Face Change: Attaining Neighbor Node Anonymity in Mobile Opportunistic Social Networks with Fine-Grained Control

M.KEERTHI SPANDANA[1], S.YAKHOOB ALI[2]
[1]PG Student, Dept of CSE, VITS, PRODDATUR.
[2]Assistant Professor, Dept of CSE, VITS, PRODDATUR.

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. Therefore, in this paper, we propose FaceChange 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 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 smartphones also demonstrates its energy efficiency.

1. INTRODUCTION

As a special form of delay tolerant networks (DTNs), mobile opportunistic social networks (MOSNs) have attracted much attention due to the increasing popularity of mobile devices, e.g., smartphones and tablets. In MOSNs, mobile devices carried by people communicate with each other directly without the support of infrastructures when they meet (i.e., within the communication range of each other) opportunistically. Such a communication model can be utilized to support various applications without infrastructures, such as packet routing between mobile nodes, encountering based social community/relationship detection, and distributed file sharing and Question & Answer (Q&A) in a community. In each system, a node is uniquely labeled by an unchanging ID (defined real ID), which is obtained from 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 canal ways be forwarded to the appropriate forwarder. 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.

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 Face Change 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 Face Change keeps node anonymity only during the encountering and postpones the real ID based encountering information collection to a moment after two neighbor nodes disconnect with each other. Illustrates the design of Face Change. When two nodes meet, they communicate anonymously. However, each of them creates encountering evidence that contains their real IDs. The encountering evidences are sent to the other node only when they separate, thus enabling the encountering information collection while keeping the anonymity during the encountering. For encountering evidence, we call the node that

creates it as the creator and the encountered node that is to receive it as the recipient.

2. EXISTING SYSTEM

- 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

DISADVANTAGES

- 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. PROPOSED SYSTEM

- We propose Face Change 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 Face Change 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.
- Face Change 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.

ADVANTAGES

- 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.

4. FEASIBILIY REPORT

PRELIMINARY INVESTIGATION

The first and foremost strategy for development of a project starts from the thought of designing a mail enabled platform for a small firm in which it is easy and convenient of sending and receiving messages, there is a search engine ,address book and also including some entertaining games. When it is approved by the organization and our project guide the first activity, ie. preliminary investigation begins. The activity has three parts:

- **Request Clarification**
- **Feasibility Study**
- **Request Approval**

REQUEST CLARIFICATION

After the approval of the request to the organization and project guide, with an investigation being considered, the project request must be examined to determine precisely what the system requires.

Here our project is basically meant for users within the company whose systems can be interconnected by the Local Area Network (LAN). In today's busy schedule man need everything should be provided in a readymade manner. So taking into consideration of the vastly use of the net in day to day life, the corresponding development of the portal came into existence.

FEASIBILITY ANALYSIS

An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time. The different feasibilities that have to be analyzed are

- **Operational Feasibility**
- **Economic Feasibility**
- **Technical Feasibility**

Operational Feasibility

Operational Feasibility deals with the study of prospects of the system to be developed. This system operationally eliminates all the tensions of the Admin and helps him in effectively tracking the project progress. This kind of automation will surely reduce the time and energy, which previously consumed in manual work. Based on the study, the system is proved to be operationally feasible.

Economic Feasibility

Economic Feasibility or Cost-benefit is an assessment of the economic justification for a computer based project. As hardware was installed from the beginning & for lots of purposes thus the cost on project of hardware is low. Since the system is a network based, any number of employees connected to the LAN within that organization can use this tool from at anytime. The Virtual Private Network is to be developed using the existing resources of the organization. So the project is economically feasible.

Technical Feasibility

According to Roger S. Pressman, Technical Feasibility is the assessment of the technical resources of the organization. The organization needs IBM compatible machines with a graphical web browser connected to the Internet and Intranet. The system is developed for platform Independent environment. Java Server Pages, JavaScript, HTML, SQL server and WebLogic Server are used to develop the system. The technical feasibility has been carried out. The system is technically feasible for development and can be developed with the existing facility.

MODULES

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 canal ways 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. This is because without a TA, no trust can be built upon the network to support applications. The TA is affixed server with both wireless capability and Internet access. Its real ID is always visible for easy access. Nodes can access the TA through two ways: 1) when moving close to the TA and 2) when having access to the Internet through WiFi or LTE. When a node connects to the TA, it can get the updated system information such as the set of legal node IDs.

