Review of "Detecting Anomalous Insiders in Collaborative Information Systems"

You Chen, Steve Nyemba, and Bradley Malin

Ieee Transaction on Dependable and Secure Computing, vol.9, n.3, 2012

Francesco Mucci

Corso di Laurea Magistrale in Informatica

Sistemi Critici e Real Time

Anno accademico 2016-2017

Outline

1. CISs (Collaborative Information Systems) and Anomaly Detection motivation.
2. CADS (Community-based Anomaly Detection System) and MetaCADS frameworks.
3. Experimental analysis of CADS and MetaCADS.
4. Conclusions.

Collaborative Infomation Systems (CISs)

CISs allow groups of users to communicate and cooperate over common tasks in a virtual environment.

CISs examples:

- Time Management Software;
- Project Management Systems;
- Knowledge Management Systems.

Collaborative Infomation Systems (CISs)

CISs allow groups of users to communicate and cooperate over common tasks in a virtual environment.

CISs in Internet:

- Wikis;
- video conferencing;
- document sharing and editing.

Collaborative Infomation Systems (CISs)

CISs allow groups of users to communicate and cooperate over common tasks in a virtual environment.

CISs to manage sensitive informations:

- CIS environments for intelligence agencies;
- Electronic Health Record (EHR) system: CIS to manage data of patient in electronic form.

Anomaly detection's motivation: outside vs insider threats

Sensitive information in CIS ⟵ target for Adversaries (Attackers).

Categories of Attackers in relation to the CIS environment:

- outside threats;
- insider threats.

Mitigate outside threats:

- cryptographic protocols;
- access control.

Anomaly detection's motivation: outside vs insider threats

Sensitive information in CIS $\longleftarrow$ target for Adversaries (Attackers).

Our setting:

- insider threats;
- centralized CIS managed by a sole organization;
- suspicious insider == authenticated user whose actions run counter to the organization's policies.

Anomaly detection's motivation: deal with internal threats

Our problem:

1. detection of insider threats;
2. the mitigation of risk in exposing sensitive information.

Security mechanisms to address this problem:

- Access and Permission Control;
- Anomaly Detection.

Anomaly detection's motivation: access control is not enough to face internal threats

Access control models notable with respect to CIS:

- Access Matrix Model (AMM)
- Role-Based Access Control (RBAC)
- Task-Based Access Control (TBAC)
- Team-Based Access Control (TeBAC)

Access control models's behaviour:

- manage each user (or group) as an independent entity;
- work under the expectation of a static environment.

Anomaly detection's motivation: access control is not enough to face internal threats

Access control models's behaviour:

- manage each user (or group) as an independent entity;
- work under the expectation of a static environment.

But in CISs:

- relational environments;
- teams constructed on-the-fly.

Anomaly Detection

Anomaly detection techniques are designed to utilize patterns of system use or user's behavior pattern to determine if any particular user is sufficiently different than expected.

Supervised Anomaly Detection:

labeled training instances are provided to parameterize a classification model; the resulting models are then applied to classify new actions into one (or more) of the labels.

- K-nearest neighbors (KNN).
- Principle components analysis (PCA).

Anomaly Detection

Anomaly detection techniques are designed to utilize patterns of system use or user's behavior pattern to determine if any particular user is sufficiently different than expected.

Unsupervised Anomaly Detection:

uses the inherent structure, or patterns, in a dataset to determine when a particular instance is sufficiently different.

- High volume users (HVUs).

Contributions of this paper

Unsupervised Anomaly Detection Framework:

- Community-based Anomaly Detection System (CADS).
- CADS extension: MetaCADS.

Framework's idea:

- in CIS, users team/goal oriented ⇒
- user should exhibit similar behavior to other users based on their co-access of similar subjects.

Contributions of this paper

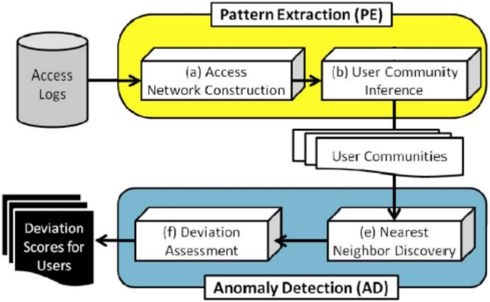
Unsupervised Anomaly Detection Framework:

- Community-based Anomaly Detection System (CADS).
- CADS extension: MetaCADS.

