Defending Sybil Attacks in Mobile Social Networks

Yan Sun[1, 2], Lihua Yin* [1, 3], Wenmao Liu[4]
[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[2] Beijing University of Posts and Telecommunications, Beijing, China
[3] Beijing Key Laboratory of IOT Information Security, Beijing, China
[4] Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Beijing, China
{sunyan, yinlihua, wenmao}@nelmail.iie.ac.cn

***Abstract*—Mobile social networks (MSNs) are a kind of delay tolerant network that consists of lots of mobile nodes with social characteristics. Recently, many social-aware algorithms have been proposed to address routing problems in MSNs. However, it also brings more security and privacy concerns. In this paper, we discuss a specific type of Sybil attack in MSNs, which few researches has been focused on. We proposed a security mechanism to detect Sybil nodes and eliminate them to ensure the routing security while routing forwarding. It needs to cooperate by two sides, which is, respectively measuring distance in client side and eliminating Sybil nodes in server side. We also demonstrate the solution is correct and analyze its energy costs.**

***Index Terms*—Sybil Attacks, Mobile Social Networks, Routing Security.**

I. INTRODUCTION

In Mobile Social Networks (MSNs), the mobile devices carrying by users are abstracted as mobile nodes with social characteristics. The topological connections between nodes not only represent both the physical device links, but also describe their social relationships. Therefore, the node in MSNs reflects the social ties of device holders while moving. Recently, many social-aware algorithms have been proposed to address routing problems in MSNs[1,2,3]. These algorithms design efficient routing strategies by making accurate analysis of social network properties. These social-aware algorithms have improved routing performance. But at the same time, these social properties in routing also bring a variety of security and privacy problem.

Sybil attacks are to disrupt routing protocols by forged identities or location, especially in the multicast routing and geographical routing. It also occurs in MSNs since MSNs usually use multicast routing and geographical routing. As shown as Fig 1, in a mobile social network scene, Alice wants to forward its message to Eva by its neighbor friend nodes. If there is a malicious node as its neighbor, its object is to cheat its neighbor node for routing selection by creating virtual nodes that are called Sybil nodes. A Sybil node has a forged identity and location and also reports its virtual location information to servers looking like a normal node. It is easy for the malicious node to forge reasonable virtual locations to disrupt routing if the malicious node knows the location information of its neighbors.

This work was supported in part by the national Natural Science Foundation of China (No.61100181, No.61070186) and the national high technology Research and Development Program of China (863 Program) (No. 2013AA014002)
* L. Yin is the corresponding author.

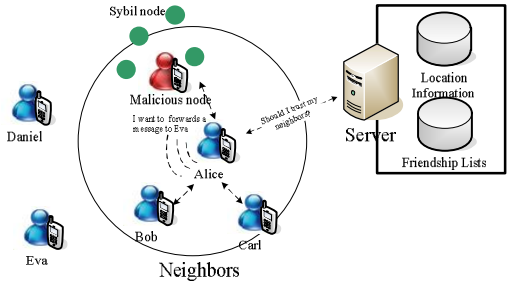

Fig. 1. A mobile social network scene

Based on the attack analysis for Sybil attacks in mobile social networks, our challenge is how to detect these virtual nodes and eliminate them to ensure the routing security while routing forwarding. In this paper, we proposed a security mechanism to detect these Sybil nodes and eliminate them while selecting routing forwarding nodes. It needs to cooperate by two sides, which is, respectively measuring distance in client side and eliminating Sybil nodes in server side. We also demonstrate the solution is correct and analyze its energy costs.

II. PROPOSED SYBIL ATTACK DEFENSE

A. Problem Statements

The attack goal of a malicious node is to cheat its neighbor node by creating virtual nodes that are called Sybil nodes. A Sybil node has a forged identity and location and reports its virtual location information to servers. It is easy for the malicious node to forge reasonable virtual locations if the malicious node knows the location information of its neighbors. To solve it, we must answer the issue that is how the malicious node could not forge a reasonable virtual location. We give the theorem 1.

Theorem 1: A malicious node cannot forge a Sybil node that has a reasonable location if it does not know the locations information of its neighbor nodes, but knows the distance information to its neighbor nodes.

Proof: we assume that the location of a malicious node is O, and it obtains locations of its three neighbor nodes, A, B, C, satisfying $OA>OB>OC$. Then, it can infer that the three neighbor nodes are in the concentric circles with the center O. The malicious node has to report these distances to A, B, C to server to forge a virtual location O'. It is difficult for it to generate three distance values satisfying a certain constraint

relationship if it doesn't know the precious location. When there is a certain density of nodes in concentric circles, the malicious node can generate several groups of distance values, some of which may be inconsistent to the constraint condition. It will be confused to determine choosing which group of distance values. Therefore, it is almost impossible to forge a reasonable virtual location.

