Risk Assessment in Social Networks Based on Anomalous Behavior Detection

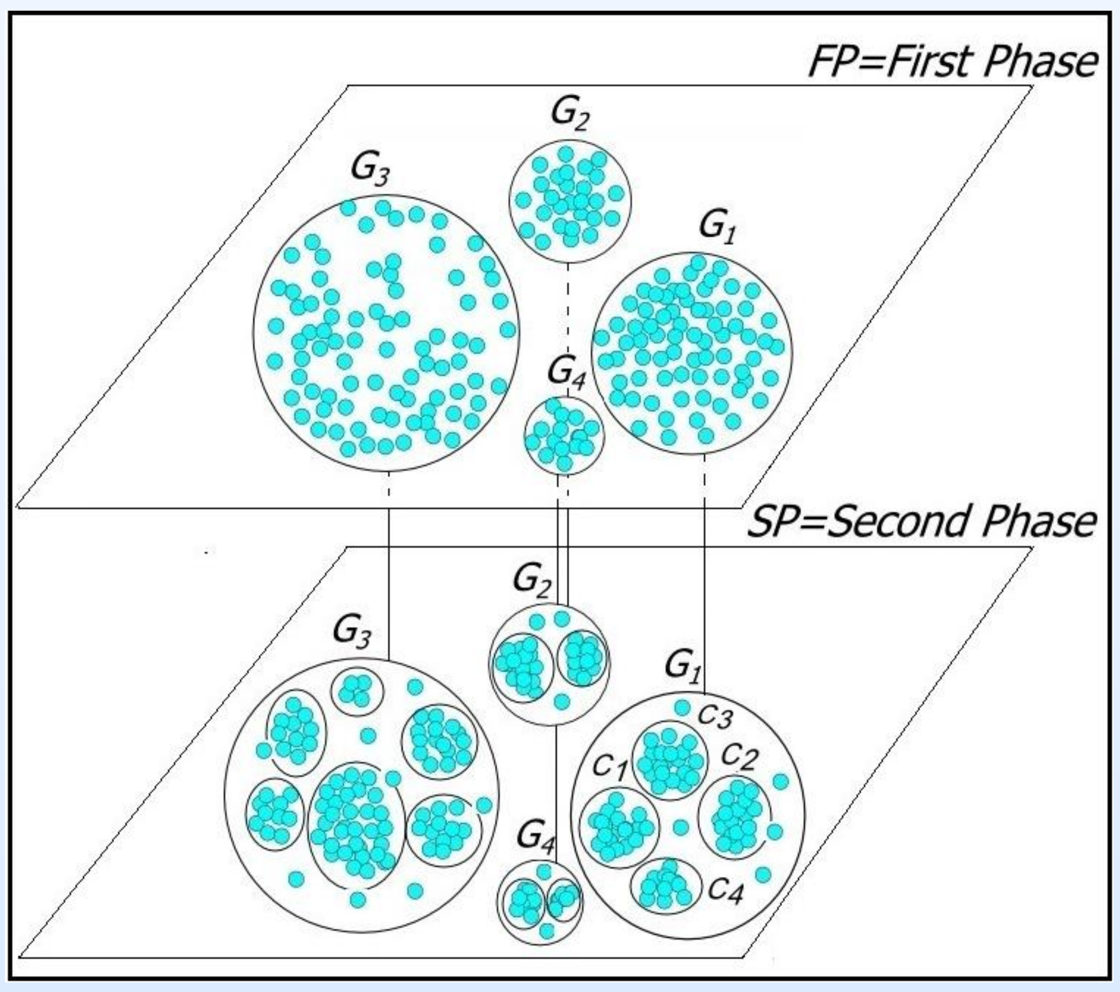
Naeimeh Laleh, Advisors: Prof. Elena Ferrari, Prof. Barbara Carminati
Insubria University, Varese Como, Italy

♦ Abstract

- Social networks are being used by millions of people and there is a dramatic increase in online social networks (OSN) such as Facebook users.
- Some of the information on these sites might contain malicious links and can lead to security risks such as, identity theft and cyber stalking
- Users can not verify the authenticity of the sender
- We need a mechanism to detect risky users with weird behavior , which might be attackers or, victims and users in collusion network that damage caused by real users, not automated programs on OSNs
- At this purpose, we characterize and understand some kind of risky behaviors to have a measure of risk in OSN
- We propose a model for risk assessment based on anomalous behavior detection in online social network.

