Identifying Attackers using Multiplex Social Network Analysis for Cyber Security

Ruchi Mittal, M.P.S Bhatia

Department of Computer Engineering, Netaji Subhas Institute of Technology
Delhi University, New Delhi
ruchi.mittal138@gmail.com, bhatia.mps@gmail.com

Abstract

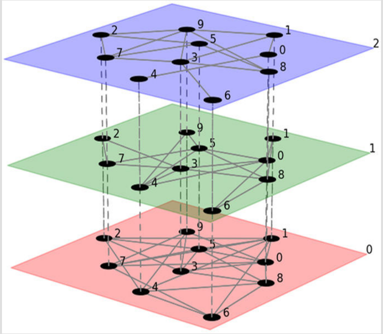
Recent research in cyber-security models the nature of attacks as graphs consisting of nodes that represent attacks and their properties, forming attack profiles. We present a novel approach to describe users' behavior using multiplex or multi-layer networks, which allows us to get more reliable outcomes. We model the relationships between attack profiles based on established features of the attacks thereby reducing the amount of information present in the multiplex graph. Cyber-security providers aim to protect users and establishments from cyber attacks. We find that a multi-layered network analysis is a reliable technique to profile hackers and hence thwart cyber attacks. In this paper, we discuss a few methods, which can help out dig out anomalous users in the network

The Problem

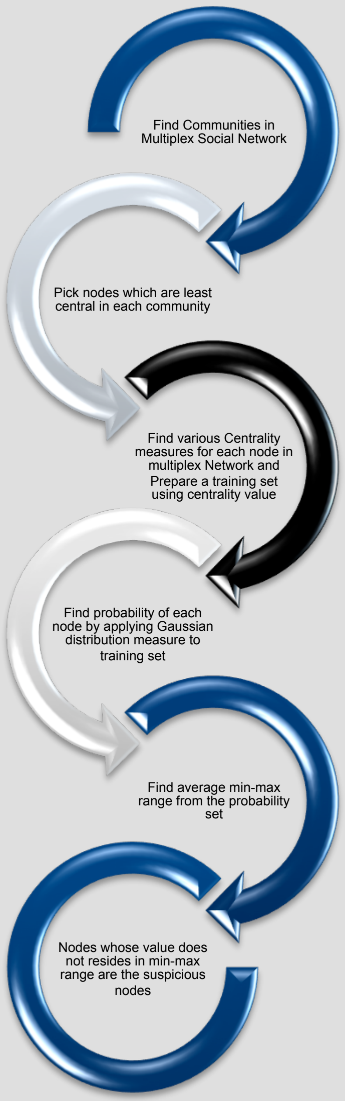
▪Identify attackers to fulfill the requirements of cyber-security using the concept of multiplex network

▪We suggest a greedy method of finding attackers' on the social network

▪This approach can successfully reduce overheads than other similar methods regarding time on large dataset, and drive to better results



Approach


Find Communities in Multiplex Social Network

Pick nodes which are least central in each community

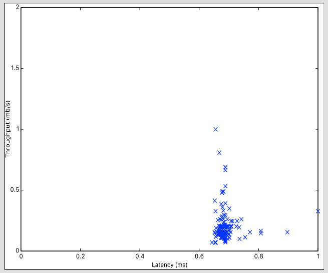
Find various Centrality measures for each node in multiplex Network and Prepare a training set using centrality value

Find probability of each node by applying Gaussian distribution measure to training set

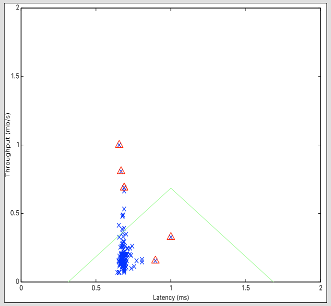
Find average min-max range from the probability set

Nodes whose value does not resides in min-max range are the suspicious nodes

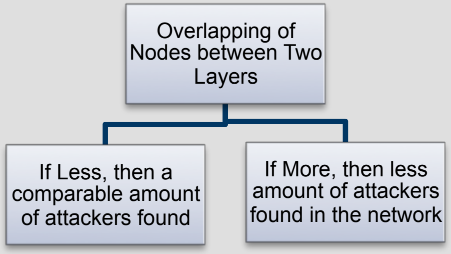
Performance Evaluation



Original graph



Nodes highlighted with triangles are attackers


Overlapping of Nodes between Two Layers

If Less, then a comparable amount of attackers found

If More, then less amount of attackers found in the network

Conclusion

▪To successfully thwart attacks, a multi-layered network analysis is best to find out such attackers.

▪Proposed methodology can be extended by incorporating the semantic content available with the communication or any other form of network like weighed or directed.

▪This works directed us to get more knowledge from the multiplex network and cyber-security. There are many ways to extend this work. It is interesting to continue the proposed algorithm to directed multiplex networks or weighted multiplex networks.

▪we are planning to reach our aim to find most central nodes of the multiplex network and may require preventions from attackers.

References

1. M. De Domenico, A. So ▯le-Ribalta, E. Cozzo, M. Kivela ▯, Y. Moreno, M. A. Porter, S. Go ▯mez and A. Arenas, 'Mathematical formulation of multilayer networks', Phys. Rev. X 3 (2013) 041022.
2. P. Wadhwa and M.P.S Bhatia, "Classification of Radical Messages on Twitter Using Security Associations," in Case Studies in Secure Computing, Auerbach Publications, 2014, pp. 273–294.
3. P. Wadhwa, M. P. S. Bhatia, „"An Approach for Dynamic Identification of Online Radicalization in Social Networks". Cybernetics and Systems 46(8): 641-665 (2015)
4. P. Wadhwa, M. P. S. Bhatia, „" New Metrics for Dynamic Analysis of Online Radicalization". Journal of Applied security research 11(2): 116-184 (2016)