National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

FACE TRANSITION: Obtaining Neighbour Node Anonymity in Mobile Opportunistic Social Networks

Priyanka Mohan*, Mrs. Shashi Rekha H
[1]Department of Studies in Computer Science and Engineering, VTU PG Centre, Mysuru, Karnataka, India

ABSTRACT

In mobile opportunistic social networks (MOSNs), mobile devices carried by people communicate with each other directly when they meet for proximity-based MOSN services (e.g., file sharing) without the support of infrastructures. In current methods, when nodes meet, they simply communicate with their real IDs, which leads to privacy and security concerns. Anonymizing real IDs among neighbor nodes solves such concerns. However, this prevents nodes from collecting real ID-based encountering information, which is needed to support MOSN services. In Face Change, each node continually changes its pseudonyms and parameters when communicating with neighbors nodes to hide its real ID

Keywords: Mobile opportunistic social networks, anonymity, encountering information.

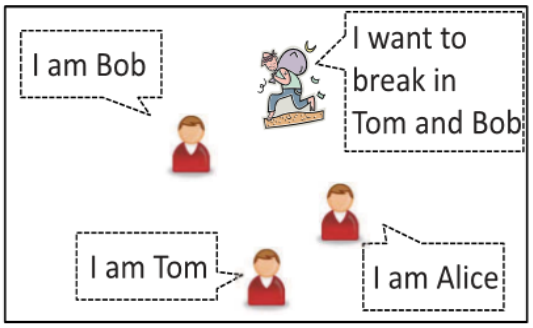
I. INTRODUCTION

Face Change that can support both anonymizing real IDs among neighbor nodes and collecting real ID-based encountering information. For node anonymity, two encountering nodes communicate anonymously. Only when the two nodes disconnect with each other, each node forwards an encrypted encountering evidence to the encountered node to enable encountering information collection. A set of novel schemes are designed to ensure the confidentiality and uniqueness of encountering evidences. FaceChange also supports fine-grained control over what information is shared with the encountered node based on attribute similarity (i.e., trust), which is calculated without disclosing attributes. Advanced extensions for sharing real IDs between mutually trusted nodes and more efficient encountering evidence collection are also proposed. Extensive analysis and experiments show the effectiveness of FaceChange on protecting node privacy and meanwhile supporting the encountering information collection in MOSNs. Implementation on smart phones also demonstrates its energy efficiency.

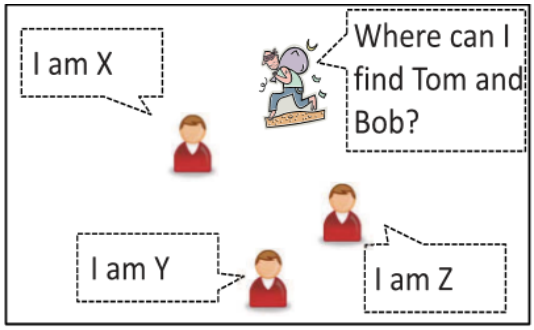
A. Aims and Objectives

- ✓ In Face Change, each node continually changes its pseudonyms and parameters when communicating with neighbours nodes to hide its real ID.
- ✓ Face Change prevents two encountering nodes from disclosing the real IDs during the encountering, so malicious nodes cannot identify targets from neighbours for attack.
- ✓ Packet routing can be conducted correctly and efficiently in Face Change.

II. ARCHITECTURE



(a)



(b)

Figure 1. Demonstration of a privacy issue and a possible solution in MOSNs.
(a) Possible privacy issue.
(b) Solution: neighbor Anonymity.

Figure 1(a), When neighbor nodes communicate with real IDs, a malicious node can easily identify attack targets from neighbors and launch attacks to degrade the system performance or steal important documents. Further, without protection, malicious nodes can also easily sense the encountering between nodes for attacks. Therefore, neighbor node anonymity is needed to prevent the disclosure of real IDs to neighbors. Clearly, a permanent pseudonym cannot achieve such a goal since it can be linked to a node, which can still enable malicious nodes to recognize targets from neighbor nodes. Thus, an intuitive method to realize the neighbor node anonymity is to let each node continuously change its pseudonym used in the communication with neighbors, as shown in Figure 1(b). However, when neighbor node anonymity is enforced, nodes cannot collect the real ID based encountering information (i.e., cannot know whom they have met), which disables a aforementioned MOSN services.