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 Face Change, 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.

5. TESTING

A. INTRODUCTION

Testing is a process, which reveals errors in the program. It is the major quality measure employed during software development. During software development, during testing, the program is executed with a set of test cases and the output of the program for the test cases is evaluated to determine if the program is performing as it is expected to perform.

B. TESTING METHODOLOGIES

In order to make sure that the system does not have errors, the different levels of testing strategies to that are applied to at differing phases of software development.

Unit Testing

Unit testing is done on individual modules as they are completed and become executable. It is confined only to the designer's requirements.

Each module can be tested using the following two Strategies,

Black Box Testing

In this strategy some test cases are generated as input conditions that fully execute all functional requirements for the program. This testing has been uses to find errors in the following categories:

- Incorrect or missing functions
- Interface errors
- Errors in data structure or external database access
- Performance errors
- Initialization and termination errors.

In this testing only the output is checked for correctness. The logical flow of the data is not checked.

White Box Testing

In this the test cases are generated on the logic of each module by drawing flow graphs of that module and logical decisions are tested on all the cases. It has been uses to generate the test cases in the following cases:

- Guarantee that all independent paths have been executed.
- Execute all logical decisions on their true and false Sides.
- Execute all loops at their boundaries and within their operational bounds
- Execute internal data structures to ensure their validity.

Integrating Testing

Integration testing ensures that software and subsystems work together a whole. It tests the interface of all the modules to make sure that the modules behave properly when integrated together.

System Testing

Here the entire software system is tested. The reference document for this process is the requirements document, and the goal is to see if software meets its requirements. Here entire 'Cybernetic Protectors Application' has been tested against requirements of project and it is checked whether all requirements of project have been satisfied or not.

Acceptance Testing

Acceptance Test is performed with realistic data of the client to demonstrate that the software is working satisfactorily. Testing here is focused on external behavior of the system; the internal logic of program is not emphasized. In this project 'Cybernetic Protectors Application' I have collected some data and tested whether project is working correctly or not. Test cases should be selected so that the largest number of attributes of an equivalence class is exercised at once. The testing phase is an important part of software development. It is the process of finding errors and missing operations and also a complete verification to determine whether the objectives are met and the user requirements are satisfied.

Test Approach

Testing can be done in two ways:

- Bottom up approach
- Top down approach

Bottom Up Approach

Testing can be performed starting from smallest and lowest level modules and proceeding one at a time. For each module in bottom up testing a short program executes the module and provides the needed data so that the module is asked to perform the way it will when embedded within the larger system.

Top down Approach

This type of testing starts from upper level modules. Since the detailed activities usually performed in the lower level routines are not provided stubs are written. A stub is a module shell called by upper level module and that when reached properly will return a message to the calling module indicating that proper interaction occurred. No attempt is made to verify the correctness of the lower level module.

Validation

The system has been tested and implemented successfully and thus ensured that all the requirements as listed in the software requirements specification are completely fulfilled. In case of erroneous input corresponding error messages are displayed.

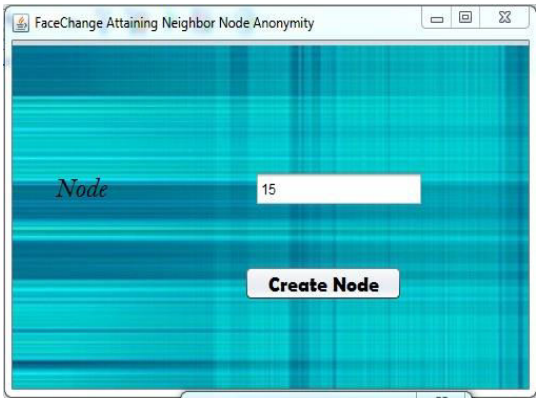
TEST CASES

S. No.	TEST CASES	INPUT	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Creating Nodes	Enter No OfNodes	Nodes Created	Nodes Created Successfully	Pass
2	Creating Nodes	Not Entered Nodes	Nodes creation Fail	Fail Create Nodes	Fail
3	Browse The File	Give the available File	File Contents Should be displayed	Display File Contents	Pass
4	Destination Node and Algorithm	Select the Destination node and algorithm	Node name and Algorithm Should be displayed	Selected Node and Algorithm displayed	Pass
5	Generate Key	Click on Generate Key Button	Private and Public Keys Should be Generate	Keys displayed	Pass
6	Verify keys	Enter the Private and Public Keys	Verify Keys Success	Keys Verified Successfully	Pass

