IDENTIFYING ANONYMITY NEIGHBOR NODE IN MOSN WITH FINE-GRAINED CONTROL

[1] V. Nirmala, [2] M. Usha

[1]Assistant Professor , [2]MCA Student
[1]MCA Department,
[1]Annamacharya PG college of Computer Studies , Rajampet, Y.S.R kadapa, Andhra Pradesh, India

Abstract:
Mobile Opportunistic Social Networks (MOSNs) is a mobile devices carried by people communicate with each other directly, when they meet for proximity-based MOSN services (eg: file sharing) without the support of infrastructures. Such a communication model utilized to support various applications without infrastructure, the packet routing between mobile nodes encountering based social community detection. For node anonymity, two encountering nodes communicate anonymously. Only when the two nodes disconnect with each others, to each node forward encrypted encountering evidence. This is designed to ensure the confidentiality and uniqueness of encountering evidence. This MOSN also supports fine-grained control over what information is shared with the encountered node based on attribute similarity (trusted nodes). The main purpose is creating the temporary nodes for the original nodes while transmission of the data and encrypt the data before sending the data to network. Identifying anonymity neighbor node in MOSN with fine-grained control is implementation on smart phones.

.

IndexTerms: **Introduction, existing work, proposed work, fine-grained control**

I. 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., smart phones 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 realID 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. 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. However, when neighbor node anonymity is enforced, nodes cannot collect the realID based encountering information (i.e., cannot know whom they have met), which disables a fore mentioned MOSN services. Consequently, there is a challenge on anonym zing neighbor nodes for privacy protection and meanwhile still supporting countering information collection in MOSNs. 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 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 packets destined for them to fetch these packets. 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 project 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 disconnected node for attacks. In the following, introduces related work. Presents the preliminary background and introduce the design of FaceChange and two advanced extensions, respectively. Section evaluates Face Change through trace-driven and Smartphone-based experiments. Concludes this paper with future work. focus on a mobile opportunistic social

network with human-carried mobile devices. 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. We assume a 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, affiliations, 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 a fixed 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.
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. Each node has a unique real ID in the network, denoted by NIDi. The real ID of each node is assigned by the TA with a signature generated by the TA's private key, through which nodes can verify the authenticity of received real IDs. DTN incentive schemes can be adopted encourage nodes to be cooperative. We assume that nodes are cooperative in FaceChange in this project, i.e., would follow the proposed FaceChange protocol in the network.

Purpose
This purpose is creating/changing the temporary nodes for the real nodes while transmission of the data to encrypt the data before sending the data to network. so, that it is providing the security for more efficient.

Scope
The Scope is designed to ensure the confidentiality and uniqueness of encountering evidences.

Existing Work
In current MOSN applications, nodes can collect real ID based encountering information easily since neighbour 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 neighbour node anonymity.
- The work in existing supports neighbour node anonymity but fails to provide encountering information collection at the same time.

DISADVANTAGES

- Neighbor nodes communicate with real IDs directly.
- A malicious node can easily identify and attack by the attacker from neighbor nodes.
- Without protection attacker can easily get the information from malicious nodes.

Proposed Work
We proposed identifying anonymity neighbor node in MOSN is a novel design that supports both neighbor node anonymity real ID based encountering information collection in MOSNs. 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.

ADVANTAGES

1. Anonymity node cannot achieve.
2. To creates the temporary node for the real node .
3. prevent the nodes from hackers, It is more efficient.
4. you will provide the security for the data.

