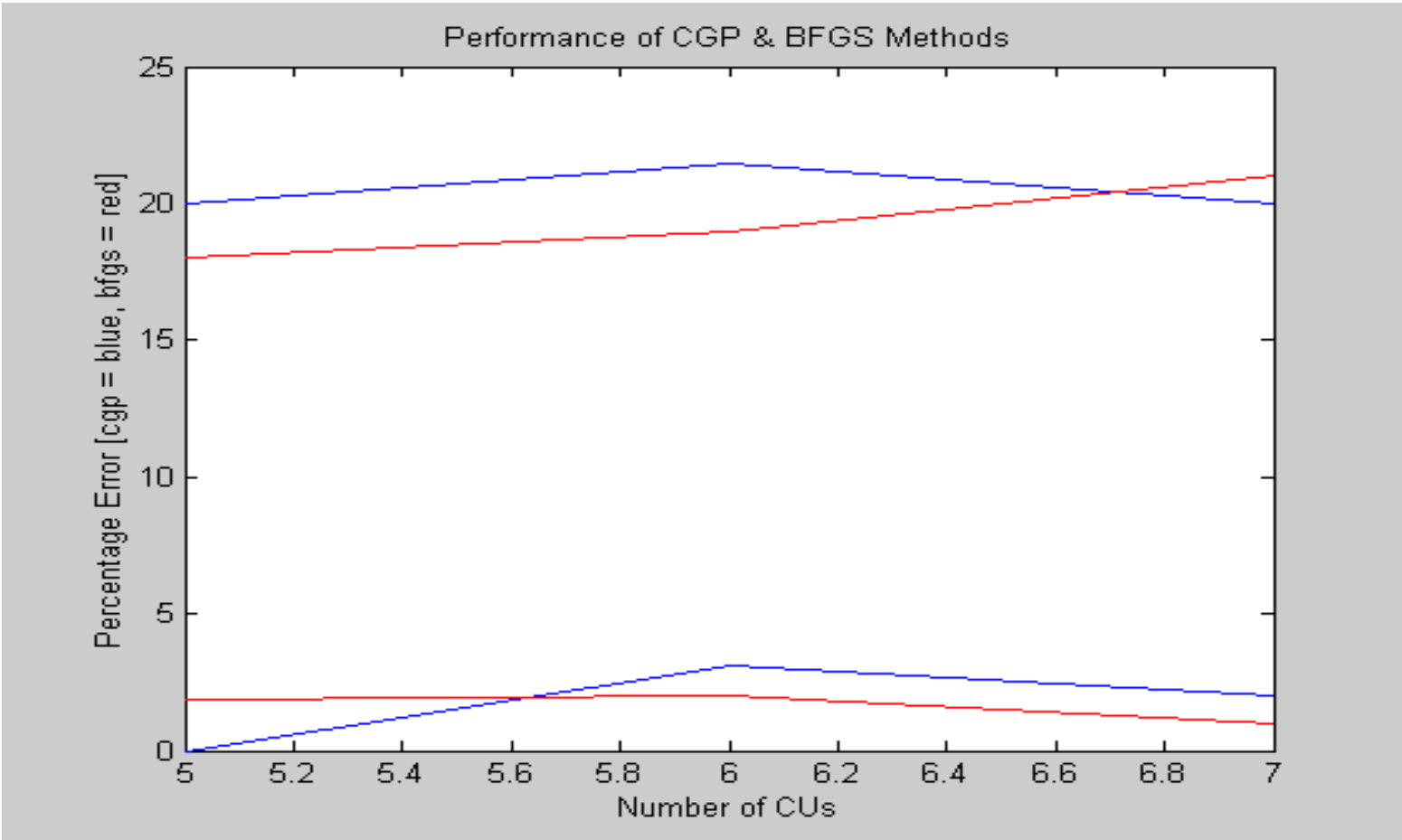
BFGS Result

	CU = 5	CU = 6	CU = 7
Host Error	2.7% 18%	2.5% 19%	1% 21%
CPU Error	3.6% 16%	1.8% 19%	1% 21%
Memory Error	3.1% 18%	3.9% 16%	3.3% 20%
Combined Error	1.9% 18%	2% 19%	1% 21%

CGP Result

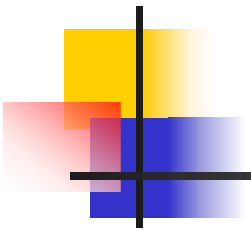
	CU = 5	CU = 6	CU = 7
Host Error	**0.4% 20%**	**1.1% 21.4%**	**2.84% 20%**
CPU Error	**2.0% 2.9%**	**2.23% 18.6%**	**2.0% 17%**
Memory Error	**0.7% 18.5%**	**0.5% 20%**	**3.1% 19%**
Combined Error	**0% 20%**	**0.31% 21.43%**	**2.0% 20%**

Summary Result



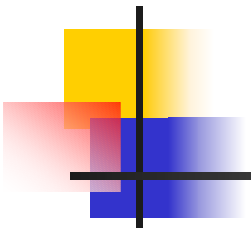
Trade-Offs of the Proposed Methods

- Advantage
  - Adaptive to Profile Drift
  - Software Based Neural Networks
  - Added protection to critical account / system
- Disadvantage
  - Requires More Computing Resources
  - Require Negative Samples to Train Neural Networks
  - Must be configured to each user



Summary

- Profile Computer Users Successfully via Basic Attributes
- Neural Networks Capable of Classifying Users



Future Work

- Implement Other Neural Network Techniques
  - Radial Basis Functions
    - Weights has local affect on neuron
- Use Other User Profile Attributes
- Analyze Results to Improve Performance