iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3622

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Reform ID-Achieving Proximate Node Anonymity in MOSNs

S. Siddharth Gupta[1], G. Guru Ramkoushik[2], P. Joseph Sylvan[3], S. Avinash[4]
[1, 2, 3] *B. Tech, CSE, TKREC, Hyderabad*
[4] *M. Tech, CSE, Assistant professor TKREC, Hyderabad*

Abstract: ***Mobile Opportunistic Social Networks(MOSNs) are the networks where the mobile devices interact or communicate with each other when they encounter each other for carrying out MOSN services such as file sharing in a proximate environment i.e., for communication when the devices(nodes) encounter in proximity. At present such services are provided but they come at cost of zero privacy because in already present methods when nodes encounter communication is done only when their Real Identities (RID) are shared which leads to privacy and security concerns. Anonymizing RIDs of proximate nodes(devices) solves such concerns. But for MOSN services to work, requires sharing of RIDs. Hereby we propose Reform ID which supports both anonymizing RIDs among proximate nodes and also collects RIDs based on encountering information (En-In). For node anonymity, two confronting nodes communicate anonymously. After the nodes terminate the anonymous communication, encountering evidence(EV) is then encrypted and forwarded by them for collection of En-In.***
Keywords: MOSN, Encountering information (En-In), Encountering evidence(EV), Real Identities(RID), proximity, anonymity, nodes

I. INTRODUCTION

MOSNs (Mobile Opportunistic Social Networks [1][2] are a special type of Delay Tolerant Networks(DTNs) [3] where communication between different nodes is done when the nodes are present in proximity or neighbourhood region. 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 [4], encountering based social community/relationship detection [5], [6], and distributed file sharing and Question & Answer (Q&A) [7] – [9] in a community. In each system, a node is uniquely labelled 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. In each system, a node is uniquely labelled 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. There are rich investigations on protecting node privacy in MOSNs [10] – [17]. 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 neighbour nodes when they are within the communication range of each other. However, when using real IDs directly, the disclosure of node ID to neighbour nodes would create privacy and security concerns.

II. RELATED WORK

A. Privacy Protection in MOSN

Anonymizing node interests or attributes for privacy protection in MOSNs has been studied [10] – [13] and [14] – [17]. which uses the solution for "the millionaire's problem" to blindly check whether two nodes have similar interests. PreFiler [11] adopts attribute-based encryption and/or bilinear pairing [18] to blindly check whether a packet matches the destination's interests and whether a node owns the attributes to hold a packet, respectively. In STAP [13], packets for a node are cached in places where it visits frequently. As a result, nodes can fetch packets for them without disclosing their location information. SLPD [19] hides the location of a node from the server by relaying its location-based requests among its social friends. ALAR [20] encrypts different fragments of a message with different keys and forwards them separately to prevent advisories from deducing its location from captured fragments. In STAMP [21], nodes generate location proofs for co-location nodes anonymously to protect their location privacy. . FindU [14] leverages secure multi- party communication to enable a user to find the best match user with limited information exchange. Liang et al. [16] further propose a serial of profile matching algorithms with full anonymity. The work in [17] lets each node continually change its pseudonym to protect its privacy in MOSNs.

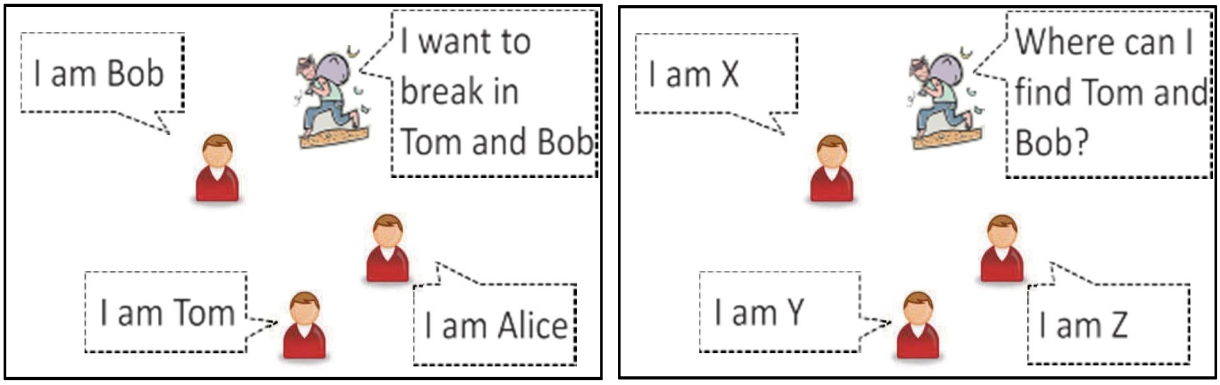
B. Social Network Based Applications in MOSNs

There are already many social network based MOSN routing algorithms [4], [22] – [25]. 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. In SMART [7], each node constructs a social map including frequently met nodes to guide packet routing. In realize peer-to-peer (P2P) file sharing and publish/subscribe overlay in DTNs, respectively. In PeopleNet [8], questions are first forwarded to matched geographical community and then propagated within the com- munity via P2P connectivity to seek for answers. Neighbour 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 neighbour node anonymity for privacy protection.

