

SLINCS: A Social Link based Evaluation System for Network Coordinate Systems

Xiaoxiao Song[†], Xiaohan Zhao[†], Eng Keong Lua[‡], Zengbin Zhang[†], Beixing Deng[†], Xing Li[†]

[†]Tsinghua National Laboratory for Information Science & Technology,
Electronic Engineering of Tsinghua University, Beijing 100084, China

E-mail: sxx05@mails.tsinghua.edu.cn

[‡]Carnegie Mellon University, Pittsburgh, PA15213, U.S.A.

E-mail: eklua@computer.org

Abstract—In recent research work of securing Network Coordinate (NC) system, they concentrate on the passive security defense mechanisms. In this paper we propose SLINCS, a social link based evaluation security system that utilizes information from existing social relationship networks to implement proactive security mechanisms for NC systems. The key idea is to eliminate suspicious nodes before they launch potential attacks.

I. INTRODUCTION

Network coordinate systems, which can estimate network delay or round trip time (RTT) with low overhead, have been proposed to support the application overlays. Previous NC systems like Vivaldi, PIC, and NPS, are easily being attacked by hackers because there is no security measure put in place. Newly established distributed NC systems, such as RVivaldi [1], Veracity [2], and systems with Kalman filter [3], have been proposed to solve the security problems in ensuring the authenticity of the node coordinates. However, they cannot actively defence potential attackers before the latter launch attacks to the systems.

In today's Internet applications, social networking that interacts with social links between users are becoming more popular. Such social friend-of-friend information can provide helpful aids to determine a node's behavior. By utilizing social relationships, the NC systems can get rid of the suspicious nodes and avoid potential attacks at the early beginning. SLINCS, under our deployment, is a system that makes use of social relationship (friend-of-friend) data extracted from dependable social network applications like Facebook to provide useful evaluation ranking of test nodes. NC systems can then request to SLINCS to obtain the cross-reference in order to make their own decisions to trust a node or not, especially when a node wants to choose trustworthy neighbors to compute its coordinate accurately. In this work, we provide a social reputation system based solution for securing NC systems in the Internet. We believe that such a solution approach is feasible, applicable and will contribute to the improvement of current security requirements of NC systems. The remaining part of this paper is organized as follows. Section 2 provides the important features in SLINCS. This is followed by a detailed description of the proposed system in section 3. Finally the paper concludes with a brief summary and a vision on the future work in section 4.

II. SLINCS FEATURES

With the aim of utilizing the information of social relationship from the Internet, SLINCS is fundamentally consisted of two kinds of nodes, "Common Node" and "Noddle", while its function is based on social link data extracted from certain Internet-based social network applications. According to Fig.1, the key features of SLINCS are grouped as:

A. SR and TP

1) *Social Relationship (SR)*: There are four basic relationship states between directly linked nodes in SLINCS, including "Friend", "Stranger", "Isolate" and "Blacklist". Each of them stands for one level of trustfulness between two directly linked nodes. Nodes will trust target nodes they regarded as "Friend" and do not trust target ones they regarded as "Blacklist", while "Stranger" means that a node does not have any social link path to a target one. The difference between "Isolate" and "Stranger" is that "Isolate" one does not link to any noddle but "Stranger" one does. Furthermore, SR states can be represented by their evaluation value accordingly. The bigger the value is, the more the target node will be trusted.

2) *Trust Profile (TP)*: TP is the evaluation data in SLINCS that records the number of times a node has been used by other nodes as their neighbor to compute coordinates.

B. Nodes

1) *Common Node*: Common node is the basic node type in SLINCS, which contains SR information related to other nodes in the system.

2) *Noddle*: Noddles are special nodes trusted by the system, which are originally deployed during the establishment of SLINCS. Common nodes expect "Isolate" nodes linked with one noddle at least, thus noddles can distinguish the "Isolate" ones easily. Unlike common nodes, noddles can also preserve the trust profiles of common ones. In order to maintain trustfulness to the system, they never use the SR knowledge they learned to compute SR values yet only use it to distinguish isolate nodes.