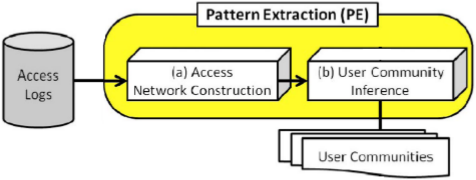
CADS for dummies:

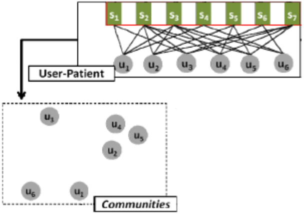
1. from co-access pattern, establishment of user communities pattern as a core set of representative patterns;
2. predict which users are anomalous by measuring their distance to such communities.

Community-based Anomaly Detection System (CADS)

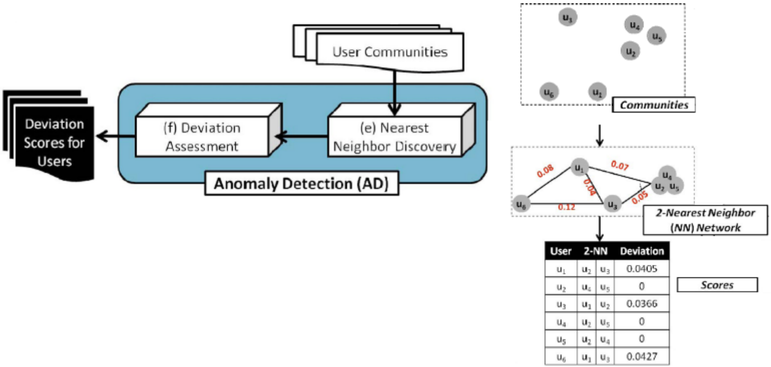

Pattern Extraction (PE)
Access Logs
(a) Access Network Construction
(b) User Community Inference
User Communities
Deviation Scores for Users
(f) Deviation Assessment
(e) Nearest Neighbor Discovery
Anomaly Detection (AD)

Community-based Anomaly Detection System (CADS)



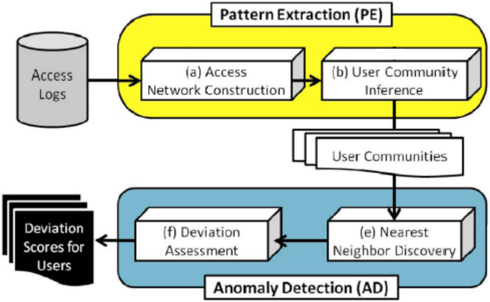

s_1 s_2 s_3 s_4 s_5 s_6 s_7
u_1 u_2 u_3 u_4 u_5 u_6
User-Patient
u_3 u_4 u_5 u_2 u_6 u_1
Communities

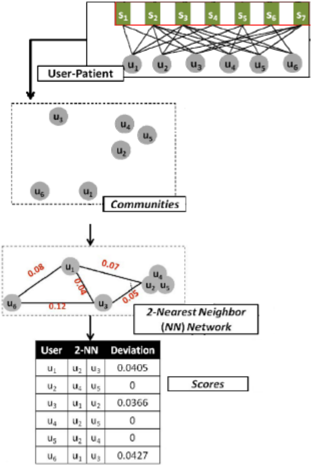
Community-based Anomaly Detection System (CADS)



User	2-NN		Deviation
u_1	u_2	u_3	0.0405
u_2	u_4	u_5	0
u_3	u_1	u_2	0.0366
u_4	u_2	u_5	0
u_5	u_2	u_4	0
u_6	u_1	u_3	0.0427

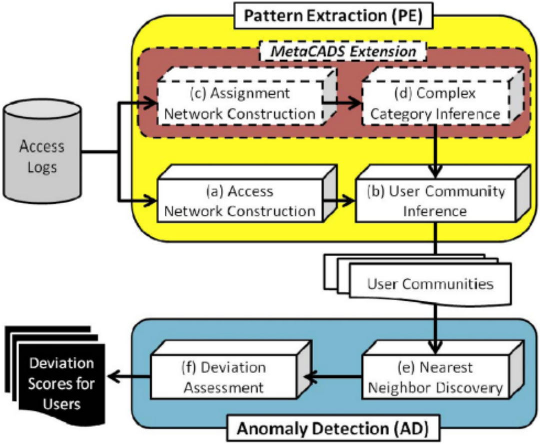
Community-based Anomaly Detection System (CADS)


