Preserving Privacy in Social Network Integration with τ-Tolerance

Christopher C. Yang
College of Information Science and Technology
Drexel University, PA, USA

Abstract— **Social network analysis and mining is very useful for law enforcement and intelligence to extract criminals or terrorists interaction patterns and identify their roles in the organizations [1][2][3]. Due to the privacy concerns, social network data is usually captured within a law enforcement or intelligence unit without sharing with other units. As a result, the utility of social network analysis is diminished when the social network data within an individual unit is incomplete. In this project, the objectives are sharing the insensitive and generalized information to support social network analysis and mining but preserving the privacy at the same time. We ensure that a prescribed level of privacy leakage tolerance is satisfied. The measurement of the privacy leakage is independent to the privacy preserving techniques of integrating social network data.**

Keywords- privacy preservation; social network analysis; privacy leakage tolerance; intelligence and security informatics;

I. INTRODUCTION

Social network data is valuable data for analyzing the patterns of actor interactions[5][6][8]; however, this data is typically distributed and each organization or agent only knows a small piece of the complete network [4][7][9]. Using a small piece of data, the social network analysis and mining (SNAM) techniques are not able to extract the essential knowledge. In some cases, an inaccurate result will be obtained. For example, each law enforcement unit has its own criminal social network. Mining on an incomplete criminal social network may not be able to identify the bridge between two criminal subgroups. Unfortunately, limited by the privacy policy, different organizations are only allowed to share a small piece of information but not their social networks. As a result, an accurate SNAM cannot be conducted unless an integration of the social networks owned by different organizations can be made.

Given two or more social networks (G_1, G_2, …) from different organizations (O_1, O_2, …), the objective is achieving more accurate social network analysis and mining results by integrating the shared crucial and insensitive information between these social networks and at the same time preserving the sensitive information with a prescribed level of privacy leakage tolerance. Each organization O_i has a piece of social network G_i, which is part of the whole picture – a social network $\boldsymbol{G}$ constructed by integrating all G_i. Conducting the SNAM task on $\boldsymbol{G}$, one can obtain the exact SNAM result from the integrated information. However, conducting the SNAM task on any G_i, one can never achieve the exact SNAM result because of the missing information. By integrating G_i and some *generalized information* of G_j, O_i should be able to achieve more accurate SNAM results although it is not the exact SNAM result. That means if O_i can obtain generalized information from all other organizations, O_i will be able to obtain a SNAM result much closer to the exact SNAM result than that obtained from G_i alone. Figure 1 presents the framework of the subgraph generalization approach of social network integration. In this paper, we focus on the definition of the tolerance of privacy leakage during social network sharing and integration.

II. TOLERANCE OF PRIVACY LEAKAGE

While sharing and integrating the generalized information for SNAM tasks, we must ensure that a specified tolerance of privacy leakage is satisfied. The measure of privacy leakage must be independent to the techniques in generating and integrating generalized information of social networks. Privacy means that no party should be able to learn anything more than the insensitive information shared by other parties and the prescribed output of the SNAM tasks. If any adversary attack can be applied to learn any private and sensitive data, there is a privacy leakage. In this problem, the shared insensitive information is the generalized information and the identity of the insensitive nodes which are the integration points. The prescribed outputs of the SNAM tasks are the centrality measures or similarity measures such as closeness centrality of a node. The adversary attack can be active or passive attacks. Active attacks refer to planting well structured subgraphs in a social network and then discovering the links between targeted nodes by identifying the planted structures. Passive attacks refer to identifying a node by its association with neighbors and then identifying other nodes that are linked to this association. Such attack can also be considered as neighborhood attacks.

The leakage of private information includes the identities of sensitive nodes and the adjacency (i.e. edges)

of any two nodes regardless if any of these nodes are sensitive or insensitive. If any of the active or passive attacks can be applied on the generalized information or the output of the SNAM tasks to learn the abovementioned private information, there is a privacy leakage. Below are the definitions of the tolerance of privacy leakage:

Zero tolerance of privacy leakage:

(1) No exact identity of sensitive nodes can be identified.
(2) No adjacency between any two exact nodes can be identified.

τ-tolerance of privacy leakage on an sensitive node:

(1) The identity of a sensitive node cannot be identified as one of τ or fewer possible known identities.

τ-tolerance of privacy leakage on the adjacency between an insensitive node and a sensitive node:

(1) The identity of an insensitive node is known but its adjacency with other sensitive nodes is not known.
(2) The adjacent nodes cannot be identified as one of τ or fewer possible sensitive nodes.

$\tau_1\tau_2$-tolerance of privacy leakage on the adjacency between two sensitive nodes:

(1) The identity of a sensitive node *A* cannot be identified as one of τ_1 or fewer possible known identities.
(2) The adjacent node of this sensitive node *A* cannot be identified as one of τ_2 or fewer possible known identities

Zero tolerance means no attack can discover the exact identity of a sensitive node or the adjacency between any two exact nodes. Most attacks cannot discover the exact identity or adjacency given a reasonable privacy preservation technique. However, many attacks are able to narrow down the identity to a few possible known identities. For example, the identity of a sensitive node is John. If an attack discovers the identity to be John, Peter or Mary, it satisfies 3-tolerance of privacy leakage but not 4-tolerance or higher. According to these definitions, the higher the value of τ is, the tighter control of the privacy leakage is.

