PROXIMITY BASED FILE SHARING IN MOBILE ONLINE SOCIAL NETWORKS WITH FINE-GRAINED CONTROL

K.Vimala,
Assistant Professor,
Department of Computer Science,
Pavai Arts and Science College for Women,
Pachal, Namakkal,Tamilnadu.

M.Sathya,
Research Scholar,
Department of Computer Science,
Pavai Arts and Science College for Women,
Pachal, Namakkal,Tamilnadu.

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. 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.

Keywords: Mobile Opportunistic Social Networks, Relaying Scheme, peer-to-peer

I. INTRODUCTION

In current MOSN applications, nodes can collect real ID based encountering information easily since neighbor nodes communicate with real IDs directly. We define two nodes as neighbor nodes when they are within the communication range of each other. However, when using real IDs directly, the disclosure of node ID to neighbor nodes would create privacy and security concerns. For example, a malicious node can first know the IDs of some central nodes or nodes with specific interests. Then, as shown in 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.

Consequently, there is a challenge on anonymizing neighbor nodes for privacy protection and meanwhile still supporting encountering information collection in MOSNs. There are rich investigations on protecting node privacy in MOSNs. However, most of related works focus on anonymizing interests and profiles and are not designed for neighbor node anonymity, which is a feature provided in this paper. The work in supports neighbor node anonymity but fails to provide encountering information collection at the same time. Therefore, we propose FaceChange to realize bot aforementioned goals based on a key observation in MOSNs. That is, disconnected nodes cannot communicate with each other directly in MOSNs, which makes attacking disconnected nodes almost impossible. This also means that knowing real IDs after the encountering would not compromise the privacy protection. Thus, the proposed FaceChange keeps node anonymity only during the encountering and postpone the real ID based encountering information collection to a moment after two neighbor nodes disconnect with each other.

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.

Encountering Evidence Generation Scheme: More similar attributes (e.g., affiliation and reputation) between two nodes often denote higher trust between them. Thus, we realize the control on the contents in an encountering evidence based on the attribute similarity. We use the commutative encryption and the solution for "the millionaire's problem" to calculate the attribute similarity blindly in this process, which protects node privacy.

With neighbor anonymity, a node may fail to recognize the destinations of its packets even when meeting them, thereby making it hard to deliver packets. We solve this problem by letting nodes pretend to be a better forwarder for packetsdestined for them to fetch these. As a result, packet routing can be conducted correctly and efficiently in FaceChange. This shows that MOSN services can be supported when FaceChange is adopted.

We further design two advanced extensions to enhance the practicability of FaceChange. The first one enables mutually trusted nodes to disclose real IDs to each other during the encountering, and the second one enhances the routing efficiency of the encountering evidence relaying. In summary, the major contribution of this paper is to propose a novel design that supports both neighbor node anonymity and real ID based encountering information collection in MOSNs. FaceChange prevents two encountering nodes from disclosing the real IDs during the encountering, so malicious nodes cannot identify targets from neighbors for attack. When nodes move away from each other, they rely on the encountering evidence to know the real IDs of nodes they have met to support MOSN services. This is acceptable since in MOSNs, a malicious node cannot communicate with a disconnected node for attacks.

II. RELATED WORK

There are already many social network based MOSN routing algorithms. Those works utilize various social factors such as frequently met friends, co-location records, centrality, transient contacts, and contact-based community to deduce a node's future meeting probabilities with other nodes. Then, packets are always forwarded to the node with a higher ability to meet their destinations. There are also some applications in MOSNs. The work proposes three distributed community detection methods in DTNs. In SMART, each node constructs a social map including frequently met nodes to guide packet routing. The works in and realize peer-to-peer (P2P) file sharing and publish/subscribe overlay in DTNs, respectively. In PeopleNet, questions are first forwarded to matched geographical community and then propagated within the community via P2P connectivity to seek for answers. Neighbor nodes in these algorithms communicate directly to collect encountering information for various services. Then, mobile users may be reluctant to participate in the MOSN services due to privacy concerns. Therefore, it is essential to provide neighbor node anonymity for privacy protection.

III. PROBLEM STATEMENT

3.1 EXISTING MODEL

In current MOSN applications, nodes can collect real ID based encountering information easily since neighbor nodes communicate with real IDs directly. We define two nodes as neighbor nodes when they are within the communication range of each other.

Most of existing system works focus on anonymizing interests and profiles and are not designed for neighbor node anonymity, which is a feature provided in this paper.

The work in existing supports neighbor node anonymity but fails to provide encountering information collection at the same time

3.1.1 Drawbacks

When using real IDs directly, the disclosure of node ID to neighbor nodes would create privacy and security concerns.

A malicious node can easily identify attack targets from neighbors and launch attacks to degrade the system performance or steal important documents.

Without protection, malicious nodes can also easily sense the encountering between nodes for attacks.