Pattern Extraction (PE)
Access Logs
(a) Access Network Construction
(b) User Community Inference
User Communities
Deviation Scores for Users
(f) Deviation Assessment
(e) Nearest Neighbor Discovery
Anomaly Detection (AD)

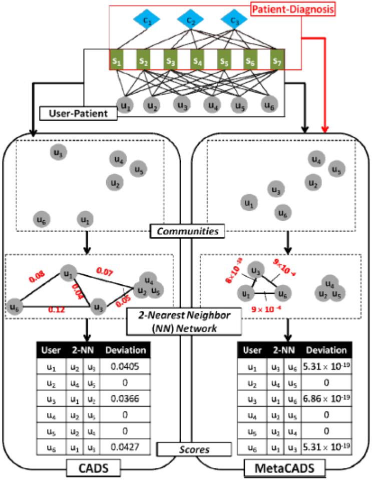


User	2-NN		Deviation
u_1	u_2	u_3	0.0405
u_2	u_4	u_5	0
u_3	u_1	u_2	0.0366
u_4	u_2	u_5	0
u_5	u_2	u_4	0
u_6	u_1	u_3	0.0427

MetaCADS


Pattern Extraction (PE)
MetaCADS Extension
(c) Assignment Network Construction
(d) Complex Category Inference
Access Logs
(a) Access Network Construction
(b) User Community Inference
User Communities
Deviation Scores for Users
(f) Deviation Assessment
(e) Nearest Neighbor Discovery
Anomaly Detection (AD)

Differences between CADS and MetaCADS



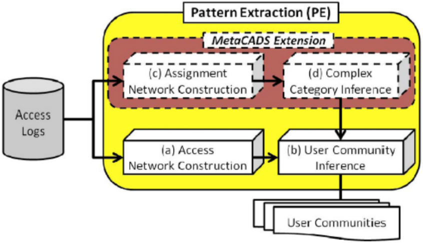
CADS

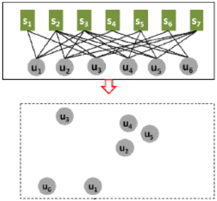
User	2-NN		Deviation
u_1	u_2	u_3	0.0405
u_2	u_4	u_5	0
u_3	u_1	u_2	0.0366
u_4	u_2	u_5	0
u_5	u_2	u_4	0
u_6	u_1	u_3	0.0427

MetaCADS

User	2-NN		Deviation
u_1	u_3	u_6	5.31×10^{-19}
u_2	u_4	u_5	0
u_3	u_1	u_6	6.86×10^{-19}
u_4	u_2	u_5	0
u_5	u_2	u_4	0
u_6	u_1	u_3	5.31×10^{-19}

CADS-PE (Pattern Extraction): steps

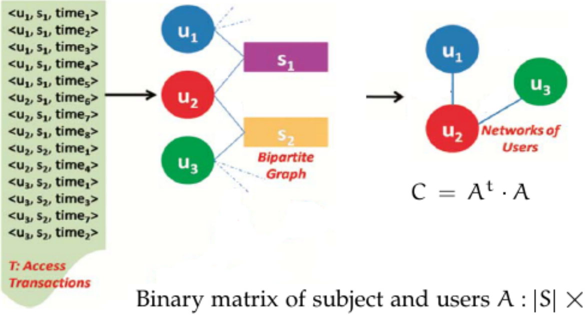

Pattern Extraction (PE)
MetaCADS Extension
(c) Assignment Network Construction
(d) Complex Category Inference
Access Logs
(a) Access Network Construction
(b) User Community Inference
User Communities



→ Bipartite Graph->Access Network of Users

→ Communities via Singular Value Decomposition

CADS-PE Network Construction: Access-log → Access Network → Relational Network of Users