Zero tolerance is the minimum requirement of any privacy preservation problem. No private information should be discovered. However, to ensure a higher standard to prevent privacy leakage, τ-tolerance is proposed and defined here. Not only the exact identity of a sensitive node cannot be discovered but also the identity cannot be identified as one out of τ or fewer possible identities. Ideally, a privacy preserving technique should achieve ∞-tolerance, which means no attack can find a clue of the possible identity of a sensitive node. In reality, it is almost impossible to achieve ∞-tolerance due to the background knowledge possessed by the adversaries. However, a good privacy preserving technique should reduce privacy leakage as much as possible, which means achieving a higher value of τ in privacy leakage.

By defining the tolerance privacy leakage, we shall develop techniques to generalize insensitive information for sharing and integrate multiple generalized social networks to conduct SNAM that satisfy the prescribed level of privacy leakage tolerance.

REFERENCES

[1] C. C. Yang, N. Liu, and M. Sageman, "Analyzing the Terrorist Social Networks with Visualization Tools," in *IEEE International Conference on Intelligence and Security Informatics* San Diego, CA, 2006.

[2] C. C. Yang and T. D. Ng, "Terrorism and Crime Related Weblog Social Network: Link, Content Analysis and Information Visualization," in *IEEE International Conference on Intelligence and Security Informatics* New Brunswick, NJ, 2007.

[3] C. C. Yang, T. D. Ng, J. Wang, C. Wei, and H. Chen, "Analyzing and Visualizing Gray Web Forum Structure," in *Pacific Asia Workshop on Intelligence and Security Informatics*, 2007.

[4] C. C. Yang, "Information Sharing and Privacy Protection of Terrorist or Criminal Social Networks," in *IEEE International Conference on Intelligence and Security Informatics* Taipei, Taiwan, 2008, pp. 40-45.

[5] C. C. Yang and T. D. Ng, "Analyzing Content Development and Visualizing Social Interactions in Web Forum," in *IEEE International Conference on Intelligence and Security Informatics* Taipei, Taiwan, 2008.

[6] C. C. Yang and M. Sageman, "Analysis of Terrorist Social Networks with Fractal Views," *Journal of Information Science,* 2009.

[7] C. C. Yang and X. Tang, "Social Networks Integration and Privacy Preservation using Subgraph Generalization," Proceedings of AMC SIGKDD Workshop on CyberSecurity and Intelligence Informatics, Paris, France, June 28, 2009.

[8] C. C. Yang, X. Tang, and B. Thuraisingham, "An Analysis of User Influence Ranking Algorithms on Dark Web Forums," *Proceedings of ACM SIGKDD Workshop on Intelligence and Security Informatics (ISI-KDD), Washington, D.C.*, July 25, 2010.

[9] C. C. Yang and B. Thuraisingham, "Privacy-Preserved Social Network Integration and Analysis for Security Informatics," *IEEE Intelligent System*s, vol.25, no.3, 2010, pp. 88-90.

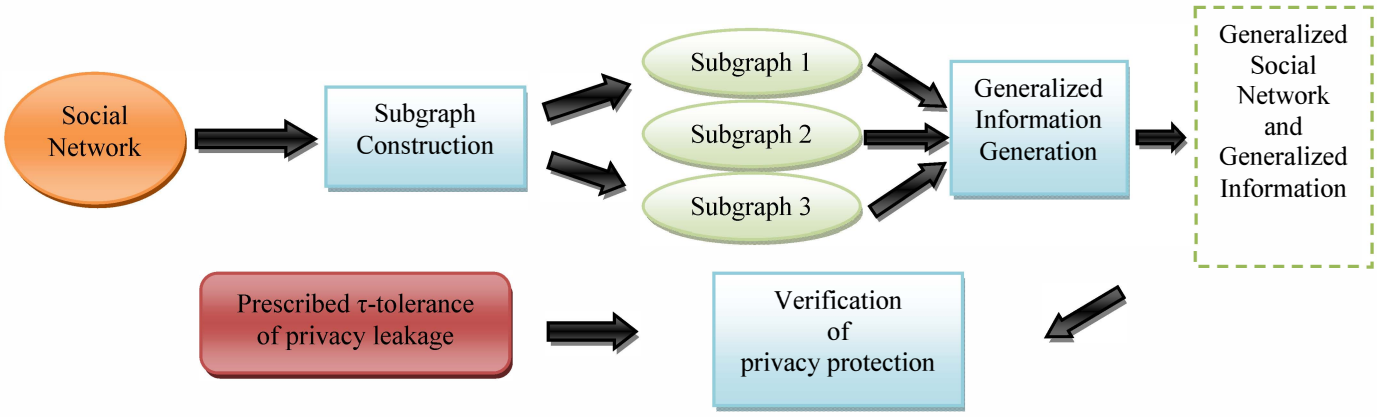

Figure 1. Framework of social network integration and privacy preservation using subgraph generalization approach.