♦ Two Phase Anomaly Detection

- Un-supervised anomaly detection (one data set without any labels)



♦ Main Contribution

- Anomalous patterns:
  - We show that anomalous users obey some surprising patterns which gives us confidence to declare as risky the ones that deviate.
- Scalability:
  - Clustering algorithm are scalable, unsupervised method for anomalous behavior detection. Low computation cost: O(n×m), where n is the number of cluster features (around 14), and m is the number of users in the data set.
- Effectiveness:
  - Experiment results show a Low False Positives, Low False Negatives and High Detection Rate. It should be robust under various attack strategies.

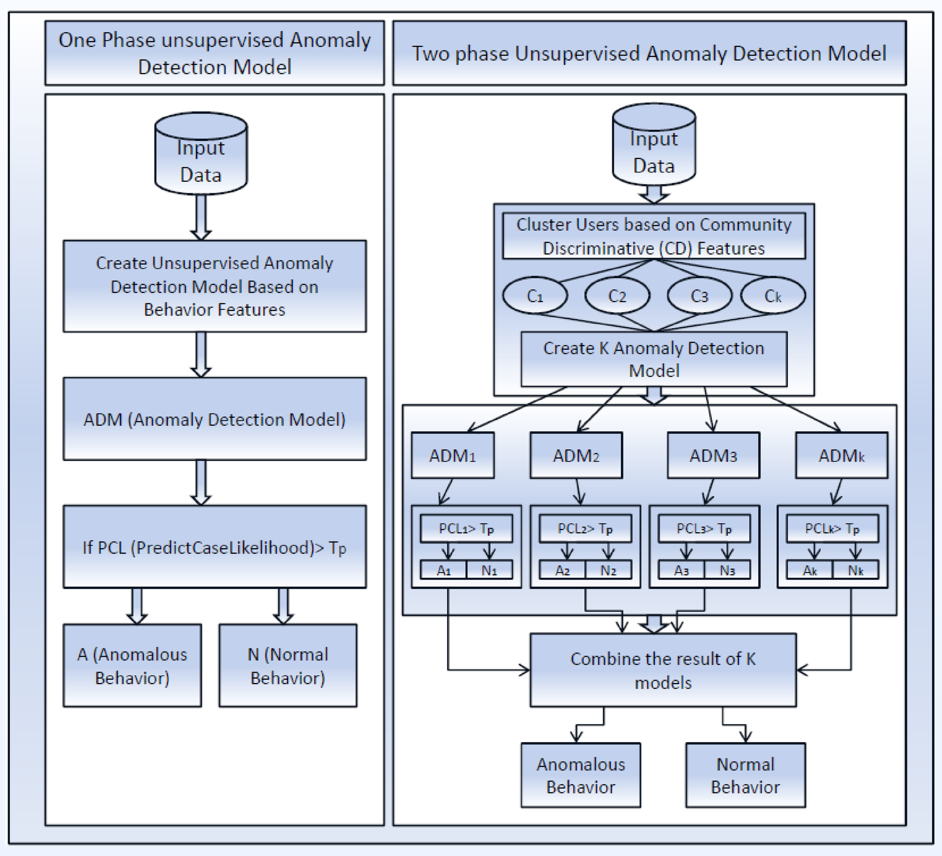
♦ Features:

- Community Discriminative Features:
  - Gender
  - Education Level
  - Number of Friends
  - Activity Level
  - Nationality
- Behaviour Features:
  - Friendship Rate Per Longevity (FRPL)
  - Average Number of mutual friends (ANMF)
  - Balance Number of Friends, Average number of mutual friends (BNFANMF)
  - Comments Rate Per Longevity (CRPL)
  - Number of comments that the user is starter (NCS)
  - Post Rate Per Longevity (PRPL)
  - Average Propagation Speed of Post Items (APSP)
  - Average Propagation Speed of Liked Items (APSL)
  - Balance No of Comment, No of like on comment (BNCNLC)
  - Balance Out, IN (BOI)
  - Balance Post: (Send & Received) (BPSPR)
  - Likes Rate Per Longevity & Propagation Speed of Liked Items (LRPLPSL)
  - Balance Number of Posts, Propagation Speed of Post Items (BNPPSP)