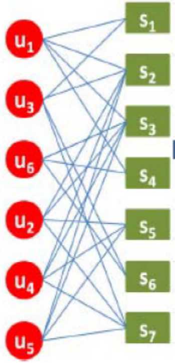
$\langle u_1, s_1, time_1\rangle$
$\langle u_1, s_1, time_2\rangle$
$\langle u_1, s_1, time_3\rangle$
$\langle u_1, s_1, time_4\rangle$
$\langle u_1, s_1, time_5\rangle$
$\langle u_2, s_1, time_6\rangle$
$\langle u_2, s_1, time_7\rangle$
$\langle u_2, s_1, time_8\rangle$
$\langle u_2, s_2, time_1\rangle$
$\langle u_2, s_2, time_4\rangle$
$\langle u_3, s_2, time_1\rangle$
$\langle u_3, s_2, time_3\rangle$
$\langle u_3, s_2, time_7\rangle$
$\langle u_3, s_2, time_2\rangle$

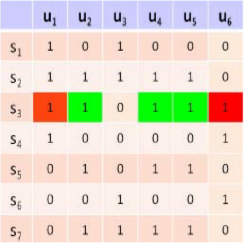
$$C = A^t \cdot A$$

Binary matrix of subject and users $A : |S| \times |U|$

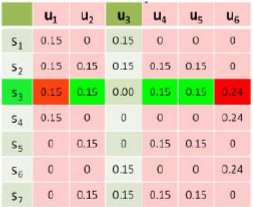
$$A(i,j) := \begin{cases} 1, & \text{se user-j accede al subject-i,} \\ 0, & \text{altrimenti.} \end{cases}$$

CADS-PE Network Construction: IDF Matrix of Subject and Users





	u_1	u_2	u_3	u_4	u_5	u_6
s_1	1	0	1	0	0	0
s_2	1	1	1	1	1	0
s_3	1	1	0	1	1	1
s_4	1	0	0	0	0	1
s_5	0	1	0	1	1	0
s_6	0	0	1	0	0	1
s_7	0	1	1	1	1	0



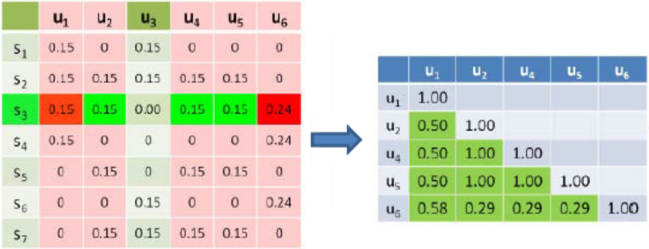
	u_1	u_2	u_3	u_4	u_5	u_6
s_1	0.15	0	0.15	0	0	0
s_2	0.15	0.15	0.15	0.15	0.15	0
s_3	0.15	0.15	0.00	0.15	0.15	0.24
s_4	0.15	0	0	0	0	0.24
s_5	0	0.15	0	0.15	0.15	0
s_6	0	0	0.15	0	0	0.24
s_7	0	0.15	0.15	0.15	0.15	0

$$A_I(i,j) = A(i,j) * IDF(i,j)$$

$$IDF(i,j) = \log \frac{|S|}{1+|s_i, where A(i,j)>0|}$$

$$A_I(i,j) := \begin{cases} 0, & \text{se } A(i,j) = 0, \\ \log \frac{|S|}{1+C(j,j)}, & \text{se } A(i,j) \neq 0. \end{cases}$$

CADS-PE Community Inference: Similarity Matrix of Pair of User

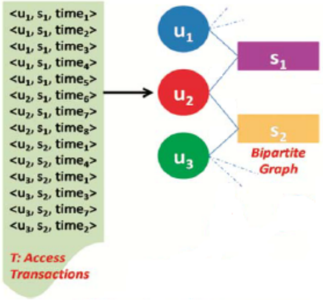


	u_1	u_2	u_3	u_4	u_5	u_6
s_1	0.15	0	0.15	0	0	0
s_2	0.15	0.15	0.15	0.15	0.15	0
s_3	0.15	0.15	0.00	0.15	0.15	0.24
s_4	0.15	0	0	0	0	0.24
s_5	0	0.15	0	0.15	0.15	0
s_6	0	0	0.15	0	0	0.24
s_7	0	0.15	0.15	0.15	0.15	0

	u_1	u_2	u_4	u_5	u_6
u_1	1.00				
u_2	0.50	1.00			
u_4	0.50	1.00	1.00		
u_5	0.50	1.00	1.00	1.00	
u_6	0.58	0.29	0.29	0.29	1.00