Thus, our problem is changed to how to eliminate the virtual locations of Sybil nodes with a high probability by the inconsistent property. To solve it, we define these location coordinates in a two-dimensional coordinate system. In the system, the real Euclidean distance between nodes exists. Algorithm 1 is proposed in the server side. It use the distance set between neighbor nodes as input. The output is a set of candidate routing nodes. If there are Sybil nodes taking part in the computation, there will be a higher dimensional location to be output. The faith is that there is no such location in a two-dimensional plane, so that it could be inferred that the node is a forged node, Sybil node. Therefore, it must be removed.

B. Our Proposed Solution

Our solution is divided into two parts: the distance measurement in client side and Sybil node elimination in server side. In client side, distance measurement is computing the distance set between initiator node v and its neighbor nodes using encrypted communication to ensure the process security. In server side, Sybil node elimination is as follows: The initiator node v selects randomly two neighbor nodes, i, j, to define a plane, so that they establish a local coordinate system L. We define a set $G(V, E)$, where V is the set consisting of initiator node v and its neighbor nodes, E is the set of distances between any two nodes in V.

Algorithm 1 *Eliminate_Sybil_Node*(v)

Input: The initiator node v which is waiting for selecting honest routing forward nodes ;

Output: the set of honest routing forward nodes neighboring v.

1: Define Plane P: $(v, i, j) \rightarrow P$, where i, j are randomly selected and satisfy $i \in Nbr(v), j \in Nbr(v)$ and $i \neq j$;

2: Define local coordinate system L:$(e(v,i), e(v,j), e(i,j)) \rightarrow L$;

3: **Initialize** $G(V, E)$:
$V = v \cup Nbr(v)$
$E = \Phi$;

4: **For** each neighbor node $k \in Nbr(v)$ **do**
p_k= Trilateration(d_{kv}, d_{ki}, d_{kj});
// The k's location p_k in L is computed using trilateration with the measured distance to nodes, d_{kv}, d_{ki}, d_{kj}.
End For

5: **For** any two nodes $i, j \in V$ **do**
$c_{ij} = |p_i - p_j|$; // find the measured distance between them, d_{ij}, and obtain the computed distance, c_{ij}.

6: **If** $|d_{ij} - c_{ij}| \leq \varepsilon$ **Then**
$E = E \cup e(i, j)$; // The edge $e(i, j)$ could be added to E satisfying $|d_{ij} - c_{ij}| \leq \varepsilon$
$c_{ij} = c_{ij} + 1$;
End For

$C = \{ e(i, j) \mid v \in e(i, j)$ and c_{ij} is the maximal in the edge containing the node v.$\}$

7: **Return** C;
End

C. Algorithm Analysis

1) Algorithm proof

Theorem 2: If the randomly selected vertices are real nodes, then there is no Sybil node in the produced set of routing forward nodes using Algorithm 1.

Proof: We assume the node v's location is p_1. It selects two neighbor node p_2, p_3 to define a plane P. They are all real nodes. After measuring the distance, E contains the edges between honest neighbor nodes. On the other hand, the forged locations of Sybil nodes have not the property of consistency in P. Such locations will be in another plane. Therefore the edge between honest node and Sybil node will not to be created, and finally Sybil node is removed.

Theorem 3: If there is at least one Sybil node in the randomly selected vertices, then the amount of the produced set of routing forward nodes is less than the one of the produced set by all real nodes.

Proof: We assume the node v's location is p_1. It selects two neighbor node p_2, p_3 to define a plane P', in which p_2 is a Sybil node. Some honest nodes will be removed because there is no consistent information between honest nodes and p_2. Therefore, the amount of the produced set of routing forward nodes in P' is less than the one of the produced set by all real nodes in P.

2) Algorithm cost

For mobile terminals, they have limited energy and computation resource. In our proposed solution, the energy cost is mainly the communication cost while measuring distance in client side. We assume that the initiator node v has n-1neighbour nodes, and then it will need to collect n-1 distance information to these neighbors. One node needs at least 2n+1 packets switching. There are n nodes, so the whole process needs (2n+1)n packets switching.

The computation cost is produced to remove Sybil nodes in server side. For the algorithm 1, it is consumed by computing trilateration and comparing the measured distance with calculated distance.

III. Conclusions

In this paper, we discuss a specific type of Sybil attack in MSNs. For resisting this, we proposed a security mechanism to detect these Sybil nodes and eliminate them while routing forwarding to ensure the routing security. It needs to cooperate by the mobile terminals and servers, that is, distance measurement in client side and Sybil node elimination in server side. We also demonstrate the solution is correct and analysis its energy cost. It not only takes advantages of the social-based routing performance, but also resists Sybil attacks.

References

[1] J. Wu and Y. Wang, "Social feature-based multipath routing in delay tolerant networks," in IEEE INFOCOM, 2012, pp. 1368-1376.

[2] E. Bulut and B. K. Szymanski, "Exploiting friendship relations for efficient routing in mobile social networks", in IEEE Tran. On Parallel and Distributed Systems, vol. 23, iss. 12, pp. 2254-2265.

[3] M. Xiao, J. Wu and L. Huang, "Community-aware opportunistic routing in mobile social networks", in IEEE Tran. On Computers, 29, May, 2013.