Table: Test Case Results

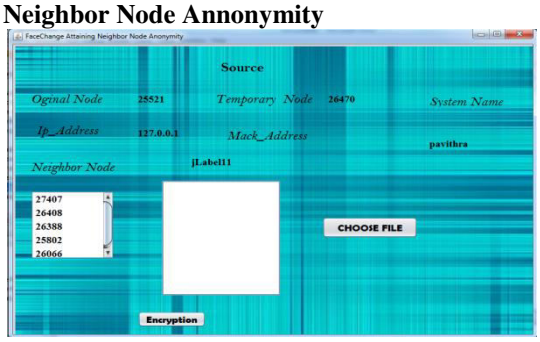
6. OUTPUT SCREENS

Create Node



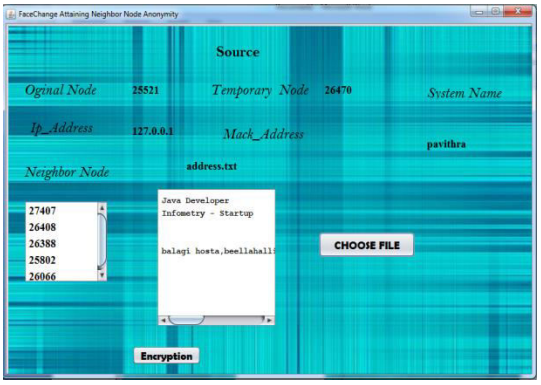
Screen 1: Create No Nodes

Neighbor Node Annonymity



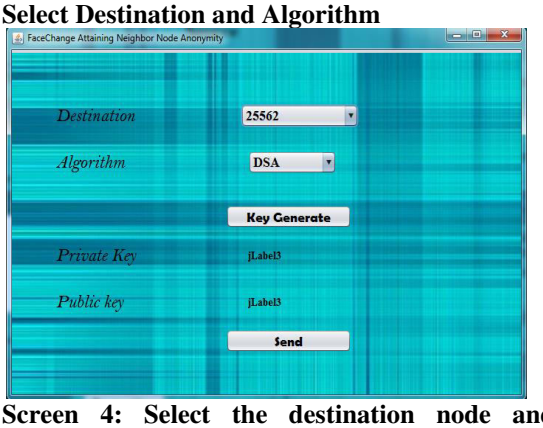
Screen 2: Neighbor Node Annonymity

Browse File



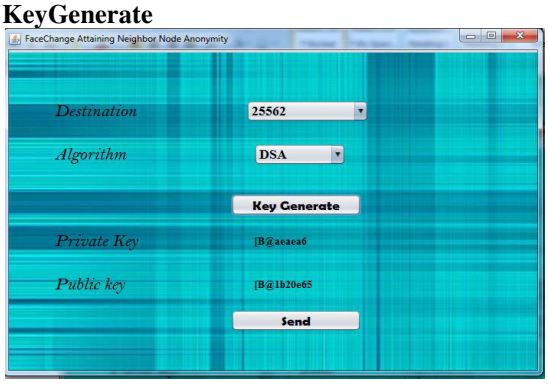
Screen 3:Browse the File to Send

Select Destination and Algorithm



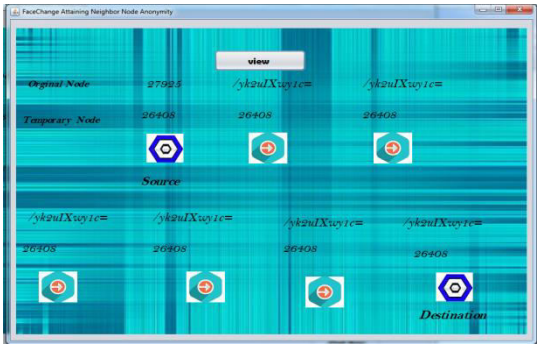
Screen 4: Select the destination node and Algorithm

