Sybil Defenses in Mobile Social Networks

Wei Chang, Jie Wu, Chiu C. Tan, and Feng Li†

Temple University, USA
Indiana University-Purdue University Indianapolis †

IEEE GLOBECOM 2013, December
Atlanta, USA

Overview

- Most distributed systems are vulnerable to Sybil attacks.
- In this paper, we consider the Sybil attacks in a mobile social network (MSN).
- Traditional social-based Sybil defenses have Two limitations:
  - Assume that the social graph of honest users is fast-mixing
  - The accuracy is related to the number of attack edges
- We propose a local ranking system for estimating trust-level between users.
  - Multi-honest communities model
  - Use both trust and distrust relations
  - Remove high suspicious edges
- We validate the effectiveness of our scheme through comprehensive simulations.

Outline

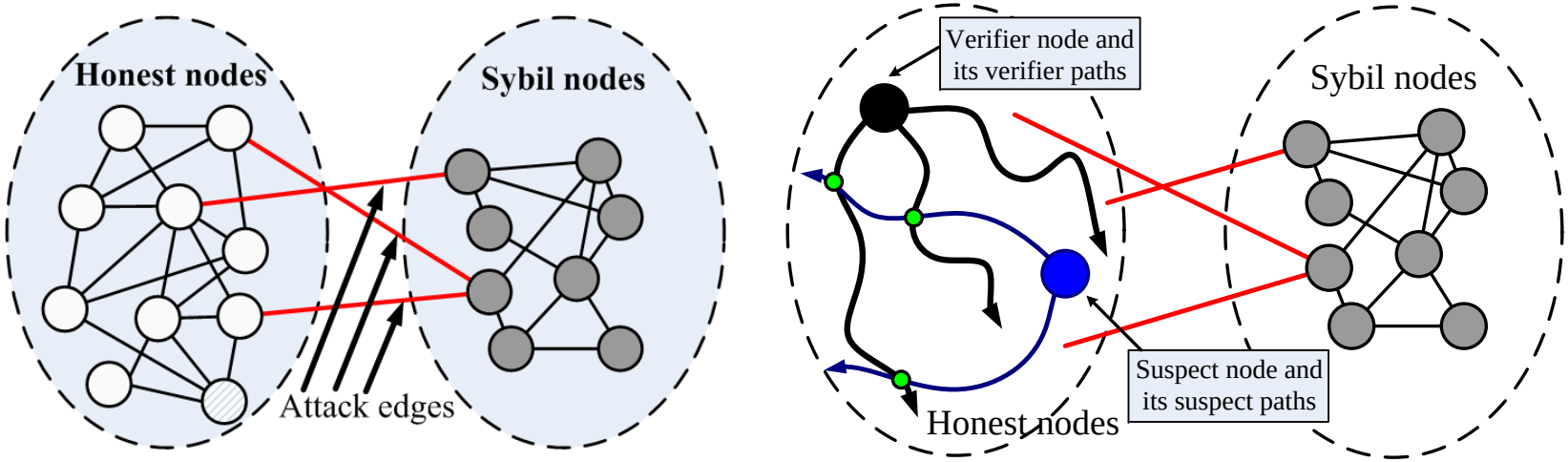
1. Introduction
2. Related Work
3. Scheme Description
4. Evaluation
5. Conclusion

Introduction

- Mobile social networks (MSN) =
  online social networks + location based services.
- A MSN can provide many new services, such as data sharing service or voting.
- The distributed and self-organized features make MSNs vulnerable to Sybil attack.
- In a Sybil attack, an adversary creates a large number of fake identities (Sybils), and since all Sybils are controlled by the adversary, she can subvert the system by making actions that benefit herself.

Cont.

- Social network-based Sybil defense



- Problems:
  - The fast-mixing feature of the honest region may not always hold.
  - The accuracy is highly related with the number of attack edges.

Main idea

- Problems vs. solution
  - The fast-mixing feature of the honest region may not always hold.
  - Honest users may cluster into one community, or several communities with similar sizes.
  - The accuracy is highly related with the number of attack edges.
  - If we cut off several high centrality edges from the social graph, the connectivity between honest nodes bears much less of an impact than that between Sybil and honest nodes.

