IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-6, Issue-3 E-ISSN: 2347-2693

Fine-Grained Control for Neighbour Node Anonymity in Opportunistic Mobile Networks

A.S. Jaiswal[1*], R. Welekar[2]

[1,2]Dept. of Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

[*]*Corresponding Author: aparna.jaiswal90@gmail.com*

Available online at: www.ijcseonline.org

Received: 18/Feb//2018, Revised: 24/Feb2018, Accepted: 16/Mar/2018, Published: 30/Mar/2018

***Abstract*—** The major objective of any communication system is to have the messages dispatched to their corresponding terminal. The network topology of DTNs/OMNs is not only highly dynamic, but also exhibits high degree of network partitioning. The maneuverability of the node in delay tolerant network considerably harms the productivity of data forwarding. The proposed approach selects the path according to the feasible number of hops needed to reach the corresponding node. The architecture anonymizes each and every node of the network by giving them fake ids. When a node wants to send its confidential data to the other node then the sender node and receiver node only knows each other's real id. Here the data is send in the encrypted form which can be decrypted using a key.

***Keywords*—** Disruption tolerant network, multicast, privacy, security, unicast.

I. Introduction

A special form of delay tolerant networks (DTNs). When neighbor nodes communicate with real IDs, a malicious node can easily identify attack targets from neighbors and launch attacks to decrease the system performance with loosing important documents. Later, without privacy protection, malicious nodes can also easily sense the encountering between nodes for attacks. To generalize the process of useful applications in opportunistic social networks to Face Change logically.

Now a day a digitalization plays important role in networking and security. Usually we have to provide privacy and confidential data. Therefore in general we have to kept data to be confidential so there might be no any privacy issue, owner of date have compulsory to kept data safe, confidential and compulsory. When sharing sensitive data Privacy-Preserving Sharing of Sensitive Information (PPSSI), and providing secure instantiation with effective approach where nodes reveling minimum confidential information. The PPSSI model we use as an application with simple database querying application with two parts: First, server that has a database and Second, a client performing disjunctive queries. In case of PAYTM safety example the PAYTM (server) has a database with user information and summary of their orders with PAYTM wallet that linked with user account and amount balance, where client poses queries correspond to data and we analyze using PPSSI where our main block is Private Set Intersection (PSI) techniques.

The problem of privacy is based on the capacity of single person or group to secure the information and handle it carefully. In some cases the rules and regulation are made to preserve privacy issues as per the individual right. The individual information may result in access for only that individual user only, hence generating matters while there may be misuse by private companies, governments and other individuals. In last some years, advances in computer science and information technologies have maximize the privacy issues. Now a days data is daily updated, collected and electronically exchanged my many other users. Privacy issues may not occurs more due to anonymity and other digital activities. The loss in personal information may increase number of legally, financially and emotionally, privacy issues. The paper is structured as follows; we introduce the literature review in section II, then we have described how we will do the implementation and proposed work which includes the algorithms we will be using in our proposed system in section III, then conclusion in section IV and then we summarize our contributions in section V.

II. Related Work

A. Privacy Protection in mobile online social networks:

In this work done method work done, by considering the user privacy where the current location is share only with the user who are in his/her friend list, only they can know his location for that in this system we introduce a new cryptography originally called the functional pseudonym (nickname) scheme based on Lagrange polynomial with the public social network IDs of the selected friends [10]. The work in uses the solution for "the millionaire's problem" to blindly check if two nodes have similar interests [12].

B. Replication vs. Forwarding:

Disruption tolerant network (DTN) refers to the type of sparse mobile ad hoc network where the nodes are connected periodically .Epidemic routing protocols replicate packets at shared opportunities hoping to find out destination. However, naive flooding wastes resources and can critically decrease the performance. Recommended rules of conduct try to restrict replication or alternatively clear useless packets in various ways: (i) using network coding [5] and coding with redundancy [18]; (ii) removing useless packets using acknowledgments of delivered data [6]; (iii) using probabilistic mobility information to infer delivery [13] (iv) replicating packets with a small probability [6]; (v) using historic information [12, 7, 6]; and (vi) bounding the number of replicas of a packet [19].

C. Social Network Analysis (SNA):

Although hub in Social Network Analysis (SNA) generally represents node that promoting the communication between other nodes [11], we elaborate the hubs concept to represent the capacity of a node to forward data of its interest. Our detailed contributions are as follows: (i) We propose a general framework for user generated data in DTNs. (ii) We provide theoretical insight on the cost-factor of data publishing.