Expectation Maximization Algorithm

- EM algorithm computes a maximum likelihood to estimate parameters such as mean and standard deviation.
  - Expectation Phase: the algorithm computes the membership probability
  - Maximization Phase: the algorithm updates mixture model parameters to maximize the likelihood of the data
- Risky level associated with a user x is given by the that user belong to his\her cluster. The result of this probability is PredictCaseLikelihood that is the result of anomaly detection model.

$$GRS(\vec{x}_i) = \begin{cases} Anomaly & \text{if } PCL\ \vec{x}_i \text{ is} \geq T_p \\ Normal & \text{if } PCL\ \vec{x}_i \text{ is} < T_p \end{cases}$$



Different Types of Anomalous Users

- **Attackers:** Attackers are anomalous users that try to exploit OSN directly to propagate malware and to carry out scams. They include:
  - Socialbots or sybil attacks
  - Identity Clone Attack
  - Cyberbullying attack
- **Victims:** In this kind of anomalies, attackers indirectly propagate some malicious links in the network. Users compromised by attackers in order to propagate malware in the network. They are:
  - Compromised account attacks
  - Socware
  - Creepers
  - Clickjacking
- **Users in collusion networks:** users that use black market applications or collaborative services to unfairly boost each other's likes in collaborative services. Users on these services earn virtual credits for liking Facebook pages posted by other users.
  - The damage of these types of social anomalies is caused by real users, not attackers and automated programs.
- **Popular Users:** Detecting popular users in OSN can be similar to detect anomalous users.

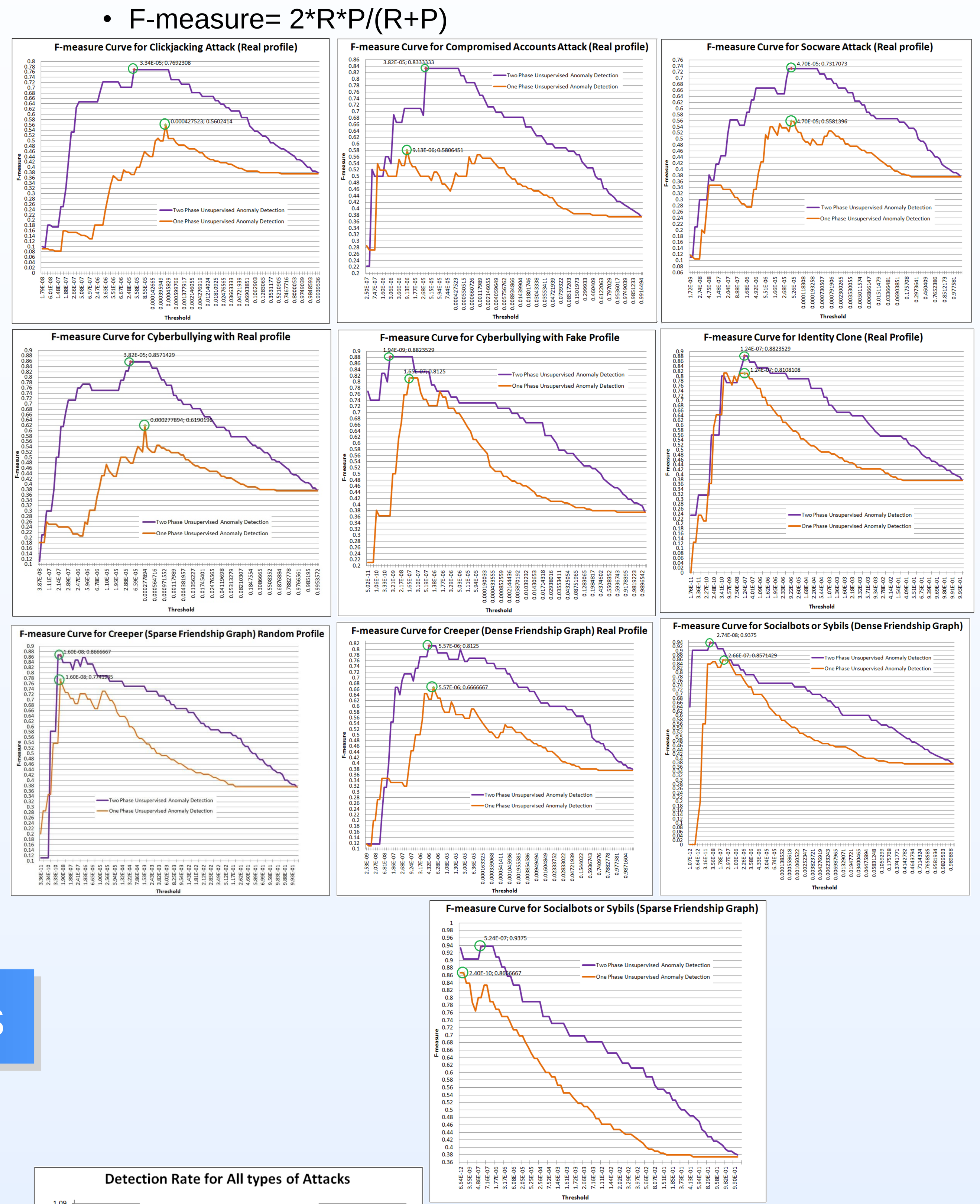
Name of feature	Mathematical Formula
*	For user $(u_i)(f_i = NoFriend_i,\ p_i = NoPost_i,\ l_i = NoLike_i,\ c_i = NoComment_i,\ cs_i = NoCommentStarter_i)$
FRPL	$\mathrm{FRPL}_i = \frac{f_i}{UserLongevity_i}$
ANMF	$ANMF_i = \frac{\sum_{j=1}^{f_i} NoMutualFriendWithFriend_j}{f_i}$
BNFANMF	$\mathrm{BNFANMF_i} = \frac{f_i}{(\sum_{j=1}^{f_i} NoMutualFriendWithFriend_j/f_i)} * \frac{1}{UserLongevity_i}$
CRPL	$\mathrm{CRPL}_i = \frac{c_i}{UserLongevity_i}$
NCS	$NCS_i = cs_i$
PRPL	$\mathrm{PRPL}_i = \frac{p_i}{UserLongevity_i}$
APSP	$\mathrm{APSP_i} = \frac{\sum_{j=1}^{p_i}((NoLikeOnPostedItem_j + NoPostOnPostedItem_j)/ItemLongevity_j)}{p_i}$
APSL	$\mathrm{APSL_i} = \frac{\sum_{j=1}^{l_i}((NoLikeOnLikedItem_j + NoPostOnLikedItem_j)/ItemLongevity_j)}{l_i}$
LRPLPSL	$\mathrm{LRPLPSL_i} = \sum_{j=1}^{l_i}(NoLikeOnLikedItem_j + NoPostOnLikedItem_j) * \frac{l_i}{UserLongevity_i}$
PRPLPSP	$\mathrm{PRPLPSP_i} = \sum_{j=1}^{p_i}(NoLikeOnPostedItem_j + NoPostOnPostedItem_j) * \frac{p_i}{UserLongevity_i}$
BNCNLC	$\mathrm{BNCNLC}_i = \frac{c_i}{(\sum_{j=1}^{c_i} NoLikeOnComment_j/c_i)} * \frac{1}{UserLongevity_i}$
BOI	$\mathrm{BOI_i} = \frac{(p_i + c_i + l_i)}{(\sum_{j=1}^{c_i} NoLikeOnComment_j + \sum_{k=1}^{p_i} NoLikeOnPost_k + \sum_{k=1}^{p_i} NoCommentOnPost_k)} * \frac{1}{UserLongevity_i}$
BPSR	$\mathrm{BPSR_i} = \frac{p_i}{((\sum_{k=1}^{p_i} NoLikeOnPost_k + \sum_{k=1}^{p_i} NoCommentOnPost_k)/p_i)} * \frac{1}{UserLongevity_i}$

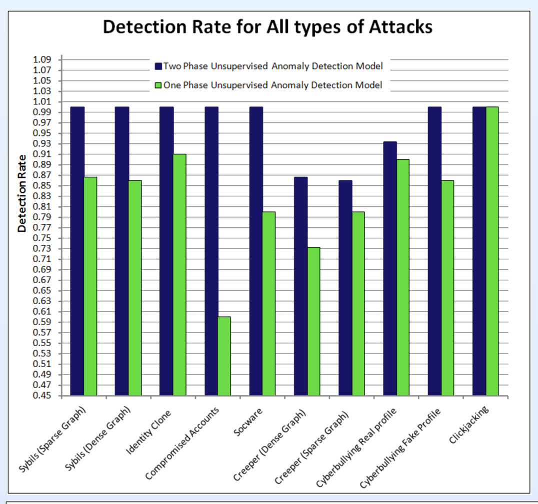
Mapping Features - Anomalous Users

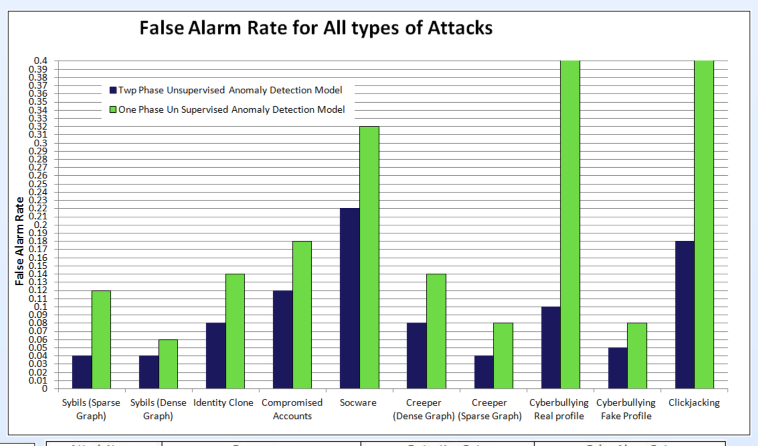
Attack Name	PI	FRPL	ANMF	BNFANMF	CRPL	NCS	PRPL	APSL	APSP	LRPLPSL	PRPLPSP	BNCNLC	BOI	BPSR
Socialbots or Sybils (Dense Friendship Graph)	×				×	×	×	×	×	×	×	×	×	×
Socialbots or Sybils (Sparse Friendship Graph)	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Identity Clone (Real Profile)					×	×	×	×	×	×	×	×	×	×
Compromised Accounts (Real Profile)								×	×	×	×			
Socware (Real Profile)								×	×					
Creeper (Dense Friendship Graph) Real Profile							×		×		×		×	
Creeper (Sparse Friendship Graph) Real Profile		×	×	×			×		×		×		×	
Cyberbullying with Real Profile					×	×	×					×	×	×
Cyberbullying with Fake Profile	×	×	×	×	×	×	×					×	×	×
Clickjacking (Real Profile)								×	×					

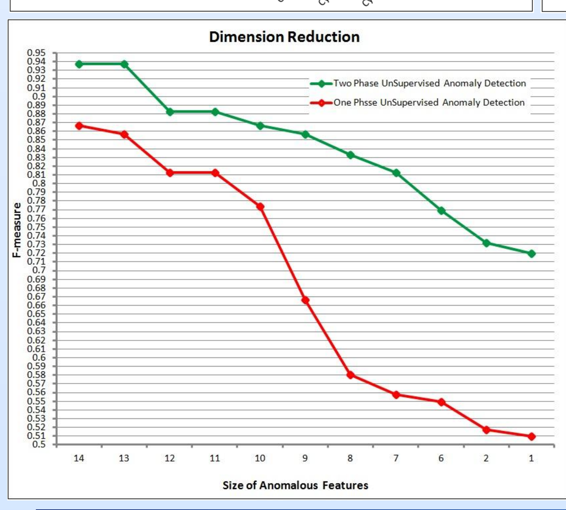
♦ Results

- Recall(R)=TP/(TP + FN), Precision(P) =TP/(TP + FP)
- F-measure= 2*R*P/(R+P)