III. PROBLEM STATEMENT

In current MOSN applications, nodes can collect real ID based encountering information easily since neighbour nodes communicate with real IDs directly. Most of the existing system works focus on anonymizing interests and profiles and are not designed for neighbour node anonymity, which is a feature provided in this paper. The work in existing supports neighbour node anonymity but fails to provide encountering information collection at the same time

When real IDs used directly, the disclosure of node ID to neighbour nodes would create privacy and security concerns. A malicious node can easily identify attack targets from neighbours 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.



(i) Possible privacy issue (ii) Solution: Neighbour Anonymity

Fig.1 Demonstration of a privacy issue and a possible solution in MOSNs

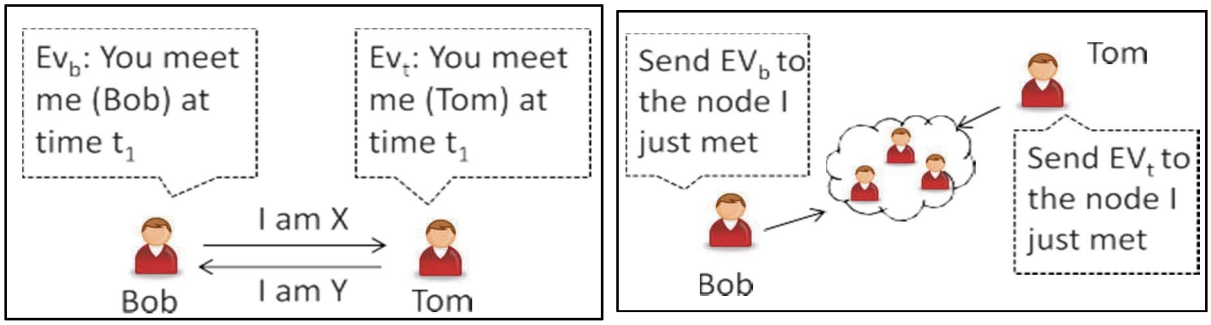
As shown in Figure 1(i), when neighbour nodes communicate with real IDs, a malicious node can easily identify attack targets from neighbours and launch attacks to degrade the system performance or steal important documents. Further, without protection, malicious nodes can also easily sense the encountering between nodes for attacks. Thus, an intuitive method to realize the neighbour node anonymity is to let each node continuously change its pseudonym used in the communication with neighbours, as shown in Figure 1(ii).

IV. PROPOSED SYSTEM

We propose Reform ID 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 ReformID keeps node anonymity only during the encountering and postpone the real ID based encountering information collection to a moment after two neighbour nodes disconnect with each other. The major contribution of this paper is to propose a novel design that supports both neighbour node anonymity and real ID based encountering information collection in MOSNs. ReformID prevents two encountering nodes from disclosing the real IDs during the encountering, so malicious nodes cannot identify targets from

neighbours 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. 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 Face Change. This shows that MOSN services can be supported when ReformID is adopted. In summary, the major contribution of this paper is to propose a novel design that supports both neighbour node anonymity and real ID based encountering information col- lection in MOSNs. ReformID prevents two encountering nodes from disclosing the real IDs during the encountering, so malicious nodes cannot identify targets from neighbours 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.

V. SYSTEM ARCHITECTURE



(i) Create the encountering evidence under neighbour node anonymity

(ii) Route the encountering evidence to the other node after separation

Fig.2 General solution for encountering record collection

Figure-2 illustrates the design of ReformID. Here in Figure-2(i) when two nodes meet, they communicate anonymously and each of them creates an encountering evidence(EV) that contains their RIDs. 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 example consider 2 users Bob & Tom, they both meet anonymously and generate an EV which they agree on. Now after the two users disconnect they send their encountering evidence to Trust Authority which calculates the trust level between the 2 EVs sent by Tom & Bob respectively. If both the EVs sent to TA are same then the users can exchange the data or any information between them in the form of packets

VI. ALGORITHM

We made use of two security algorithms namely DSA & DH (Diffie Hellmann Key Exchange) algorithms.

A. DSA Algorithm

DSA algorithm is used for generation of public and private keys. Key in DSA algorithm is generated in 2 phases. he first phase is a choice of algorithm parameters which may be shared between different users of the system, while the second phase computes public and private keys for a single user.