III. SYSTEM METHODS AND DESIGN

Most current security mechanisms in NC systems are passive, because their cognition towards malicious nodes depends

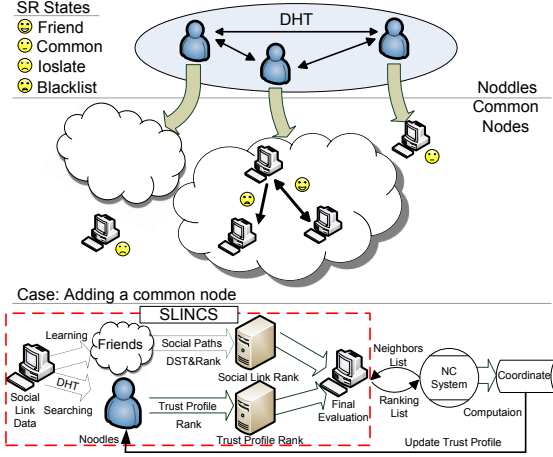


Fig. 1. SLINCS Framework

on the results of previous launched attacks. In other words, those mechanisms can not avoid potential attacks before they take place. Therefore, we deploy an active mechanism to solve the problem. The following methods used in SLINCS are essential to the design of our system:

A. Learning Method

The data of a node's SR with other nodes is saved in its social link matrix (SLM) whose elements are the value of SR. Thus, a node can learn the information about social links of certain paths from itself to its friends in the part of its friends' SLM, and then refresh its own.

B. Preserving Method

In consideration of the recoverable and robust of the system, nodes can use DHT (Distributed Hash Table) [4] to preserve and look for their trust profile to the certain noddles.

C. Evaluation Method

1) *Trust Level Evaluation*: In SLINCS, it is possible that two nodes do not connect with each other, but they may be linked through other nodes in some paths. And when there is more than one path, the SRs in these paths may be different. Thus we introduce DST (Dempster-Shafer Theory) [5] into our system to better elicit the appropriate relationship between these nodes from the different or even conflicting SR information.

2) *Final Evaluation Function*: We use the rank of trust profile (R_{tp}) and the rank of relationship values (R_{rv}) as parameters in our evaluation function to generate a target node's evaluation value (EV) to a selected one. The primary function is:

$$EV = \mu * R_{rv} + (1 - \mu) * R_{tp} \quad (1)$$

The value of coefficient μ is between 0 to 1, which indicates the weights of R_{rv} and R_{tp} . And it can be modified during the experiments.

In the nascent stage of SLINCS, we deploy adequate noddles into the system first, and then add common nodes

successively. During the constitution process, a social link matrix will be constructed in each node, while links between nodes and noddles will be formed in a hash table as well. According to the case in Fig.1, when a newcomer node enters the system after SLINCS has been established, it should firstly use Learning Method to refresh its SLM, as well as use Preserving Method to configure itself and form its TP with several suitable noddles by employing DHT method.

SLINCS can be widely used by all the current NC systems. Nodes in these systems can obtain useful rank evaluation of their neighbors by providing a chosen neighbor list. SLINCS will use an Evaluation Method to compute the evaluation values. Especially when there is not only one path between two nodes, the DST method would be employed. Then a new evaluation rank of all the neighbors in the list will be generated. It can be directly used by the nodes to choose certain neighbors and filter some suspicious nodes before calculating coordinates. It can also serve as a reference for the nodes to make better decisions on their own. Thus the overall accuracy of NC systems will be enhanced in the unauthentic conditions.

IV. CONCLUSION AND FUTURE WORK

The work in this paper proposed a social link based evaluation system, SLINCS, which we are currently developing. This paper presented a general framework and main characteristics of SLINCS. In future work, we will fully develop SLINCS and analyze its performance with real data. Moreover, we will study the influence of social relationship value, trust profile data and then try to figure out a considerable ranking evaluation function in order to better improve its performance.

V. ACKNOWLEDGMENT

This work is supported by the National Basic Research Program of China(No.2007CB310806), the National Science Foundation of China(No.60473087, No.60703052) and the National High Technology Development Program of China(No. 2007AA010306).

REFERENCES

- [1] D. Saucez and B. Donnet and O. Bonaventure. A Reputation-Based Approach for Securing Vivaldi Embedding System. Lecture Notes in Computer Science, vol 4606, 2007.
- [2] M. Sherr and B. T. Loo and M. Blaze. Veracity: A Fully Decentralized Service for Securing Network Coordinate Systems. In proceedings of IPTPS'08.
- [3] M.A. Kaafar and L. Mathy and C. Barakat. K. Salamatian and T. Turletti and W. Dabbous. Securing Internet Coordinate Embedding Systems. In proceedings of ACM SIGCOMM'07.
- [4] Sean Rhea and Brighton Godfrey and Brad Karp and John Kubiatowicz and Sylvia Ratnasamy and Scott Shenker and Ion Stoica and Harlan Yu. A Public DHT Service and Its Uses. In proceedings of ACM SIGCOMM'05.
- [5] Maxim Rayay and Panos Papadimitratos and Virgil D. Gligor and Jean-Pierre Hubaux. On DataCentric Trust Establishment in Ephemeral Ad Hoc Networks. In proceedings of Infocom'08.