Pseudonym cannot achieve

3.2 PROPOSED SYSTEM

We propose FaceChange to realize both aforementioned goals based on a key observation in MOSNs. That is, disconnected nodes cannot communicate with each other directly in MOSNs, which makes attacking disconnected nodes almost impossible. This also means that knowing real IDs after the encountering would not compromise the privacy protection. Thus, the proposed FaceChange keeps node anonymity only during the encountering and postpone the real ID based encountering information collection to a moment after two neighbor nodes disconnect with each other.

The major contribution of this paper is to propose a novel design that supports both neighbor node anonymity and real ID based encountering information collection in MOSNs.

FaceChange prevents two encountering nodes from disclosing the real IDs during the encountering, so malicious nodes cannot identify targets from neighbors for attack. When nodes move away from each other, they rely on the encountering evidence to know the real IDs of nodes they have met to support MOSN services. This is acceptable since in MOSNs, a malicious node cannot communicate with a disconnected node for attacks.

3.2.1 Advantages Of Proposed System

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.

We realize the control on the contents in an encountering evidence based on the attribute similarity.

Packet routing can be conducted correctly and efficiently in FaceChange. This shows that MOSN services can be supported when FaceChange is adopted.

IV. METHODOLOGY

Network Model

We focus on a mobile opportunistic social network with m human-carried mobile devices, denoted by N_i ($i \in [1,m]$). We assume that the network is large. Otherwise, a node can easily guess the identities of its neighbors. Mobile devices/nodes follow the mobility of people carrying them to move in the network. Each node (i.e., device) has a limited communication range, and two nodes can communicate only when they are within the communication range of each other. Efficient neighbor discovery method that dynamically adjusts the neighbor scanning interval can be adopted to save energy.

Adversary Model

In this paper, we assume malicious nodes can attack targetnodes only when they find targets from neighbor nodes.This is reasonable since 1) an attacker in MOSNs cannot communicate with the target directly if they are not neighbors, and 2) it is costly to attack every encountered node. This meansthat malicious nodes can steal privacies or launch attacks only after identifying target nodes from neighbor nodes. Thus, in this paper, we focus on preventing real ID leakage during the communication between neighbor nodes, while still supporting encountering information collection.

Cryptographic Techniques

1) Bilinear Pairing: Let G1, G2 and GT be three cyclic groups with the same prime order q, and $P \in$ G1 and $Q \in$ G2 be generators of G1 and G2, respectively. A bilinear pairing is a map e: G1 × G2 → GT satisfying the following properties [18]:

• Bilinearity: $\forall a, b \in Z\ q : e(aP, bQ) = e(P,Q)ab$
• Non-degeneracy: $e(P,Q)$ _= 1
• Computability: e can be computed efficiently

We utilize symmetric pairing in this paper, in which G1 = G2 = G and they have the same generator P. As mentioned in Section IV-A, upon the start of the system, the TA first generates parameters for the adopted bilinear pairing, i.e., *BiParas*. In this step, TA randomly selects a security parameter ς and runs the bilinear pairing generation function $F(\varsigma)$ to generate these parameters (*BiParas*): (e, q, P,G,GT).
2) Commutative Encryption: A commutative encryption algorithm E(·)satisfies the commutative property. That is, for any encryption keys ki and kj , message M, rational number t and $\gamma < 1/2t$, it holds
• Eki (Ekj (M)) = Ekj (Eki (M)),
• $\forall M1$ _= $M2$, Pr(Eki (Ekj ($M1$)) = Ekj (Eki ($M2$))) < γ.
where Eki (M) is the result of encrypting M with key ki. Many commutative encryption algorithms exist, such as RSA [36] and one-time pad. These algorithms have different complexity and security levels. Nodes can select a commutative encryption algorithm based on their specific requirements. The work in adopts Pohlig-Hellman encryption to realize a commutative encryption algorithm with acceptable security and complexity.