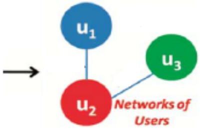
$$\hat{R}(i,j) = \mathrm{Sim}(u_i, u_j) = \mathrm{Cosine}(U_i, U_j) = \frac{u_i^t \cdot u_j}{\|U_i\|_2 * \|U_j\|_2}$$

CADS-PE Community Inference: Communities via Singular Value Decomposition



$\langle u_1, s_1, time_1 \rangle$
$\langle u_1, s_1, time_2 \rangle$
$\langle u_1, s_1, time_3 \rangle$
$\langle u_1, s_1, time_4 \rangle$
$\langle u_1, s_1, time_5 \rangle$
$\langle u_2, s_1, time_6 \rangle$
$\langle u_2, s_1, time_7 \rangle$
$\langle u_2, s_1, time_8 \rangle$
$\langle u_2, s_2, time_1 \rangle$
$\langle u_2, s_2, time_4 \rangle$
$\langle u_3, s_2, time_1 \rangle$
$\langle u_3, s_2, time_3 \rangle$
$\langle u_3, s_2, time_7 \rangle$
$\langle u_3, s_2, time_2 \rangle$

T: Access Transactions



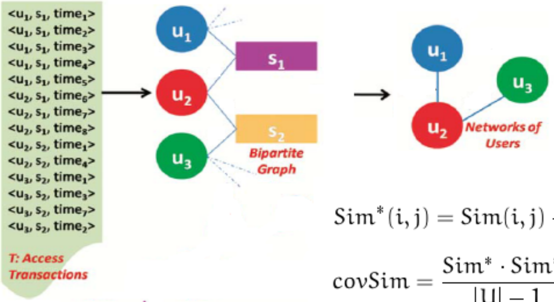
$$\mathrm{Sim}^*(i,j) = \mathrm{Sim}(i,j) - \frac{\mathrm{sum}(\mathrm{Sim}(i,))}{|U|}$$

$$\mathrm{covSim} = \frac{\mathrm{Sim}^* \cdot \mathrm{Sim}^{*t}}{|U| - 1}$$

$$\mathrm{SVD}(\mathrm{covSim}) = \Omega * \Lambda * V^t$$

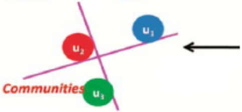
Method for transforming correlated variables into a set of uncorrelated ones that better expose the various relationships among the original data items; and for identifying and ordering the dimensions along which data points exhibit the most variation.

CADS-PE Community Inference: Communities via Singular Value Decomposition


$\langle u_1, s_1, time_1 \rangle$
$\langle u_1, s_1, time_2 \rangle$
$\langle u_1, s_1, time_3 \rangle$
$\langle u_1, s_1, time_4 \rangle$
$\langle u_1, s_1, time_5 \rangle$
$\langle u_2, s_1, time_6 \rangle$
$\langle u_2, s_1, time_7 \rangle$
$\langle u_2, s_1, time_8 \rangle$
$\langle u_2, s_2, time_1 \rangle$
$\langle u_2, s_2, time_4 \rangle$
$\langle u_3, s_2, time_1 \rangle$
$\langle u_3, s_2, time_3 \rangle$
$\langle u_3, s_2, time_7 \rangle$
$\langle u_3, s_2, time_7 \rangle$
T: Access Transactions
u_1
u_2
u_3
s_1
s_2
Bipartite Graph
u_1
u_3
u_2
Networks of Users

$$Sim^*(i,j) = Sim(i,j) - \frac{sum(Sim(i,))}{|U|}$$

$$covSim = \frac{Sim^* \cdot Sim^{*t}}{|U|-1}$$



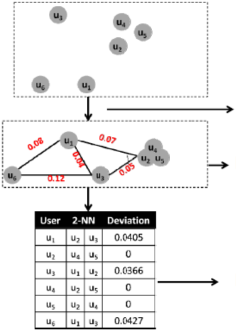
$$SVD(covSim) = \Omega * \Lambda * V^t$$

$$Z = V^t \cdot Sim$$

$$Z_j = [Z_{1j}, Z_{2j}, ...Z_{nj}]$$

Each row in matrix Z is the projection of all users on a principal component, or community;
the j-th user can be presented as the j-th column of Z.