Outline

1. Introduction
2. Related Work
3. Scheme Description
4. Evaluation
5. Conclusion

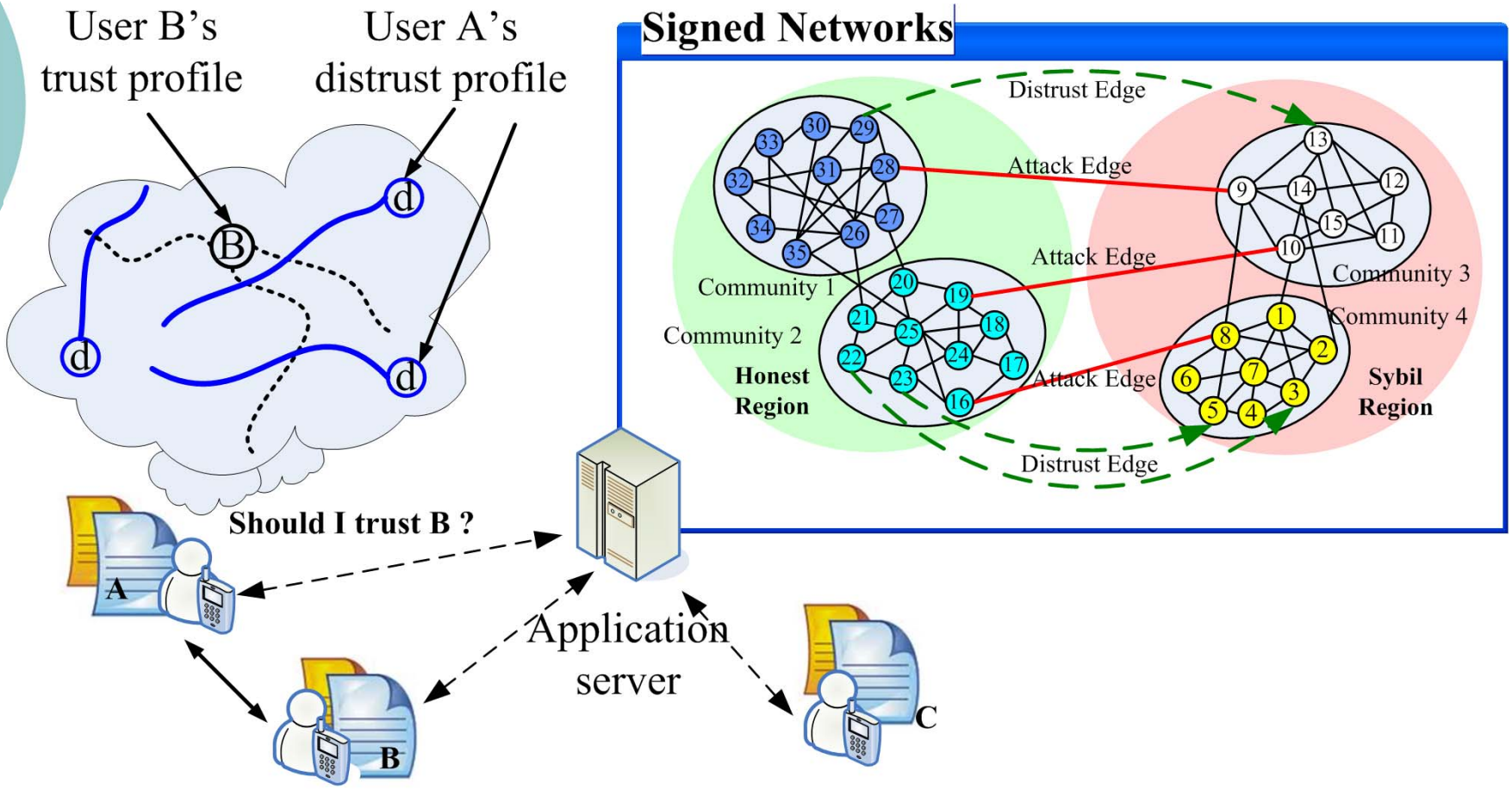
Related Work

- Neighborhood monitoring-based Sybil defense
- Social network-based Sybil defense
- Sybil attack in online social networks