V. PERFORMANCE EVALUATION

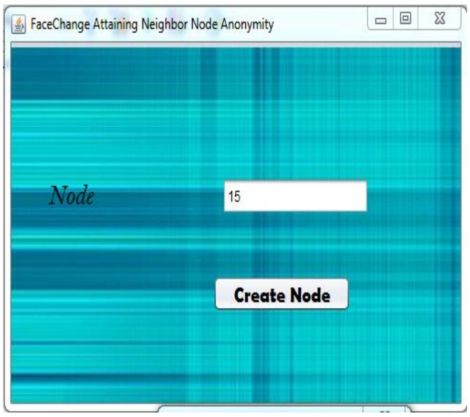

Fig 5.1.1 Create Node

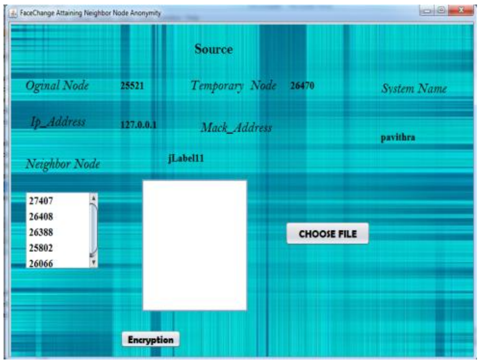

Fig 5.1.2 Source

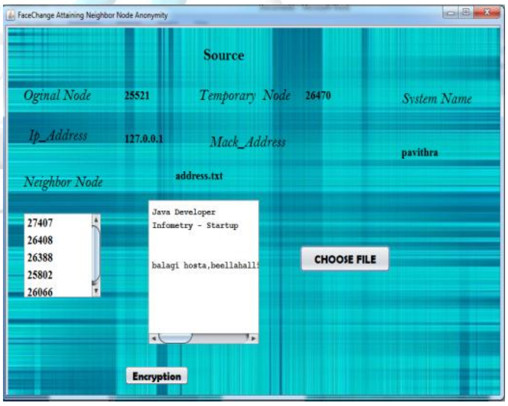

Fig 5.1.3 Select file

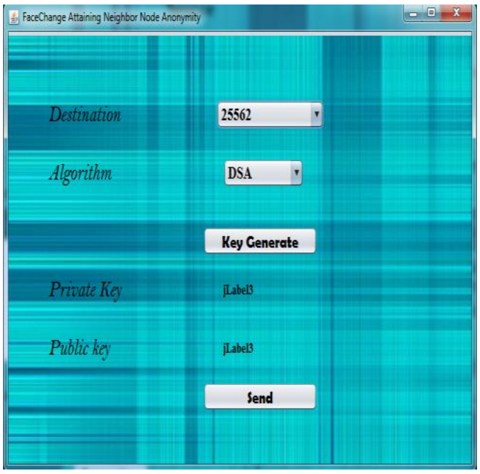

Fig 5.1.4 Key Generate

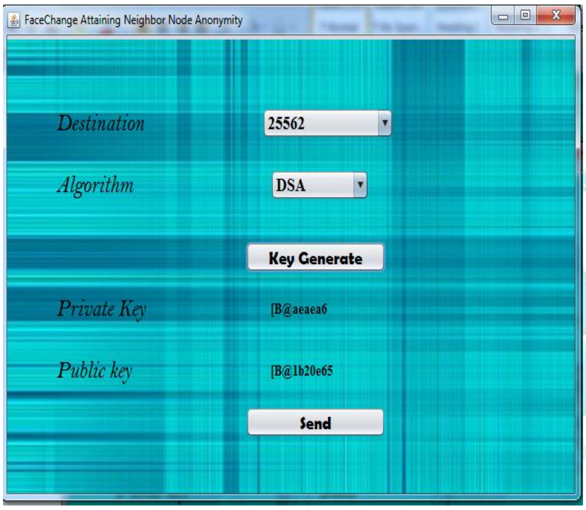

Fig 5.1.5 Select node

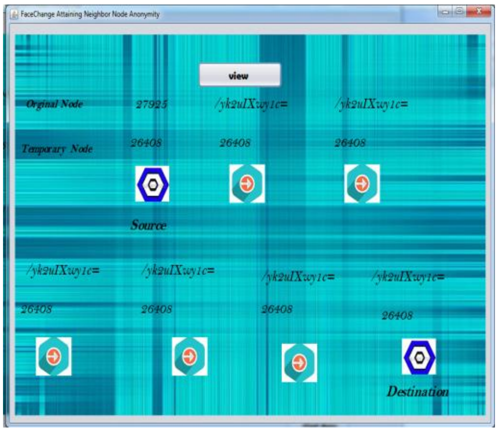

Fig 5.1.6 Node details

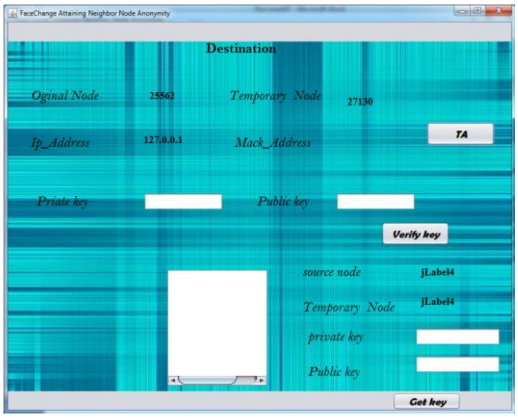

Fig 5.1.7 Destination node

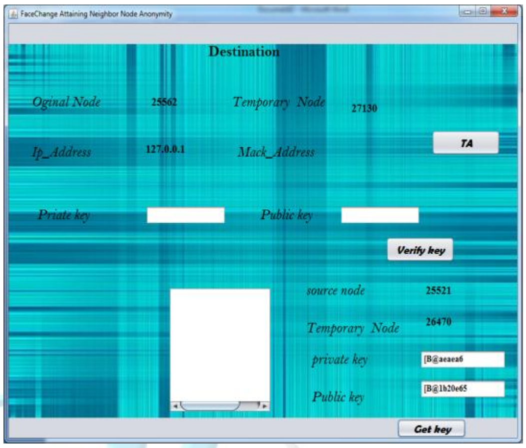

Fig 5.1.8 Verify Key

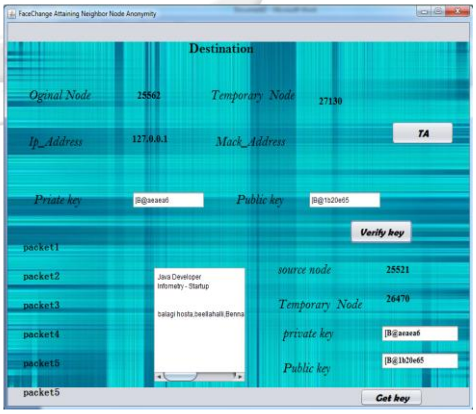

Fig 5.1.9. Verified Key and received packets

VI. CONCLUSION

In this STUDY, we propose FaceChange, a system that supports both neighbor anonymity and real ID based encountering information collection in MOSNs. In FaceChange, each nodecontinually 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.

VII. REFERENCE

[1] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," in *Proc. SIGCOMM*, 2004, pp. 145–158.

[2] J. Wu, M. Xiao, and L. Huang, "Homing spread: Community home-based multi-copy routing in mobile social networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2319–2327.

[3] T. Ning, Z. Yang, H. Wu, and Z. Han, "Self-interest-driven incentives for ad dissemination in autonomous mobile social networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2310–2318.

[4] A. Balasubramanian, B. Levine, and A. Venkataramani, "DTN routing as a resource allocation problem," in *Proc. SIGCOMM*, 2007, pp. 373–384.

[5] P. Hui, E. Yoneki, S. Y. Chan, and J. Crowcroft, Distributed community detection in delay tolerant networks," in *Proc. MobiArch*, 2007, Art. no. 7,

[6] K. Chen and H. Shen, "SMART: Lightweight distributed social map based routing in delay tolerant networks," in *Proc. IEEE ICNP*, Oct./Nov. 2012, pp. 1–10.

[7] K. Chen, H. Shen, and H. Zhang, "Leveraging social networks for p2p content-based file sharing in disconnected MANETs," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 235–249, Feb. 2014.