CADS-AD (Anomaly Detection): steps

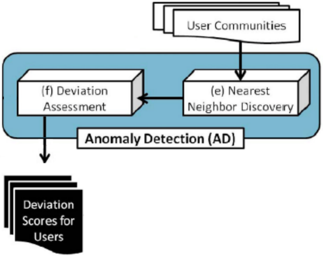


User	2-NN		Deviation
u_1	u_2	u_3	0.0405
u_2	u_4	u_5	0
u_3	u_1	u_2	0.0366
u_4	u_2	u_5	0
u_5	u_2	u_4	0
u_6	u_1	u_3	0.0427

Distance via Weighted Euclidean Distance

Nearest Neighbor Network

Deviation Scores Calculation



CADS-AD search for the k-nearest neighbors (KNNs): CADS-PE community structure → Distance matrix

Modified Euclidean Distance:

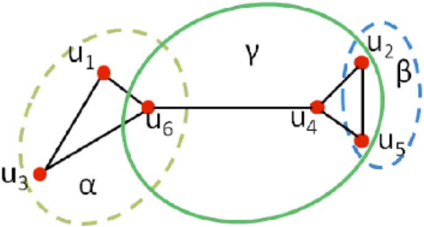
$$D(i,j) = Dis(u_i, u_j) = \sqrt{\sum_{q=1}^{l} (Z_{qi} - Z_{qj})^2 \cdot \frac{\lambda_q}{\lambda_{tot}}}$$

$$\lambda_{tot} = \sum_{j}^{l} \lambda_j.$$

This measure weights the principal components proportionally to the amount of variance they cover in the system.

These distances are stored in a matrix D of size $|U| \times |U|$, where $D(i,j)$ indicates the distance between u_i and u_j.

CADS-AD search for the *k*-nearest neighbors (KNNs): "*k*"-NNs? Conductance, a measure of network quality



$$\psi(A) = \frac{N_A}{\min(vol(A), vol(V - A))}$$

$$N_A = |(g,h) : g \in A, h \notin A|$$

$$vol(A) = \sum_{y \in A} deg(y)$$

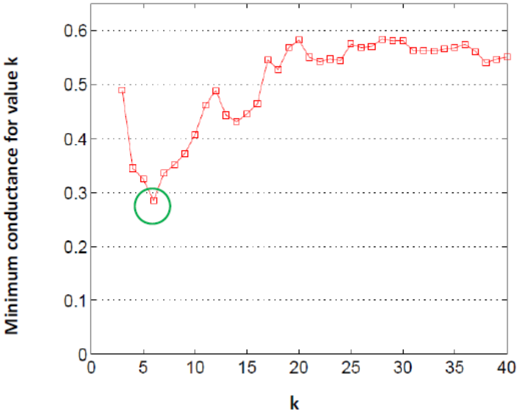
$$\psi(\alpha) = \frac{1}{\min(7,7)} = \frac{1}{7}$$

$$\psi(\beta) = \frac{2}{\min(4,10)} = \frac{2}{4} \qquad \psi(\alpha) < \psi(\beta) = \psi(\gamma)$$

$$\psi(\gamma) = \frac{2}{\min(4,10)} = \frac{2}{4}$$

CADS-AD search for the k-nearest neighbors (KNNs): Distance matrix graph $\rightarrow$ value of k

Minimum conductance at k=6

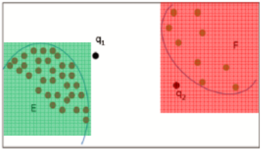


CADS-AD measuring Deviation from k-NN

How to measure deviation from nearest neighbors?

- Every user can be assigned a radius value *r* by recording the distance to his *k*th nearest neighbor.
- The smaller the radius, the higher density of the user's network.