Outline

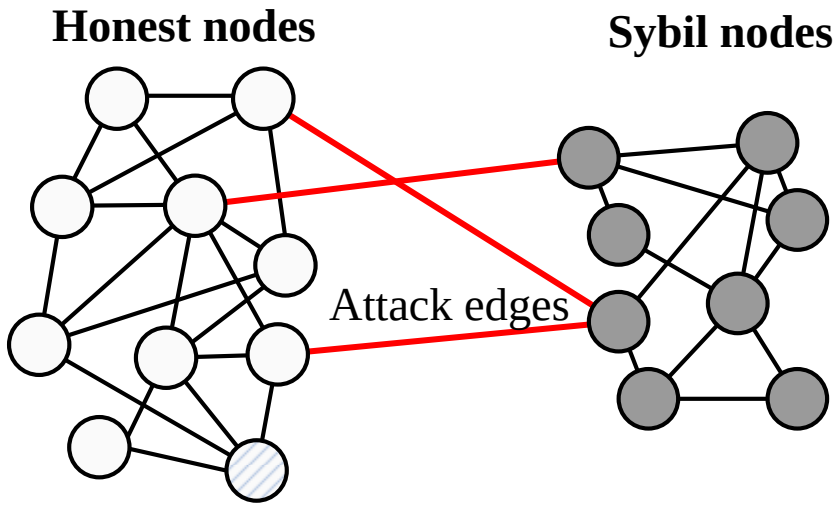
1. Introduction
2. Related Work
3. Scheme Description
4. Evaluation
5. Conclusion

Scheme description: System Model



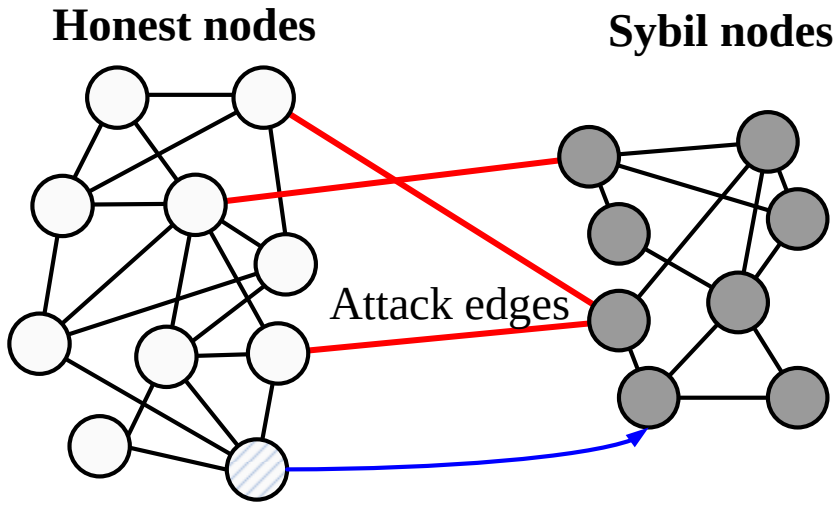
Signed network-based Sybil defense

- Distrust edges' generation
  - Volunteers report abnormal conditions
  - Identity switching
  - Same person, different identities



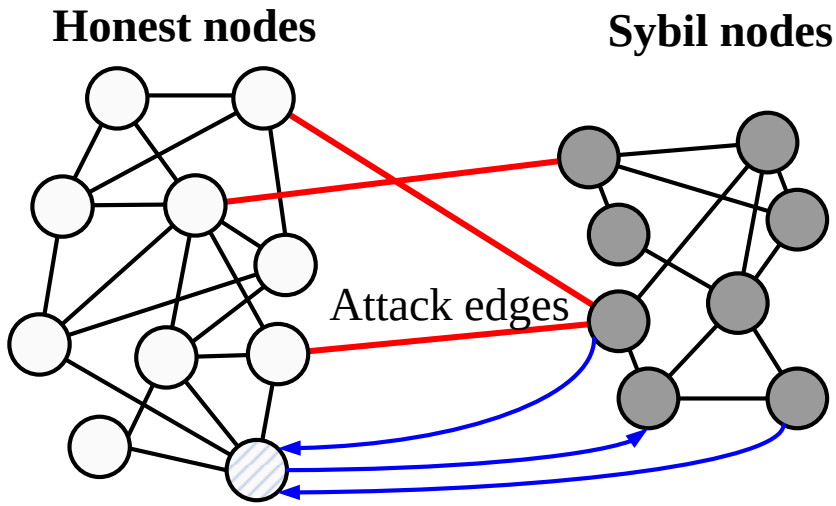
Signed network-based Sybil defense

- Distrust edges' generation
  - Volunteers report abnormal conditions
  - Identity switching
  - Same person, different identities



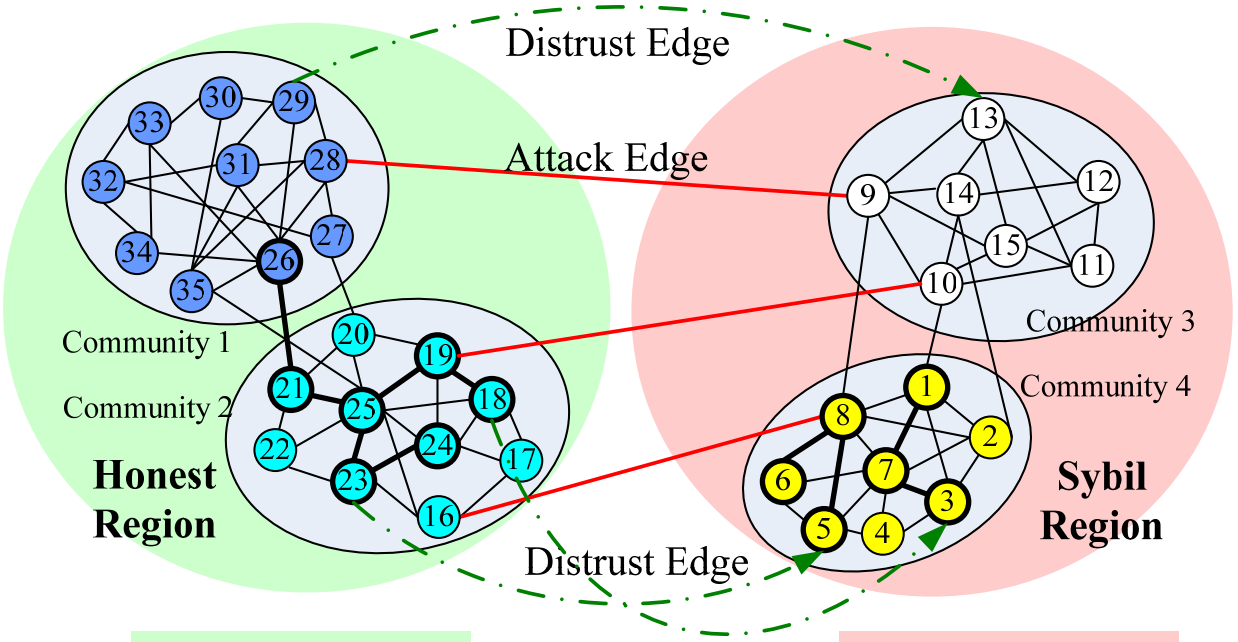
Signed network-based Sybil defense

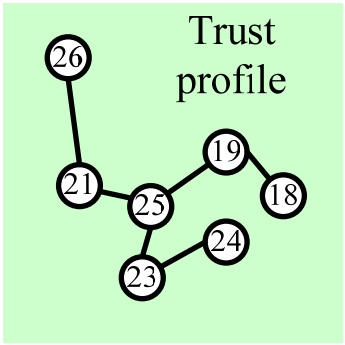
- Distrust edges' generation
  - Volunteers report abnormal conditions
  - Identity switching
  - Same person, different identities

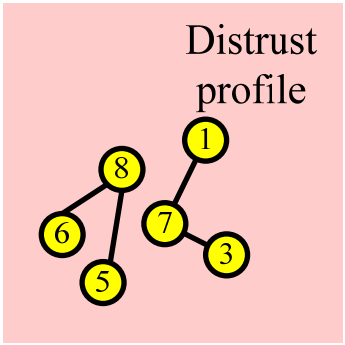


Cont.

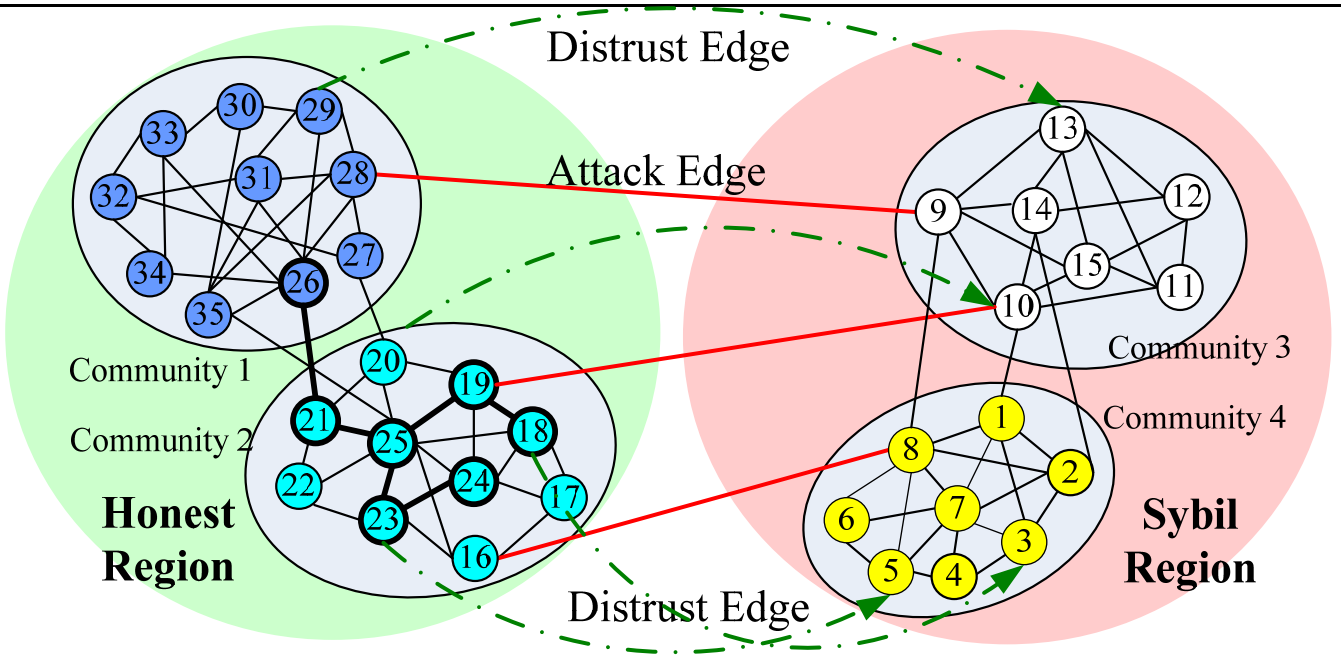
- Trust and distrust social profiles

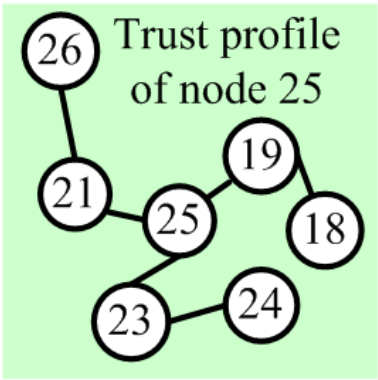


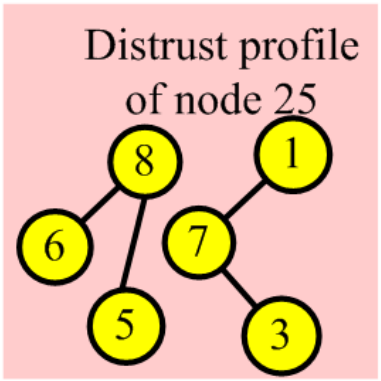


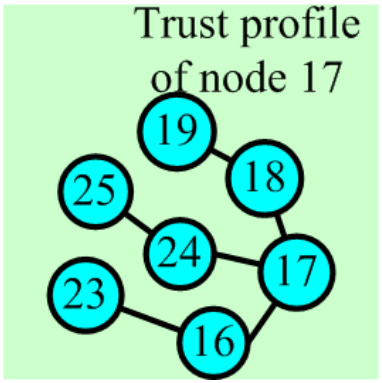


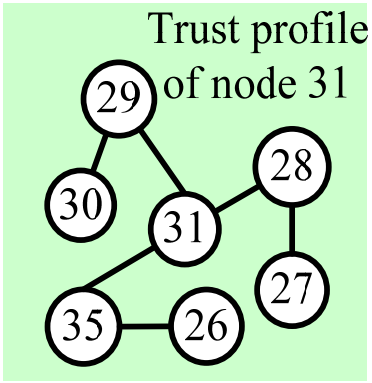
Trust level estimation

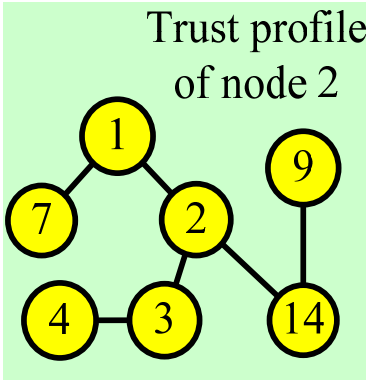












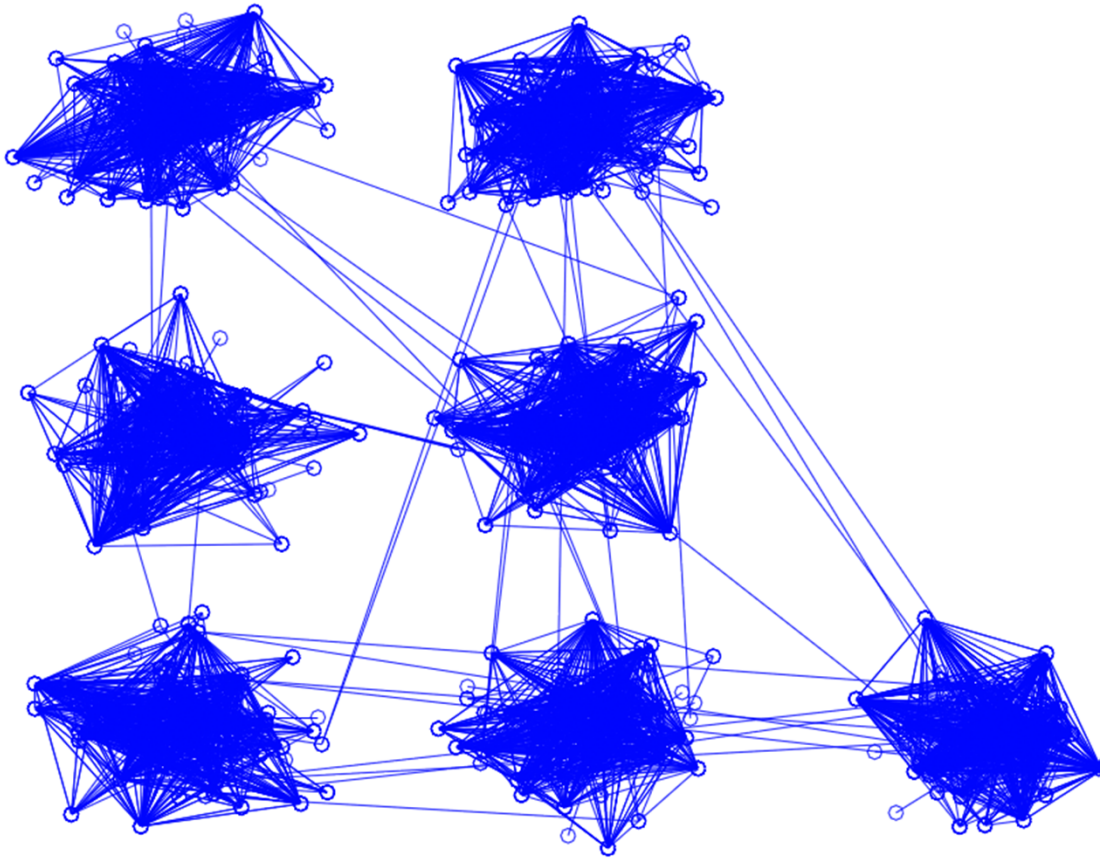
Security Analysis

- Attacker's dilemma situation
  - In order to boost the trust scores, it is better for Sybils to cluster into one community, such that the verifier paths are more likely to encounter a suspect path.
  - For reducing the distrust scores, the attacker should build Sybils into multiple communities
- Bad mouthing strategy
  - Distrust profiles are based on the distrusted relations from the high trusted nodes.
  - It will cause high centrality, which will be removed by our pruning algorithm.

Pruning algorithm: gateway-breaking

- Server periodically prunes the graph
- Server randomly selects several pairs of antagonistic nodes with high centrality
- Gateway verification
  - If one node's connectivity to the third node is much larger than that of the other node, it is very possible that the two nodes reside at different communities.
  - We use the number of unique paths to measure the connectivity feature.
- Remove high-intensity antagonistic gateways

Evaluation



Cont.

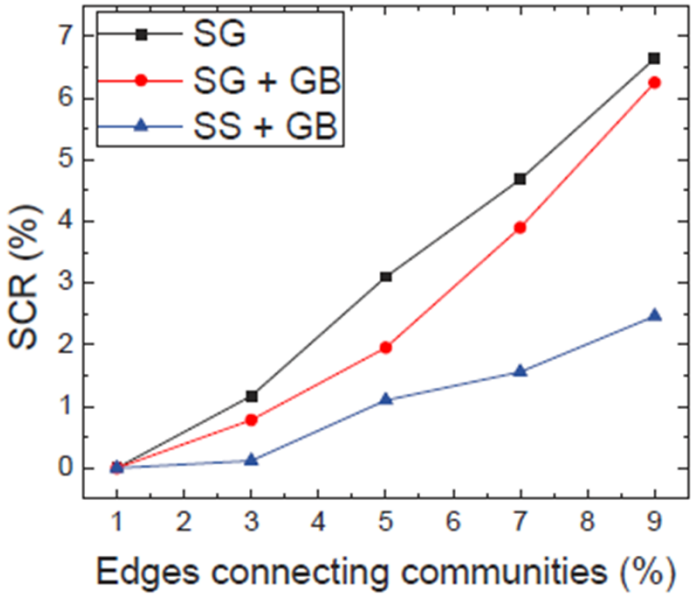


Fig. 7. The impacts of the number of attack edges.