IV. RESULTS AND DISCUSSION

Home page

Screen 1: Home page

Description: To display the home page

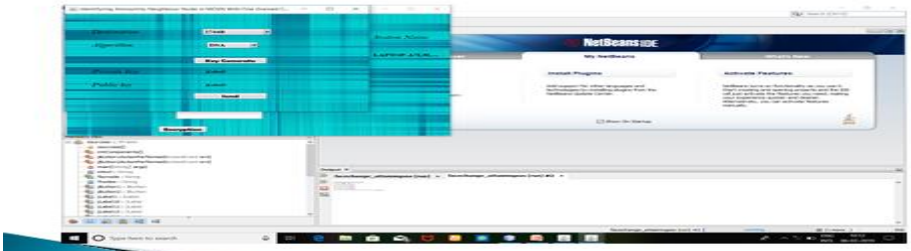
Create node

Screen .2: Create Node
Description: To create the nodes

Choose file

Screen 3: Choose file
Description: Choose the files

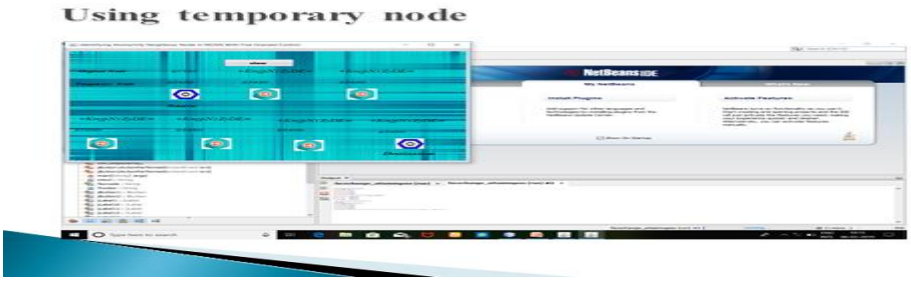
Using algorithm



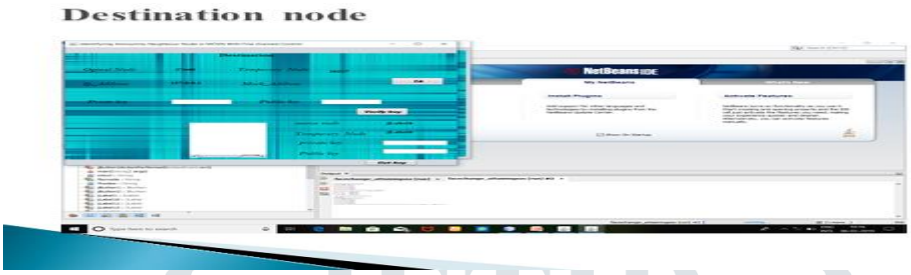
Screen 4: Using Algorithm
Description: Using RSA Algorithm and encrypt the data

Key generation

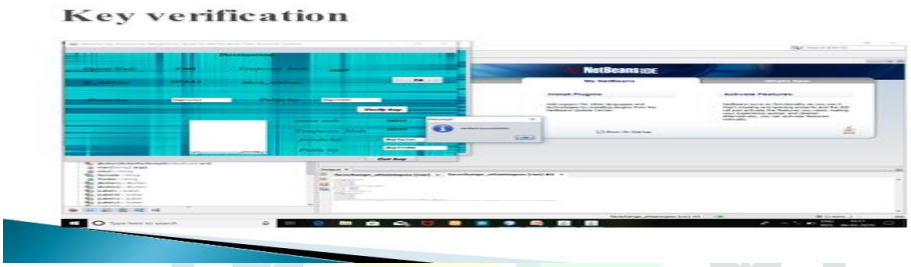
Screen .5: Key generation
Description: To generate public and private keys, before sending the files



Screen 6: Using temporary node
Description: View the original nodes and temporary nodes and choose destination

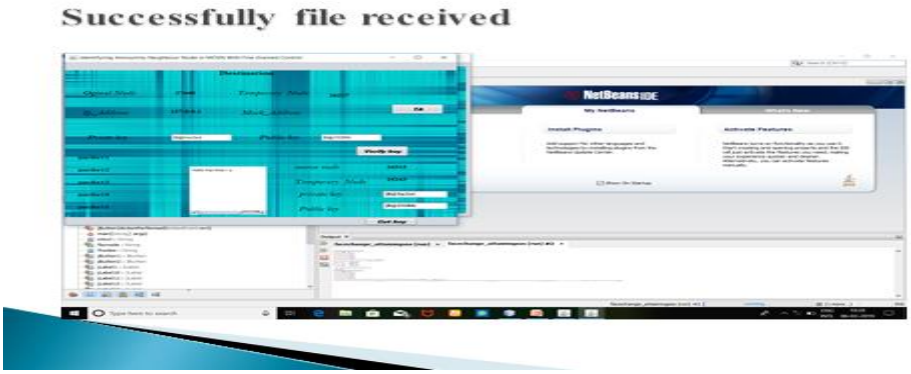


Screen 7: Destination node
Description: Receive keys and enter private and public keys



Screen 8: Key verification
Description: verify the private and public key, decrypt the data

Screen 9: File Receiving
Description: File verification successfully



Screen 10: File successfully received
Description: File is successfully received

Conclusions

System that supports both neighbor anonymity and real ID based encountering information collection in MOSNs. To ensure the security and efficiency of the encountering evidence collection of trusted based control over, what information can be included in the encountering evidence in supported for identifying anonymity neighbor node in MOSN with fine-grained control. Trust based control over what information can be included in the encountering evidence is supported in Identifying anonymity neighbor node in MOSN. 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 Identifying anonymity neighbor node in protecting node privacy and supporting the 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 Identifying anonymity neighbor node in MOSN seamlessly.

.

References

[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 disruption tolerant 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 interest casting in opportunistic networks," in *Proc. IEEE WCNC*, Apr. 2012, pp. 2829–2834.