5 nearest



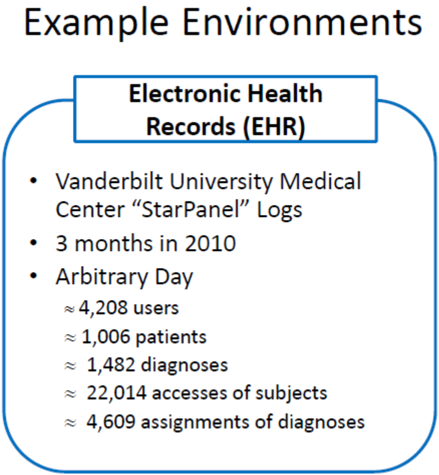
Radius for points in the green area are 1, and for q₁ is 3

Radius for points are larger than 10

$$\mathrm{Dev}(u_i) = \sqrt{\frac{\sum_{u_j \in knn_i} (r_j - \bar{r})^2}{k-1}}$$

$$\bar{r} = \frac{\sum_{u_j \in knn_i} r_j}{k}$$

Experimental Analysis of CADS and MetaCADS: EHR "StarPanel"



Example Environments

Electronic Health Records (EHR)

- Vanderbilt University Medical Center “StarPanel” Logs
- 3 months in 2010
- Arbitrary Day

  ≈ 4,208 users

  ≈ 1,006 patients

  ≈ 1,482 diagnoses

  ≈ 22,014 accesses of subjects

  ≈ 4,609 assignments of diagnoses

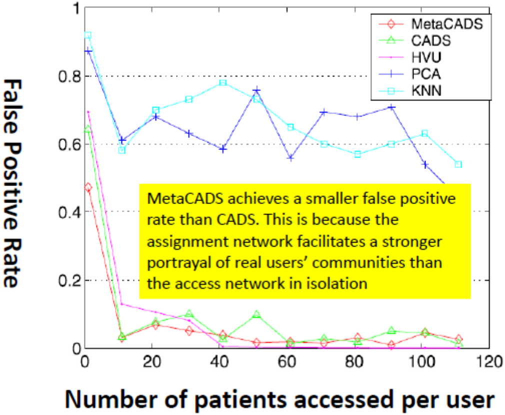
Experimental Analysis of CADS and MetaCADS: Experimental Design

Users were simulated in several settings to test:

1. Sensitivity to number of patients accessed of a specific users:
   - fixed number of simulated-user;
   - random number of subject (range from 1 to 120) accessed by simulated-user.
2. Sensitivity to number of anomalous users:
   - simulated users from 0.5% to 5% of total users;
   - number of records accessed by simulated user fixed to 5.
3. Sensitivity to diversity:
   - random number of simulated users (from 0.5% to 5%);
   - random number of records accessed by simulated users (from 1 to 150).

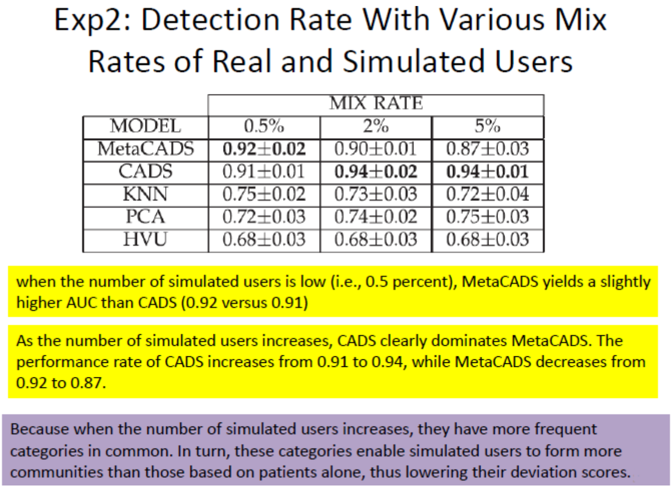
Experimental Analysis of CADS and MetaCADS: Sensitivity to number of patients accessed of a specific users

Exp1: False Positive Rate Decreases, when the Number of Subjects Accessed Increases



MetaCADS achieves a smaller false positive rate than CADS. This is because the assignment network facilitates a stronger portrayal of real users' communities than the access network in isolation

Experimental Analysis of CADS and MetaCADS: Sensitivity to number of anomalous users



Exp2: Detection Rate With Various Mix Rates of Real and Simulated Users

	MIX RATE		
MODEL	0.5%	2%	5%
MetaCADS	**0.92±0.02**	0.90±0.01	0.87±0.03
CADS	0.91±0.01	**0.94±0.02**	**0.94±0.01**
KNN	0.75±0.02	0.73±0.03	0.72±0.04
PCA	0.72±0.03	0.74±0.02	0.75±0.03
HVU	0.68±0.03	0.68±0.03	0.68±0.03