D. Key Concepts:

Due to node density and unnecessarily occurrence node mobility, end-to-end connections are difficult to maintain in such networks. Alternatively, exploitation of node mobility gives permission to nodes to physically carry data hand over and forward data. The main problem in data forwarding is selection of the nodes to broadcast. Social network analysis (SNA) has been exploited for data forwarding in DTNs [10]. There are two key concepts in SNA: First is Community, which is naturally generated according to social relation among people; social community is the natural outcome from the "small-world" aspect, which is formalized as a random graph problem in [19]. Second is Centrality, which shows that nodes in a community are the common as per other nodes and act as communication hubs. Since relations among mobile users are likely to have long-term characteristics neighbor and are less volatile than node mobility, social-based forwarding schemes [10], [20] outperform traditional schemes that are based on blind interest or mobility-based prediction [16]. Many data forwarding techniques focus on forwarding data to only destination. Multicast, on the other hand is more preferable to send data to multiple users for data publication and multiuser communication. For example, in sparse vehicular ad-hoc networks, people may publicize live information of crowd to other following peoples. However, effectively multicast is challenging in DTNs. Even though there is previously work dine on multicasting in DTNs, they are restricted to semantic multicast models [13] and multicast capacity analysis [14]. Some others introduced community for multicast [7], but may not provide any strategy for selecting paths from a social network point.

E. Cumulative Probabilities:

In this we propose approach to social aware broadcast in DTNs. We accomplish social network concepts, centrality and community to improve the cost-factor of broadcast. More especially, our point of broadcasting data at the other destinations with the forwarding data and time constraint while minimize the data forwarding cost measured by the number of carry used. From this probabilistic perspective, the essential difference between broadcast and unicast in DTNs is that the selection of carry for multicast is based on the carry cumulative probabilities of forwarding data to multiple destinations. We first consider broadcasting as a single data item in the network, and then generalize the problem to multiple data items with the constraint of limited carry buffer. First, we propose effective relay selection strategies for both single-data and broadcast-data multicast problems based on social network concepts. In particular, we provide community based solutions for maintaining global network knowledge at separate mobile nodes. Such knowledge is not sufficient for calculating the cumulative data forwarding to multiple resources. Second, we develop model for broadcast carry selection, and furthermore derive theoretical performance bounds of our broadcasting system. These theoretical results show that the proposed strategies are having better nodes as carry and are able to ensure that the performance factor for multicasting can be used in various networks.

III. LIMITATIONS

The main issue while sending data there may be a selection of proper nodes in the network. Social network analysis (SNA) is mostly used for data sending in DTNs. There is need to preserve the privacy while sharing information obtained in the form of many other and in our daily life cycle, ranging from national security to social networking. It has two parts: First is collecting information, second revealing the interest and sharing the requested information. This may give chance to generate challenges: how to give access to such parties that authorize other parties to share information, how efficiently this can be done in real-world practical problem. This gives the idea of Privacy-Preserving Sharing of Sensitive Information, and generates a visible and correct instantiation, generated in the form of simple database querying. Proposed system functions as privacy to safe parties from revealing the respective impressionable information. To discover the method of changing applications in mobile online social networks, the concept of user-oriented data to plays the roles and contact of user interests in DTNs. The multicast with single and many data files, developed models for multicast hub selection, and generated the sensitive difference between multicast and unicast in DTNs.

IV. Proposed Work

1. Key Generation: The key generation provides generate secret guideline. The key authorities consist of a hub authority. There are secure communication channels between a hub authority and each local authority during the start key system and generation time.
2. Storage node: This is a server that stores data send from senders and give access to other users. It may be dynamic or static. Same as the previous design, we assume the storage node to be semi- trusted, which is authentic but interested.
3. Data Sender: This has an ability of sender to send confidential data and to store them into the other data storage node for easy sharing or for reliable delivery to users in the intense networking environments.
4. User: This is a mobile node who gives access to data stored at the storage node. If a user provides a set of attributes gratifying the access policy of the encrypted data defined by the sender, and is not lift in any of the attributes, then he will be able to decrypt the data.

Here, we form a network. Each node is connected to neighbouring node and it is independently deployed in network. In this we browse and select the source file. And selected data from that file is converted into fixed size of packets. And the packet is send from source to detector. The detection is defined as a mechanism for a PACKET IN NETWORK to detect the occurrences of anomalous moving attackers. In this module we also provide path and check whether the path given is authorized or not. If path is authorized the packet is send, otherwise the packet will not be send.

According to port number only we are going to find the path is authorized or not. If the packet is received from other port it will be filtered and discarded. This filter removes the unauthorized packets and authorized packet is send. Data Encryption Algorithm is an encryption algorithm. It uses a block cipher with a 128-bit key, and is very secure. It is considered from the best publicly known algorithms.

V. Conclusion

In this paper, we propose Fine-Grained Control for Neighbour Node Anonymity in Opportunistic Mobile Networks, which enables every node to send their confidential information to other nodes without revealing their real ids to the intermediate nodes. Here only the sender node knows the real id of the receiver node to which the data is to be sent and also only the receiver node knows the real id of the owner of the data. The system finally authorizes the sender node and the receiver node to communicate with each other without the leakage of their confidential information. Privacy assurance are correctly defined and accomplished with inferable security.