[8] F. Li and J. Wu, "MOPS: Providing content-based service in disruptiontolerant networks," in *Proc. IEEE ICDCS*, Jun. 2009, pp. 526–533.

[9] M. Motani, V. Srinivasan, and P. S. Nuggehalli, "PeopleNet: Engineering a wireless virtual social network," in *Proc. MOBICOM*, 2005, pp. 243–257.

[10] G. Costantino, F. Martinelli, and P. Santi, "Privacy-preserving interestcasting in opportunistic networks," in *Proc. IEEE WCNC*, Apr. 2012, pp. 2829–2834.

[11] R. Lu *et al.*, "Prefilter: An efficient privacy-preserving relay filtering scheme for delay tolerant networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1395–1403.

[12] L. Guo, C. Zhang, H. Yue, and Y. Fang, "A privacy-preserving socialassisted mobile content dissemination scheme in DTNs," in *Proc. IEEEI NFOCOM*, Apr. 2013, pp. 2301–2309.

[13] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2147–2155.

[14] M. Li, N. Cao, S. Yu, and W. Lou, "findu: Privacy-preserving personal profile matching in mobile social networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2435–2443.

[15] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1969–1977.

[16] X. Liang, X. Li, K. Zhang, R. Lu, X. Lin, and X. S. Shen, "Fully anonymous profile matching in mobile social networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 641–655, Sep. 2013.

[17] R. Lu, X. Lin, Z. Shi, B. Cao, and X. S. Shen, "IPAD: An incentive and privacy-aware data dissemination scheme in opportunistic networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 445–449.

[18] M. K. F. Dan Boneh, "Identity-based encryption from the weil pairing," in *Proc. CRYPTO*, 2001, pp. 213–229.

[19] M. Kantarcioglu and C. Clifton, "Privacy-preserving distributed mining of association rules on horizontally partitioned data," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 9, pp. 1026–1037, Sep. 2004.

[20] A. C. Yao, "Protocols for secure computations," in *Proc. FOCS*, Washington, DC, USA, Nov. 1982, pp. 160–164.

[21] E. M. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant manets," in *Proc. MobiHoc*, 2007, pp. 32–40.