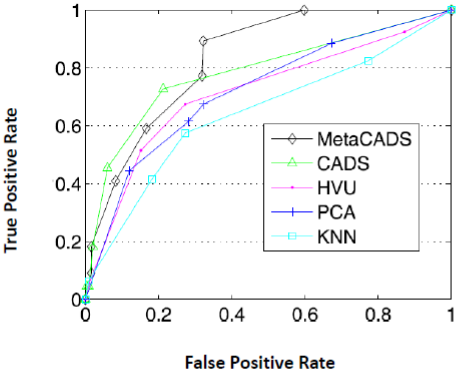
when the number of simulated users is low (i.e., 0.5 percent), MetaCADS yields a slightly higher AUC than CADS (0.92 versus 0.91)

As the number of simulated users increases, CADS clearly dominates MetaCADS. The performance rate of CADS increases from 0.91 to 0.94, while MetaCADS decreases from 0.92 to 0.87.

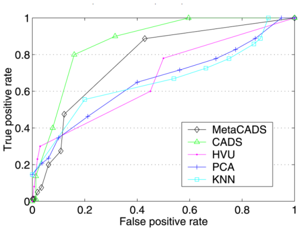
Because when the number of simulated users increases, they have more frequent categories in common. In turn, these categories enable simulated users to form more communities than those based on patients alone, thus lowering their deviation scores.

Experimental Analysis of CADS and MetaCADS: Sensitivity to diversity

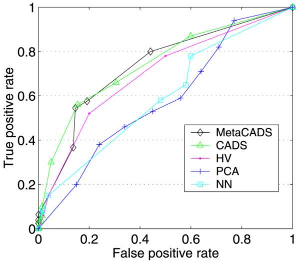
Exp3: MetaCADS dominates when the mix rate is low (mix rate = 0.5%)



Experimental Analysis of CADS and MetaCADS: Sensitivity to diversity

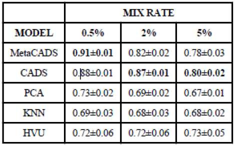


(b) mix rate = 2%



(c) mix rate = 5%

AUC Scores (+/− One Standard Deviation) of the Detection Models on Different Rates



	MIX RATE		
MODEL	**0.5%**	**2%**	**5%**
MetaCADS	**0.91±0.01**	0.82±0.02	0.78±0.03
CADS	0.88±0.01	**0.87±0.01**	**0.80±0.02**
PCA	0.73±0.02	0.69±0.02	0.67±0.01
KNN	0.69±0.03	0.68±0.03	0.68±0.02
HVU	0.72±0.06	0.72±0.06	0.73±0.05

Conclusions

Achievements:

- Detecting anomalous users in CIS: unsupervised relational models $>_p$ supervised models.
  - Mix rate (number of intruders) low: MetaCADS $>_e$ CADS.
  - Mix rate (number of intruders) high: MetaCADS $<_e$ CADS.

Future works:

- Incorporate additional semantics.
- Parameterizing models where size of communities and local networks is variable.
- The framework is an unsupervised system, it may be implemented in real time environments with offline training.

Problems:

- Mimicry attacks.
- Masqueraders $\neq$ Traitors.

Bibliography

- You Chen, Steve Nyemba, Bradley Malin, "Detecting Anomalous Insiders in Collaborative Information Systems", *Ieee transcation on dependable and secure computing, vol. 9, no. 3*, 2012.

- You Chen, Bradley Malin, "Detection of Anomalous Insiders in Collaborative Environments via Relational Analysis of Access Logs", *Conference on Data and Applications Security and Privacy*, 2011.

- You Chen, Steve Nyemba, Wen Zhang, Bradley Malin, "Specializing network analysis to detect anomalous insider actions", *Security Informatics, Springer Open*, 2012.

Grazie per l'attenzione.

Recap and "Questions?"

CADS and MetaCADS

CADS to detect anomalous insiders in a CIS:

- utilizes a relational framework;
- calculates the deviation of users based on their nearest neighbor networks to predict anomalous users.

MetaCADS extends CADS to incorpate the semantics of the subjects accessed by the users.

- Community-based unsupervised models $>_p$ supervised models.
  - Low number of intruders: MetaCADS $>_e$ CADS.
  - High number of intruder: CADS $>_e$ MetaCADS.
- CADS and MetaCADS can be implemented in real time environments.