References

[1] Kang Chen, Member and Haiying Shen, "Face Change: Attaining Neighbor Node Anonymity in Mobile Opportunistic Social Networks With Fine-Grained Control" in *IEEE/ACM Transactions on Networking(TON), vol. 25 issue 2, April 2017*

[2] K. Chen and H. Shen, "Fine-grained encountering information collection under neighbor anonymity in mobile opportunistic social networks," in *Proc. IEEE ICNP, Nov. 2015, pp. 179–188.*

[3] W. Gao and Q. Li, "Wakeup scheduling for energy-efficient communication in opportunistic mobile networks," in *Proc. IEEE INFOCOM, Apr. 2013, pp. 2058–2066.*

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

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

[6] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on opportunistic forwarding algorithms" *IEEE Trans. Mobile Comput., vol. 6, no. 6, pp. 606–620, Jun. 2007.*

[7] M. C. Chuah, "Social network aided multicast delivery scheme for human contact-based networks," in *Proc.1st Simplex, vol.1, issue 3, Feb. 2009.*

[8] V. Conan, J. Leguay, and T. Friedma n, "Characterizing pairwise inter-contact patterns in delay tolerant networks," in *Proc. 1st Int. Conf. Autonomic Comput. Commun. Syst., Article no. 19, Oct. 2007.*

[9] P. Costa, C. Mascolo, M. Musolesi, and G. Picco, "Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks" in *IEEE J. Sel. Areas Commun., vol. 26, no. 5, pp. 748–760, Jun.2008.*

[10] Junggab Son, Donghyun Kim, Rahman Tashakkori, Alade O, Tokuta, Heekuck Oh, "A New Mobile Online Social Network Based Location Sharing with Enhanced Privacy Protection" in *IEEE Computer Communication and Networks (ICCCN), 25th International Conference, Aug. 2016.*

[11] N. Eagle and A. Pentland, "Reality mining: Sensing complex social systems," in *Pers. Ubiquitous Comput., vol. 10, no. 4, pp. 255–268, 2006.*

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

[13] V. Erramilli, A. Chaintreau, M. Crovella, and C. Diot, "Delegation for-warding," in *Proc. ACM MobiHoc, 2008, pp. 251–260.*

[14] K. Fall, “Delay tolerant network architecture for challenged internets,” in *Proc. ACM SIGCOMM, 2003, pp. 27–34.*

[15] L. Freeman, “A set of measures of centrality based on betweenness, Sociometry”, in *IEEE vol. 40, no. 1, pp. 35–41, 1977.*

[16] W. Gao and G. Cao, “Fine-grained mobility characterization: Steady and transient state behaviors,” in *Proc. ACM MobiHoc, 2010, pp.61–70.*

[17] W. Gao and G. Cao, “On exploiting transient contact patterns for data forwarding in delay tolerant networks,” in *Proc. IEEE ICNP, 2010, pp.193–202.*

[18] W. Gao and G. Cao, “User-centric data dissemination in disruption tolerant networks,” in *Proc. IEEE INFOCOM, 2011, pp. 3119–3127.*

[19] W. Hsu and A. Helmy, “On nodal encounter patterns in wireless LAN races” in *IEEE Trans. Mobile Comput., vol. 9, no. 11, pp. 1563–1577, Nov. 2010.*

[20] W. Gao, Q. Li, B. Zhao, and G. Cao, “Multicasting in delay tolerant networks: A social network perspective,” in *Proc. ACM MobiHoc, 2009, pp. 299–308.*

[21] P. Hui, J. Crowcroft, and E. Yoneki, “Bubble rap: Social-based for-warding in delay tolerant networks,” in *Proc. ACM MobiHoc, 2008, pp. 241–250.*

Authors Profile

Miss. Aparna S. Jaiswal has done Bachelor of Engineering in Information Technology from Rashtrasant Tukadoji Maharaj Nagpur University, India in 2014 and currently pursuing Mater of Technology in Department of Computer Science and Engineering from Shri Ramdeobaba College of Engineering and Management, Nagpur, India. Her research work focuses on Networking, Data Security and Data Mining. She is a member of Computer Society of India since 2014.

Mrs. Rashmi R. Welekar pursed Bachelor of Computer Science and Engineering from Amravati University, India in year 1999 and Master of Technology from Nagpur University, India in year 2007. She is currently working as Assistant Professor in Department of Computer Science and Engineering, Shri Ramdeobaba College of Engineering, Nagpur, India since 2006. She has published more than 25 research papers in reputed international journals and conferences. Her main research work focuses on Computer Networks, Object Oriented Programming, Operating systems, Data Mining and Network Security. She has total 12.9 years of Teaching Experience.