VI. DIFFIE HELLMANN KEY EXCHANGE ALGORITHM

The keys generated using the DSA algorithm must be transmitted between the two users in a secure channel. Diffie Hellmann key exchange algorithm here is used to transmit the keys between the sender and the receiver

VI. MODULES

A. Preventing Nodes

ReformID 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 receive.

B. 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, neighbour 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.

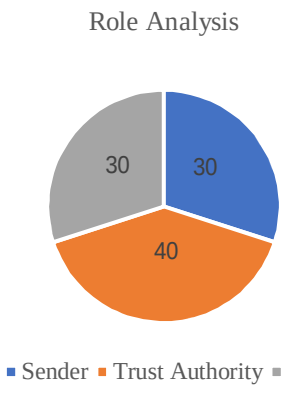
C. Trust Authority (TA)

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. 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 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.

D. 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 ReformID, neighbour 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.

VIII. RESULT ANALYSIS



Role analysis gives the information about the role of different users present in a system. Here the sender and receiver both have the same level of preference. Trust authority has got a bit of higher role than sender and receiver

IX. CONCLUSION

In ReformID, each node continually changes its pseudonyms and parameters when communicating with neighbours 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 ReformID. 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 ReformID 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 ReformID seamlessly.

X. FUTURE ENHANCEMENTS

Further two extensions can be used to enhance ReformID's practicality. The first extension, White List being motivated by our daily experiences, designs a scheme to support the function of "white list" on top of ReformID. It allows mutual-trusted nodes to collect the encountering information during the encountering directly. The second one, *Advanced Encountering Evidence Relaying* enhances the efficiency of the encountering evidence relaying by letting the recipient node specify more information about how to reach it.

A. White List

The design of ReformID introduced in Section IV realizes strong anonymity among neighbours at the cost of indirect encountering information collection. However, in reality, we commonly see that a person has a few trusted peers and is willing to share his/her real identity with them during the encountering. Therefore, we further propose an advanced scheme to allow such a feature among mobile devices in ReformID, which is named "white list" in this paper. Since neighbour anonymity still needs to be maintained, we need to realize two functions to enable the "white list" feature. First, we need to enable anonymous trusted node identification, i.e., nodes can discover trusted nodes anonymously. Second, we need to ensure that two mutually-trusted nodes can share their real identifies secretly under eavesdropping.

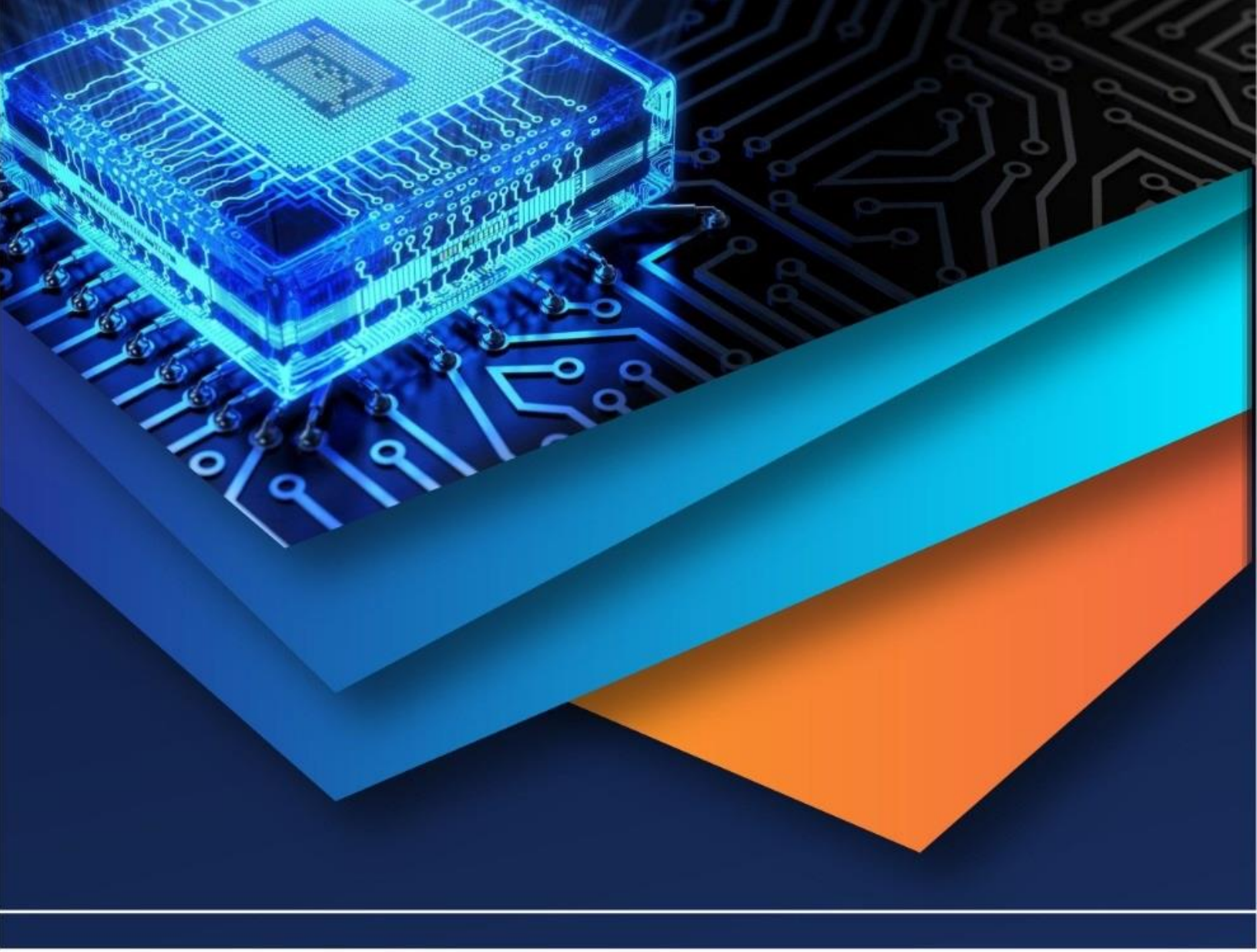
B. Advanced Encountering Evidence Relaying

