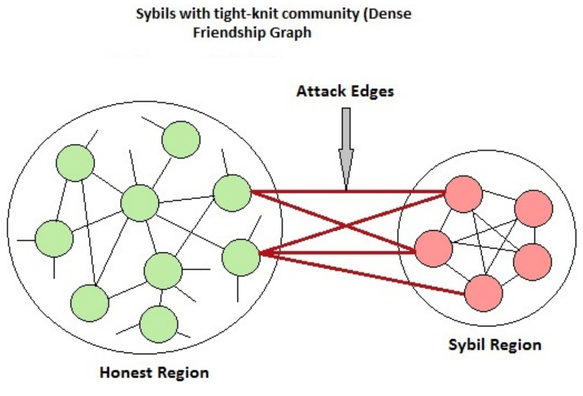
Distributed Activity based Sybil Identification over Decentralized Social Networks

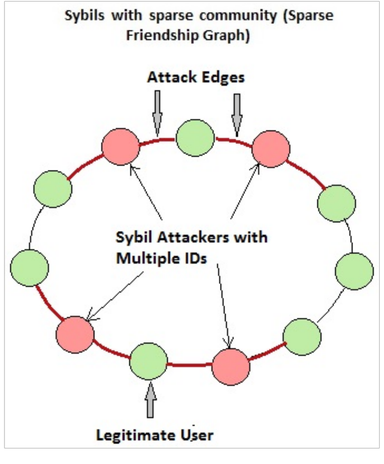
Naeimeh Laleh, Kambiz Ghoorchian

naimeh.laleh@gmail.com, ghoorian@kth.se

Sybil Attack Identification

- Sybil Attack
  - One of the most prevalent and practical attacks against online social networks (OSNs).
  - Malicious node creates multiple fake identities using social-bots.
  - Performs an attack using those identities.
- Types of Sybil attack:
  - Sybils with **tight-knit** community (Dense Friendship Graph):
    - Sybils are connected to each other [1].
  - Sybils with **sparse** community (Sparse Friendship Graph):
    - Sybils do not shape a community themselves[2].

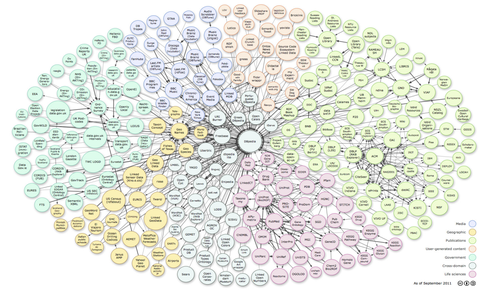




- Problems:
  - Attacks are difficult to capture in **large scale**.
  - It requires general knowledge for calculating action probabilities in a centralized solution.
- Objectives:
  - Detect anomalies in extracted behavioral communities using distributed anomaly detection[3].
  - Minimize the communication overhead and energy consumption.

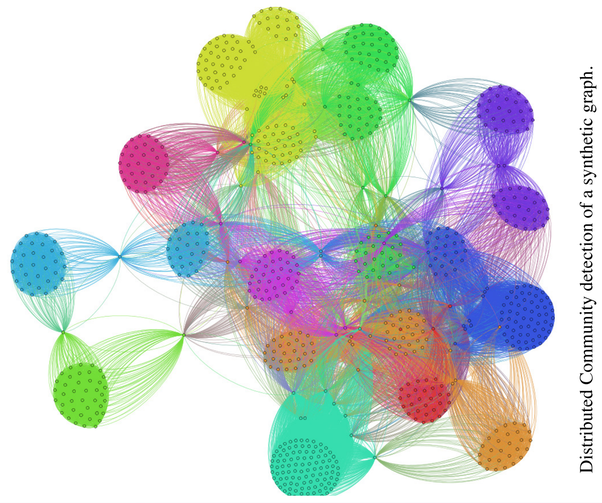
Distributed Community Detection

- Community
  - Set of nodes tightly connected with respect to some properties.
  - Ambiguous, can have different meaning depending on the required resolution.
    - Ex. Continent vs Country communities in FB.



Sample Community Detection over Linked Data Graph.
(http://upload.wikimedia.org/wikipedia/commons/3/34/LOD_Cloud_Diagram_as_of_September_2011.png)

- Community detection:
  - The task of identifying communities in a graph with respect to some resolution.
  - A type of clustering, NP-Hard [4].
  - Ex. Minimum cut, Hierarchical, Modularity based, Statistical.
  - Diffusion-based [5]
    - Specific graphs extracted from **cliques**.
    - Extracts communities by diffusing colors in to the graph.
    - Developed for *"Cross-Document Coreference Resolution"*.