III. METHODOLOGY

Modules

- ❖ Preventing Nodes
- ❖ Encountering Evidence Relaying Scheme
- ❖ Trust authority (TA)
- ❖ Packet Routing Process

Modules description:

Preventing Nodes: FaceChange can prevent malicious nodes from acquiring meaningful private information by overhearing the encountering evidences and packets transmitted between two nodes. Firstly the encountering evidence is encrypted by a key originated from two randomly generated numbers from the two encountering nodes, which are not disclosed in the network. Then, the eavesdropper cannot understand the content in the transmitted encountering evidences. Secondly in MOSN routing, the receiver of a packet is not necessary the destination of the packet. As a result, the eavesdropper cannot determine the ID of a node based on packets it receives

Encountering Evidence Relaying Scheme: In this scheme, during the encountering, the recipient node specifies a relay node and encrypts its real ID with the public key of the relay node. It then forwards such information to the creator. Later, after the two nodes separate, the creator routes the encountering evidence to the relay node, which decrypts the ID of the recipient node and further routes the evidence to the recipient node, thereby delivering the encountering evidence. A trusted node refers to the node that is believed to keep its private key secure (i.e., does not share it with any other nodes). Otherwise, neighbor anonymity may be broken during the encountering. This is because, when two nodes meet, each node encrypts its real ID with the public key of the relay node and sends that to the encountered node. Then, if the relay node's private key is disclosed, the real ID is no longer safe.

Trust authority (TA) The trust authority (TA), for the corresponding service. Since those services are

built upon node encountering, nodes need to collect real ID based encountering information. For example, nodes need to know whom they have met to identify proximity based social community/relationships. In packet routing, nodes need to collect the encountering information to deduce their future meeting probabilities with others. Then, a packet can always be forwarded to the appropriate forwarder Trust Authority (TA) in the system responsible for some system management functions such as system parameters and certificates distribution and attribute validation(e.g., reputation, affiliation, and ID), both of which can be conducted off-line.

Packet Routing Process: In traditional MOSN packet routing, two encountering nodes first delivers packets destined for the other node. They then compare routing utilities and forward the other node packets that the other node has a higher routing utility for their destinations. In FaceChange, neighbor node anonymity blocks the first step by preventing nodes from recognizing the destinations of their packets even when meeting them. To solve this problem, we let each node claim to have higher routing utility for itself to fetch packets for it.

IV. CONCLUSIONS

Face Change, a system that supports both neighbor anonymity and real ID based encountering information collection in MOSNs. In Face Change, each node continually changes its pseudonyms and parameters when communicating with neighbors nodes to hide its real ID. Encountering evidences are then created to enable nodes to collect the real ID based encountering information. After two encountering nodes disconnect, the encountering evidence is relayed to the encountered node through a selected relay node. Practical techniques are adopted in these steps to ensure the security and efficiency of the encountering evidence collection. Trust based control over what information can be included in the encountering evidence is supported in Face Change .Advanced extensions have also been proposed to support the "white list" feature and enhance the encountering evidence relaying efficiency. Extensive analysis and experiments are conducted to prove the effectiveness and energy efficiency of Face Change in protecting node privacy and supporting he encountering information collection in MOSNs. In the future, we plan to investigate how to generalize the process of adapting applications in mobile opportunistic social networks to Face Change seamlessly.

V. ACKNOWLEDGEMENT

The authors are hereby expressing their sincere thanks to HOD, faculty members and supporting staff of 'Centre of PG Studies, VTU, Mysuru' for providing valuable guidance and support. Without their cooperation this could have not been made.

VI. REFERENCES

1. M K. F. Dan Boneh, "Identity-based encryption from the weil pairing," in Proc. CRYPTO, 2001, pp. 213–229.
2. A C. Yao, "Protocols for secure computations," in Proc. FOCS, Washington, DC, USA, Nov. 1982, pp. 160–164.
3. F Li and J. Wu, "MOPS: Providing content-based service in disruption tolerant networks," in Proc. IEEE ICDCS, Jun. 2009, pp. 526–533.
4. M Motani, V. Srinivasan, and P. S. Nuggehalli, "People Net: Engineering a wireless virtual social network," in Proc. MOBICOM, 2005,pp. 243–257.
5. G Costantino, F. Martinelli, and P. Santi, "Privacy-preserving interest casting in opportunistic networks," in Proc. IEEE WCNC, Apr. 2012,pp. 2829–2834.