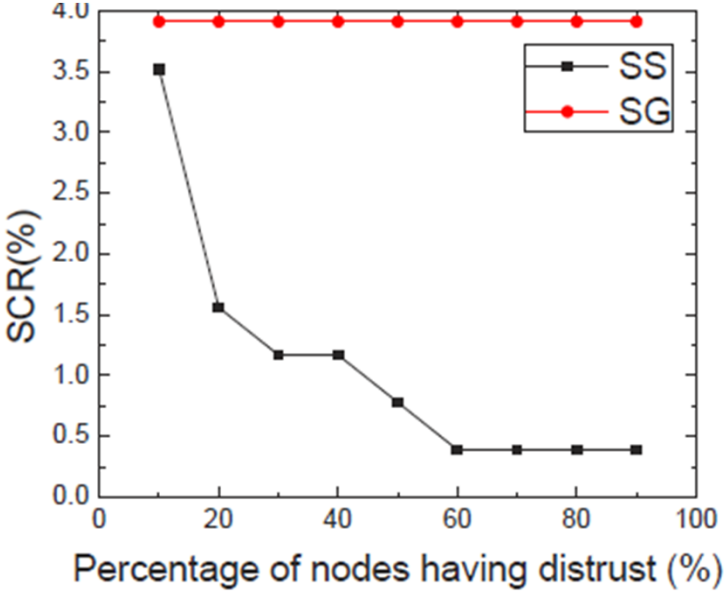
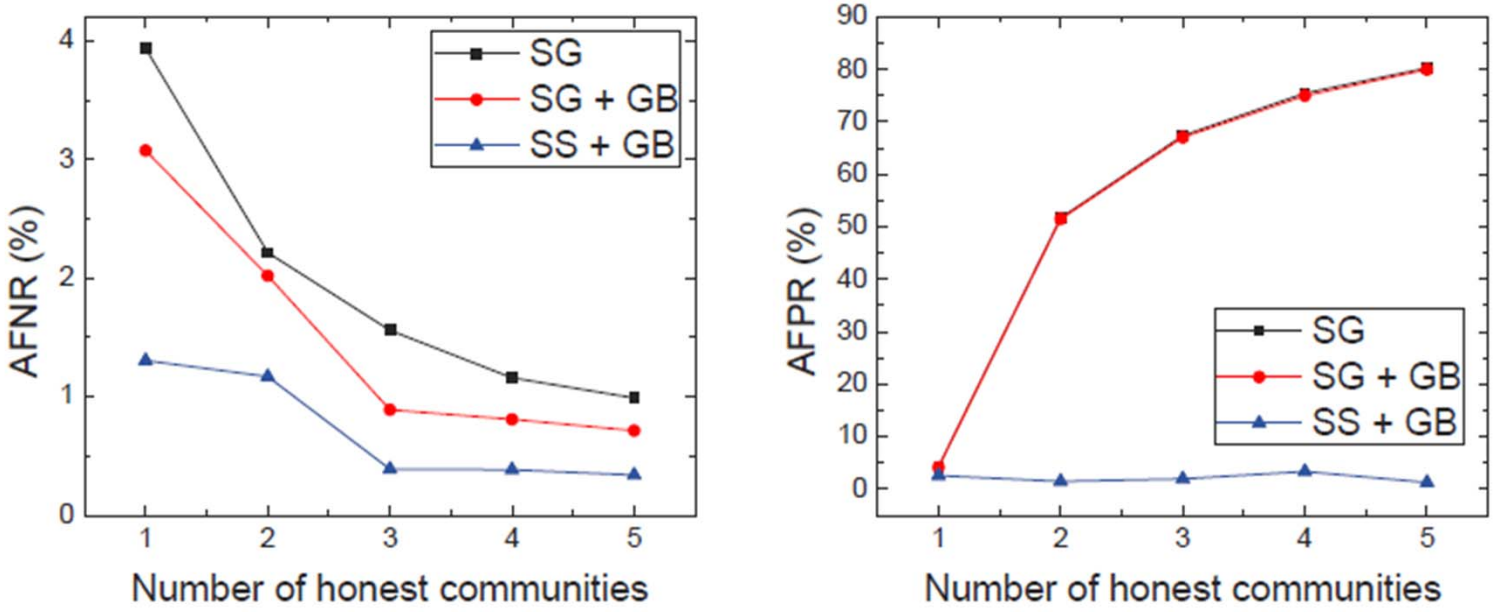


Fig. 8. The impacts of the number of distrust relations.

Cont.



(a) avg. false negative rate.

(b) avg. false positive rate.

Fig. 10. The impacts of the number of honest communities.

Conclusion

1. We propose a new system to defense Sybil attacks in mobile social networks.
2. Our proposed solution explores both trust and distrust relations among the nodes. It suits for different community structures of social graphs.
3. Our scheme potentially can enhance the accuracy of any graph-based Sybil defense by removing some suspicious edges.

Thank you!