KeyGenerate



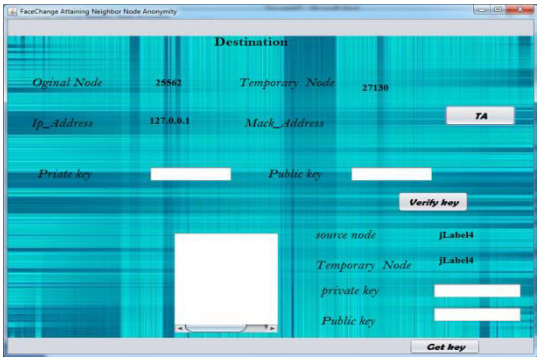
Screen 5: Generate Private and Public Keys

Data Transmission



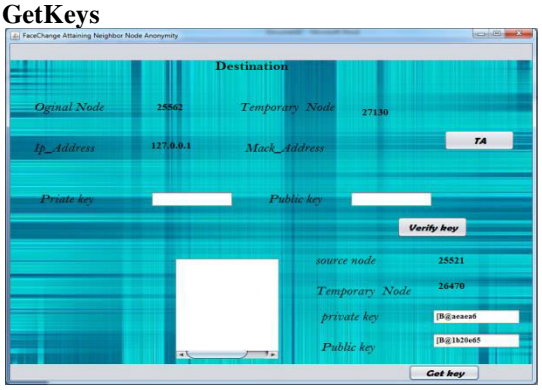
Screen 6: Data Transmission to Destination

Destination



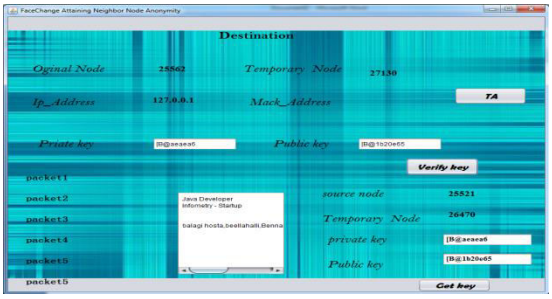
Screen 7: Destination

GetKeys



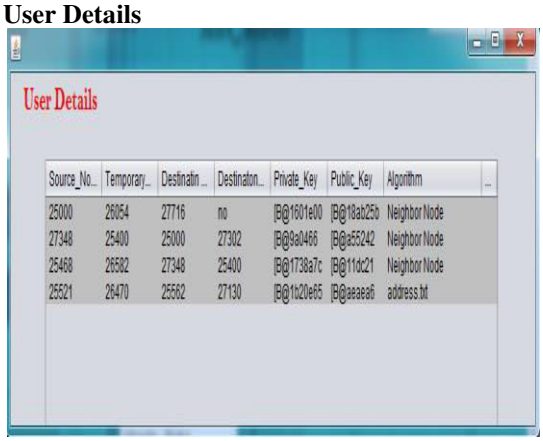
Screen 8: Get Private and Public keys

Verify and Retrieve



Screen 9: Verify and Retrieve the File

User Details



Screen 10: User Details at TA

CONCLUSION

In this paper, we propose 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 isrelayed 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 evidencere laying efficiency. Extensive analysis and experiments are conducted to prove the effectiveness and energy efficiency of Face Change in protecting node privacy and supporting the encountering information collection in MOSNs.

REFERENCES

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

[2] J. Wu, M. Xiao, and L. Huang, "Homing spread: Communityhome-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 incentivesfor 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 asa resource allocation problem," in Proc. SIGCOMM, 2007, pp. 373–384.

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

[6] K. Chen and H. Shen, "SMART: Lightweight distributed social mapbased 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 forp2p content-based file sharing in disconnected MANETs," IEEE Trans.MobileComput., vol. 13, no. 2, pp. 235–249, Feb. 2014.

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

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

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

[11] R. Lu et al., "Prefilter: An efficient privacy-preserving relay filteringscheme 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 socialassistedmobile content dissemination scheme in DTNs," in Proc. IEEEINFOCOM, Apr. 2013, pp. 2301–2309.