Attack Name	F-measure		Detection Rate		False Alarm Rate	
	Two Phase Anomaly Detection model	One Phase Anomaly Detection model	Two Phase Anomaly Detection model	One Phase Anomaly Detection model	Two Phase Anomaly Detection model	One Phase Anomaly Detection model
NA 1	0.8018868	0.7368421	0.9444444	0.7	0.04347826	0.02115159
NA 2	0.8067568	0.7191011	0.9022222	0.7111111	0.002350176	0.02820211
NA 3	0.8045977	0.7613636	0.8777778	0.7444444	0.01645123	0.02232667
NA 4	0.807947	0.770115	0.8866668	0.7444444	0	0.0299765
NA 5	0.8165138	0.7374302	0.9888889	0.7333333	0.04582844	0.02702703
Average NA	**0.80754042**	**0.7449704**	**0.92000002**	**0.72666664**	**0.0216216212**	**0.02573678**
SA1	0.8207547	0.6976744	0.956044	0.6593407	0.039953	0.02467685
SA2	0.8095238	0.7692308	0.9444444	0.7142857	0.04211793	0.02527615
SA3	0.8186046	0.7368421	0.9263158	0.6923077	0.03760282	0.0199765
SA4	0.8041237	0.6909091	0.9176471	0.6263736	0.03721489	0.0199765
SA5	0.7678571	0.754491	0.9450549	0.6923077	0.05522914	0.02527615
Average SA	**0.80417278**	**0.72982948**	**0.93790124**	**0.67692308**	**0.042423556**	**0.02303643**
MSA1	0.8113208	0.7283237	0.9450549	0.6923077	0.04112808	0.02232667
MSA2	0.7943925	0.7664671	0.9340659	0.7032967	0.04465335	0.02410106
MSA3	0.7926267	0.7305389	0.9450549	0.6703297	0.04700353	0.02762632
MSA4	0.8133971	0.7950311	0.9340659	0.7032967	0.03877791	0.017050529
MSA5	0.7951196	0.6878307	0.8901099	0.7142857	0.04347826	0.03877791
Average MSA	**0.80137134**	**0.7416383**	**0.9296703**	**0.6967033**	**0.043008226**	**0.0259764978**

♦ References

- Viswanath, Bimal, et al. "Towards Detecting Anomalous User Behavior in Online Social Networks." *Proceedings of the 23rd USENIX Security Symposium (USENIX Security)}*.2014.
- Yang, Zhi, et al. "Uncovering social network sybils in the wild." *ACM Transactions on Knowledge Discovery from Data (TKDD)* 8.1 (2014): 2.
- Fire, Michael, Roy Goldschmidt, and Yuval Elovici. "Online Social Networks: Threats and Solutions." (2013): 1-1.
- Boshmaf, Yazan, Konstantin Beznosov, and Matei Ripeanu. "Graph-based Sybil detection in social and information systems." *Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on.* IEEE, 2013.
- Stein, Tao, Erdong Chen, and Karan Mangla. "Facebook immune system."*Proceedings of the 4th Workshop on Social Network Systems.* ACM, 2011.
- Adali, Sibel, et al. "Measuring behavioral trust in social networks." *Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on.* IEEE, 2010.
- Akcora, Cuneyt Gurcan, Barbara Carminati, and Elena Ferrari. "Privacy in social networks: How risky is your social graph?." *Data Engineering (ICDE), 2012 IEEE 28th International Conference on.* IEEE, 2012.
- Bouguessa, Mohamed. "Unsupervised Anomaly Detection in Transactional Data." *Machine Learning and Applications (ICMLA), 2012 11th International Conference on.* Vol. 1. IEEE, 2012.
- Adali, Sibel, and Jennifer Golbeck. "Predicting Personality with Social Behavior." *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012).* IEEE Computer Society, 2012.

♦ Future work

- Our approach is based on a distributed, cluster-based anomaly detection algorithm.
- Data in many anomaly detection applications may come from many different sources
- A key problem is how to minimise the communication overhead and energy consumption in the network when identifying anomalous behaviors.