Colluding Network Attack Strategies with Incomplete Information

Henry Xu*, Frank Liao**, Jonathan Beltran†,
Georges Arsene Kamhoua†, Kianoosh Boroojeni†
*University of California, Berkeley; **Carnegie Mellon University; †Florida International University

School of Computing and Information Sciences

School of Letters and Sciences

Information Systems Program

Introduction

Social networks have afforded a new age of interconnectedness, tying society together in an expansive web previously thought impossible. However, with this seemingly limitless amount of connections comes an attack called the collusion attack, which involves a number of malicious agents working together to compromise a target. The new connectivity provided by social networks has catapulted this attack into the limelight, as malicious actors can now move their attacks online.

In this project, we developed a framework for testing various attack strategies on different network models.

Probability Model

The probability model attempts to portray the chances that a node in the network will accept a connection from another. The probability of this event is important to an attacker's path planning and to the simulation itself.

Naïve Model

$$P(N_i \rightarrow N_j) = \frac{P_{ij}^2}{F_i + F_j - P_{ij}^2 - 2}$$

N_i *is a node* i

P_{ij}^n *is the number of paths of length* n *between* N_i *and* N_j

F_i *is the total connections of* N_i

The naïve model presents the attacker with the ability to approximate the chance of a successful connection. However, the model is limited to graph topology features, which means it doesn't consider human features of each profile.

Random Model

Due to the unpredictability of the chance of successfully connecting with a victim, the second option is to arbitrarily determine the probabilities at run time. In this way, the probability is declared to be inapproximable with solely graph features.

Attack Model

Our proposed attack is a modified breadth first search originating from n starting locations, where n is the number of attackers. The fringe we use is a custom minimum priority queue capable of discerning the best next node to attack and the best attacker to attack said node.

Assumptions

1. The attackers and target share one graph.
2. All nodes two(2) hops away are visible and can be added as friends.
3. The attackers and target are not already friends.

Algorithm

1. After selecting n colluding attackers, we enqueue all nodes two(2) hops away from the attackers, assigning a probability value* to each. The probability value, further described in the probability model section, provide a gauge of how likely a node is to accept the attacker in question as a friend.
2. We then dequeue the node and associated attacker with the highest probability value, and send a friend request from the attacker to the node.
   a. If the request is successful, we enqueue all of the friends of the node, assigning probability values if not previously encountered or updating the existing values if the node is already in the fringe.
   b. If the request is unsuccessful, we proceed to dequeue the next best colluding attacker and node pair.
3. We continue to dequeue the next best attacker and node pair and repeat the process outlined in (2) until we dequeue the target or have no nodes left to dequeue, upon which our attack is complete.

* When complete knowledge of the graph is available, we assign a weight to each node instead of a probability value. The weight is a combination of the probability value and the distance from the desired target. This weight allows us to find the desired target with greater efficiency and minimizes the number of unnecessary friend requests. In our simulations, we give higher priority to the distance.

Results

Framework

The framework is fully functional, and flexible enough to be adapted to a variety of social network attacks.

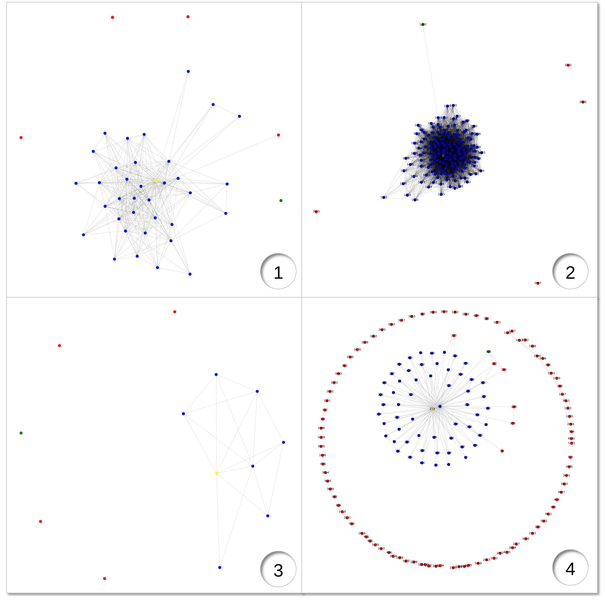
Proposed Attack

1. **Five(5) colluders, naïve probability function, complete knowledge of the network**: Success rates varied from attack failure to approximately five(5) percent. In all cases, just one attacker was needed to find the target, and the leftover attackers explored extraneous parts of the graph.

2. **Five(5) colluders, naïve probability function, no knowledge:** Failure was the most common result (~0%), with success attributed mostly to chance. In cases where the target was found, only one attacker was truly needed.

3. **Five(5) colluders, pseudorandom probability function, no knowledge :** The attack failed in all trials.

4. **Five Hundred(500) colluders, naïve probability function, complete knowledge:** Attack success rates hovered around 50 percent. Only one attacker was necessary to find the target.



Conclusions

Results are largely problematic. There are three main issues with the algorithm:

1. **Usefulness of collusion** - In all trials, only one attacker was truly needed to execute the attack.
2. **Arbitrary nature of probability model** - The probability model we used provided little advantage over assigning pseudorandom probabilities
3. **Low success rates** - The success rates of the attack hovered around five(5) percent at best with a realistic number of nodes. When ninety-nine(99) percent of the network was designated as attackers, we still had only a fifty(50) percent success rate.

Future work includes more a more intensive study of the probability model given human features, and detection of such attacks from cliques of attackers.

References

Angelopoulos, Spyros, and Konstantinos Panagiotou. "Optimal strategies for weighted ray search." arXiv preprint arXiv:1704.03777 (2017).

Nguyen, Tri P., Hung T. Nguyen, and Thang N. Dinh. "Towards Optimal Strategy for Adaptive Probing in Incomplete Networks." arXiv preprint arXiv:1702.01452 (2017).

Nguyen, Hung T., and Thang N. Dinh. "Targeted cyber-attacks: Unveiling target reconnaissance strategy via Social Networks." Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on. IEEE, 2016.

Li, Xiang, et al. "Privacy Issues in Light of Reconnaissance Attacks with Incomplete Information." Web Intelligence (WI), 2016 IEEE/WIC/ACM International Conference on. IEEE, 2016.

Acknowledgments

Supported by NSF Grant CNS-1560134 to the REU ASSET - Advanced Secured Sensor Enabling Technologies