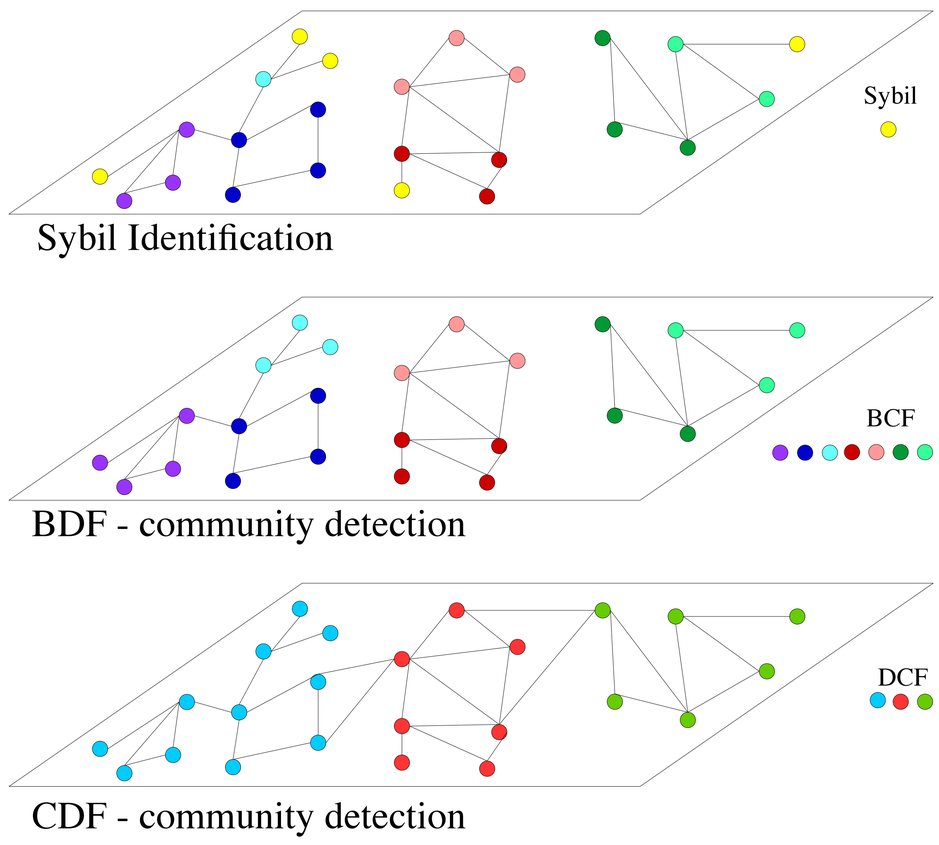


Distributed Community detection of a synthetic graph.

Distributed Sybil Identification

- Similar People tend to exhibit similar **behavior** and **friendship** patterns.
- Extend our distributed community detection algorithm to account for **social graphs**.
- Develop friendship and behavioral community structures using:
  - *Community discriminative Features (CDF)*:
    - Gender,
    - Educational Level,
    - Number of Friends,
    - Activity Level and
    - Nationality.
  - *Behavioral discriminative Features (BDF)*:
    - Number of Average Mutual Friends (AMF),
    - Friendship per Longevity (FpL),
    - Comments per Longevity (CpL),
    - Post per Longevity (PpL),
    - Likes per Longevity (LpL),
    - Number of Initiative Comments (IC),
    - Number of Likes and Comments on a Comment (LCoC) and
    - Balanced number of Sent and Received Comments (BSRC).
- Extract patterns using community detection algorithm.
- Identify anomalies comparing different community membership patterns.

Visualization



Distributed Sybil Identification using community detection

References

[1] Yang, Zhi, et al.,: Uncovering social network sybils in the wild. Presented at the ACM Transactions on Knowledge Discovery from Data (TKDD),8.1,2014.

[2] Boshmaf Yazan, Konstantin Beznosov, and Matei Ripeanu,: Graph-based Sybil detection in social and information systems. Presented at Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on. IEEE, 2013.

[3] Ning, Peng, Sushil Jajodia, and Xiaoyang Sean Wang,: Design and implementation of a decentralized prototype system for detecting distributed attacks. Presented at Computer Communications 25.15 (2002): 1374-1391.

[4] Santo Fortunato,: Community detection in graphs. CoRR 2009, V.abs/0906.0612.

[5] Fatemeh Rahimian, Sarunas Girdzijauskas, and Seif Haridi,: Parallel Community Detection For Cross-Document Coreference. Presented at the 2014 IEEE/WIC/ACM International Conference on Web Intelligence (WI'14), Warsaw, Poland, August 2014.