Specifically, when a recipient node sends the information of the relay node to the creator of the encountering evidence, it attaches the community ID of the relay node and its own community ID that has been encrypted with the public key of the relay node. Consequently, the encountering evidence creator can use the community ID of the relay node to conduct community based routing to forward the encountering evidence to the relay node. After receiving the encountering evidence, the relay node can decrypt the community ID of the recipient node and use such information to forward the encountering evidence to the recipient node more efficiently. In this process, each node only discloses its encrypted com- munity ID to neighbouring nodes, which can only be decrypted by the selected relay node. As a result, the node anonymity is not broken in this advanced extension.

REFERENCES

[1] 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.
[2] 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.
[3] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," in Proc. SIGCOMM, 2004, pp. 145–158.
[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 commu- nity detection in delay tolerant networks," in Proc. MobiArch, 2007, Art. no. 7,
[6] F. Li and J. Wu, "MOPS: Providing content-based service in disruption- tolerant networks," in Proc. IEEE ICDCS, Jun. 2009, pp. 526–533.
[7] M. Motani, V. Srinivasan, and P. S. Nuggehalli, "PeopleNet: Engi- neering a wireless virtual social network," in Proc. MOBICOM, 2005, pp. 243–257.
[8] G. Costantino, F. Martinelli, and P. Santi, "Privacy-preserving interest- casting in opportunistic networks," in Proc. IEEE WCNC, Apr. 2012, pp. 2829–2834.
[9] R. Lu et al., "Prefilter: An efficient privacy-preserving relay filter- ing scheme for delay tolerant networks," in Proc. IEEE INFOCOM, Mar. 2012, pp. 1395–1403.
[10] L. Guo, C. Zhang, H. Yue, and Y. Fang, "A privacy-preserving social- assisted mobile content dissemination scheme in DTNs," in Proc. IEEE INFOCOM, Apr.

2013, pp. 2301–2309.
[11] 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.
[12] 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.
[13] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in Proc. IEEE INFO- COM, Mar. 2012, pp. 1969–1977.
[14] 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.
[15] 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.
[16] S. Zakhary and M. Radenkovic, "Utilizing social links for location privacy in opportunistic delay-tolerant networks," in Proc. IEEE ICC, Jan. 2012, pp. 1059–1063.
[17] X S. Zakhary and M. Radenkovic, "Utilizing social links for location privacy in opportunistic delay-tolerant networks," in Proc. IEEE ICC, Jan. 2012, pp. 1059–1063.
[18] X. Lu, P. Hui, D. Towsley, J. Pu, and X. Zhang, "Anti-localization anonymous routing for Delay Tolerant network," Comput. Netw., vol. 54, no. 11, pp. 1899–1910, 2010.
[19] X. Wang et al., "Stamp: Ad hoc spatial-temporal provenance assurance for mobile users," in Proc. IEEE ICNP, Oct. 2013, pp. 1–10.
[20] E. M. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant manets," in Proc. MobiHoc, 2007, pp. 32–40.
[21] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: Social-based forwarding in delay tolerant networks," in Proc. MobiHoc, 2008, pp. 241–250.
[22] W. Gao and G. Cao, "On exploiting transient contact patterns for data forwarding in delay tolerant networks," in Proc. IEEE ICNP, Oct. 2010, pp. 193–202.
[23] X. Zhang and G. Cao, "Transient community detection and its appli- cation to data forwarding in delay tolerant networks," in Proc. IEEE ICNP, Oct. 2013, pp. 1–10.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY