Data Dissemination in Mobile Social Networks with Meshwork Coding

M.Swathy[#1], *M.Tech, Computer Science Engineering, d mediswathy532@gmail.com*

Md Fareeduddin[#2], *Associate Professor, Department of CSE, mfareed_kzmn@yahoo.co.in*
 # TallaPadmavathi Engineering College, Warangal, Telangana, India

Abstract: ***With the huge popularization of personal hand-held mobile devices, more people use them to establish network connectivity and to query and share data among themselves in the absence of network infrastructure, creating mobile social networks (MSNet). Currently, data route/forward approaches for such intermittently connected networks are commonly "store-carry-and-forward" schemes, which exploit the physical user movements to carry data around the network. Considering the traditional geo-centrality information, they provide different route algorithms to cater to the super user that wants to either minimize total duration or maximize dissemination ratio. We are providing of meshwork coding for information dissemination over a wireless network, it allows for a simple, distributed and robust algorithm where nodes do not need any information from their neighbors. In this paper, we analyze the time needed to diffuse information throughout a network when network coding is implemented at all nodes. We then provide an upper bound for the dissemination time for ad-hoc networks with general topology. Moreover, we derive a relation between dissemination time and the size of the wireless network. It is shown that for a wireless network with N nodes, the dissemination latency is between O(N) and O(N^2), depending on the reception probabilities of the nodes. These observations are validated by the simulation results.***

Index Terms—Mobile social networks (MSNs), Mesh networks, Ad-Hoc networks.

1. INTRODUCTION

THE INCREASE in the number of mobile devices has enabled users to be ubiquitously connected through wire- less and mobile communications technologies. However, unlike conventional mobile ad hoc networks, persistent connectivity is not a necessity in every type of network. This has led to a totally progressive kind of social network called mobile social networks (MSNs). MSNs can be viewed as modern kinds of delay-tolerant networks (DTNs) in which mobile users interact with each other to share user-centric data objects among interested observers.

The information dissemination problem, at its root, is a classical broadcast problem: sharing data residing at one node (source) with all others (destinations) in the network. Of late, a more modern version of the one-to-many (broadcast) problem has gained prominence; this is typically referred to as *data sharing* among multiple peer-to-peer (p2p) nodes, or the *all-to-all* problem. This problem arises when each node in a network obtains only *a fraction of the total information* (e.g., part of a video-on-demand file or a software update) desired collectively by all. In a simplified version of the all-to-all data-dissemination problem, a source file desired by all is divided into N mutually exclusive *information packets*, and each packet is stored at exactly one node in the network. Every node's objective is to acquire the remaining N − 1 pieces of the source file; the order in which each node receive s the remaining information packets is not relevant.

There is a plausible argument as to why meshwork coding provides substantial benefits for data dissemination. In the beginning, each node has only a small fraction of the full file and seeks to gather the remaining pieces. With time, a node gathers some of the other pieces, but does not have any information regarding which pieces the neighboring nodes may possess. At any instant, the profile of packets at any two node s in the network will include common and remaining non-overlapping subsets. Intuitively, this suggests that, if each node encodes all the data it presently contains via network coding and broadcasts it, recipient nodes will have acquired coded versions containing information about the missing pieces. After a sufficient number of such encoded packet transmissions from other nodes, each node will be able to decode the full file. Thereby, by using meshwork coding, nodes do *not* need extra information from other nodes concerning the state of the network.

In this paper, we focus only on dissemination latency and do *not* consider the latency caused by encoding/decoding of NC, which has been studied separately in the literature. In fact, authors in explore the design of a sparse network coding matrix that significantly decreases encoding/decoding time. Clearly, the net latency of data dissemination is the sum of our result and the encoding/decoding time.

2. SYSTEM MODEL

As usual, a network graph is denoted as G(V, E), with $|V| = N$ nodes and links $E \in V \times V$. We assume that the network is slotted (i.e., all nodes are synchronized) for simplicity and that all transmissions occur synchronously with a common clock. Further, without loss of generality, we assume that during each time slot, a node $u \in V$ can broadcast exactly one packet. When node v broadcasts, node $u \in V$ receives the signal correctly with probability P_{vu}.

Clearly, in all broadcast wireless networks, the role of the multiple access or MAC protocol is fundamental to managing interference [13]. We consider an interference-free (orthogonal) access that allows only one node to transmit at a time. This includes, among others, a single-cell 802.11-type infrastructure network based on CSMA/CA if all nodes lie within the (common) carrier sensing range. The probability of a node capturing the common channel at any time is assumed to be uniform among all nodes.

3. DATA DISSEMINATION USING MESHWORK CODING

Assume that each node u initially has a single *information packet* X_u to be shared with every other node in the network. Hence, the set of unique (information) packets in the network, initially and at all subsequent times, is given by $\{X_1 . . . X_N\}$ for a network with N nodes. Each information packet is a vector of r symbols, where each symbol is an element of a finite field F_2^Q , i.e., X_u for each node $u \in V$. For convenience, assume that q divides the length of packets transmitted (otherwise, zero padding is applied). Moreover, all packets are linearly independent vectors in F_2^Q [12], reflecting the fact that nodes have different information to share. The results and derivations presented in this paper can be extended to a case when some nodes have more than one message and some have none or when all the messages are there with one particular node to start with.

With time, each node receives a sequence of linear combinations of information packets at the other nodes. Hence, after a sequence of

broadcasts, node u possesses a set of coded messages, $S_u(t)$ at time (slot) t.

$$S_u(t) = \{M_1, M_2, ..., M_{|S_U(t)|}\}, \quad (1)$$

Each message M_i is a linear combination of the underlying *information packets*, initially possessed by the nodes and can be represented as

$$\mathbf{m}_i = \sum_{k=1}^{N} \alpha_{i,k}\mathbf{x}_k = \boldsymbol{\alpha}_i^T \mathbf{X}, \quad i = 1, 2, ..., |S_u(t)|, \quad (2)$$

Clearly, $S_u(t)$ (set of messages at node u at time t) spans a subspace in $F^r_{2^Q}$, as observed by rewriting Eq. (2) in the following form:

$$\mathbf{M}_u(t) = \mathbf{A}_u(t)\,\mathbf{X}, \quad (3)$$

where A_u is the coefficient matrix consisting of NC coef-ficients and X contains the N information packets in the network, given by

$$\mathbf{X} = [\mathbf{x}_1\ \mathbf{x}_2 \dots \mathbf{x}_N]^T, \mathbf{M}_u(t) = [\mathbf{m}_1\ \mathbf{m}_2 \dots \mathbf{m}_{|S_u(t)|}]^T$$

$$\mathbf{A}_u(t) = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \dots & \alpha_{1,N} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{|S_u(t)|,1} & \alpha_{|S_u(t)|,2} & \dots & \alpha_{|S_u(t)|,N} \end{bmatrix}$$

4. STOPPING TIME

The data dissemination algorithm terminates when *all* nodes are able to decode the broadcast messages to recover the underlying N set of information packets, which happens when Eq. (3) for all u ∈ V has a unique solution, i.e., when the coefficient matrix at each node has full rank N.

Matrix A_u has rank N if and only if $S_u(t)$, the subspace scanned by messages in u at time t, has dimension N .

Privacy is the last aspect of safety in MSNs that has recently gained unprecedented attention. This is particularly because of the social aspect of MSNs in which information relevance like users' location and identity is considered critical issues for both the attackers and system administrators. Many researchers have suggested ways to reveal users' information selectively and for them to remain unnoticed or unidentified over the network. To do this, privacy preferences are generally specified to obfuscate users' private information and present it in a coarser and falsified manner.

Safety can be described as the condition of being protected against different types of failure, damage, error, accidents, harm, or any other non desirable event. In early works, like, the term security was used to convey this meaning, but later, with the emergence of various networks and safety issues, security has been specified to a more technical concept. What we mean by safety in this paper is to be in control of recognized hazards and to achieve an acceptable level of trust, security, and privacy. This can take the form of protection from an event or exposure to something that causes damage.

5. PERFORMANCE EVALUATION

Trust is a critical determinant of sharing information and developing new relationships in a network. In other words, trust is based on the reputation between individuals and is a capital asset that people may invest great amount of resources in building and that is acquired slowly but can be destroyed very quickly. In traditional networks, trust relies mainly on the infrastructure, and this infrastructure is trusted by end users to fulfill the routing task and provides naming service which also simplifies the establishment of trust between users. Furthermore, when higher level of trust is required, the network infrastructure can be complemented by a safe infrastructure.

In order to establish cooperation between nodes in mobile networks through the direct and the indirect observation and created policies in which nodes compromise to obtain a service. In

other words, their method obtains direct past experience using direct observation while indirect ones are for using recommendations. A non collaborative fading parameter that decreases the reputation values of users is considered. Another strategy to make users collaborate which seems applicable for MSNs, was proposed in which users are obliged to be cooperative by handling essential and effective messages throughout the network while messages are either primary or secondary. Messages that are considered to be essential for a device itself are called primary, whereas secondary messages are useful for other users and carrying them is proof of the cooperation between the devices. By using a barter exchange, a user receives a message only if it provides the same number of messages to the other participant. Here, nodes are located in a line, with equal distance, d, between neighbors. At first, we let the transmit power remain fixed and increase the size of the network by adding more nodes. When there are only a few nodes in the network, stopping time has a linear relation with the number of nodes in the network. However, when the size of the network keeps increasing, the linear relation is not valid anymore. This is consistent with our findings in Lemmas 2 and 3. For a small number of nodes in the network, nodes are in transmission range of each other; i.e., a transmitted packet is heard by all of the nodes in the network (with nonzero probability $P_{uv} > 0$); hence, the stopping time is O(N). On the other hand, when the size of the network keeps expanding, after a while we have $P_{uv} = 0$ for some nodes in the network and that affects the trend of the dissemination delay.

In a 2-D grid topology, nodes are located on a equispaced 2-D lattice. As for the linear network, we first let the transmission power remain fixed while increasing the size of the network by adding more nodes. Figure 1 presents the simulation result and the analytical upper bound, which happens to be smaller than the transmission range of all the nodes in our simulation. In other words, for the fixed transmission power, each node can hear from all other nodes

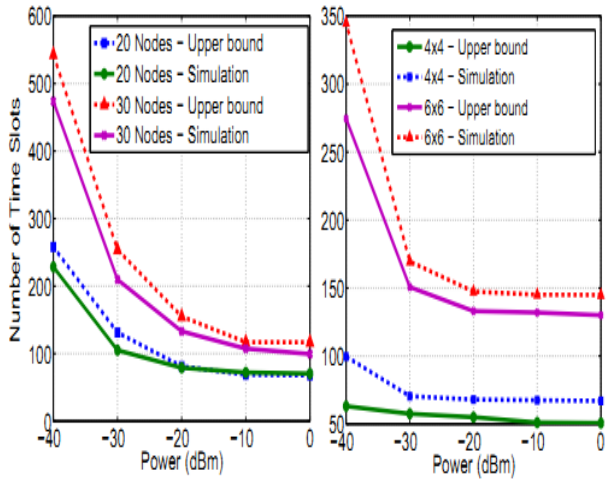

Fig. 1 Analytical upper bound and simulation results versus nodes' transmis-sion power for (left) linear network (right) grid network. $N_0 = 4 \times 10^{-14}$

It is for this reason that the stopping time has a linear trend with the size of the network. Finally, for different transmission power, analytical upper bounds and simulation results are presented in Figure 1.

5. SECURITY

Network information security is concerned with the confidentiality, integrity, and availability of data, regardless of the form that the data may take. However, the security services of other hand, MSNs are defined as specific opportunistic P2P networks which do not have an access point in between them and having little protection, these types of networks usually employ encryption methods to provide security. An attacker however may try to break the encryption of the network; hence, security policies were defined.

These policies address constraints on functions and access of external attacks, adversaries, and unauthorized users. To offer a comprehensive study on MSN security issues, we put them in three groups: 1) access control to exert control over interactive nodes; 2) confidentiality to ensure that a given message cannot be understood by anyone else other than its desired recipients; and 3) intrusion detection to monitor the network for malicious activities or policy violations. Security is a classic angle of network safety that has been massively discussed in the MSN literature. Albeit widespread research on this area, proposed schemes still need refinements or adjustment. Anonymous social-location-based architectures such as that in, which do not imply a specific implementation of any particular component, are examples of these schemes. They should be managed through a centralized infrastructure on the Internet or integrated into a P2P trust net- work. However, the way in which preferences are chosen and returned to the stationary component could be optimized for different metrics. This mechanism could be designed to provide k-anonymity for a set of users' encrypted identifier rather than just one at a time. This relates to a more general set theory problem. A set of social network information associated with asset of users should be chosen in a way that the set of preferences cannot map back to any one or any set of the users within some guarantee.

6. CONCLUSIONS

The concept of MSNs is a novel social communication paradigm that exploits opportunistic encounters between human-carried devices and social networks. Like any other emergent archetype of technology, MSNs demand time to be totally safe and immune. Having social aspects included, they encompass more complex and correlated challenging safety problems that make it difficult to suggest solutions and represent a clear classification on safety issues. This paper has aimed In a wireless network with general topology, we provide an analytical upper bound for the amount of time needed to spread information through the whole network. Our result show that by using network coding the stopping time is between O(N) and O(N ^{2}) where N is number of nodes inside the network.

7. REFERENCES

[1]. N. Vastardis and K. Yang, "Mobile social networks: Architectures, social properties and key research challenges," IEEE Commun. Surveys Tuts., vol. 15, no. 3, pp. 1355–1371, 3rd Qtr., 2013.

[2]. P. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. of 41st Allerton Conf.* Communication Control and Computing, Oct. 2010.

[3]. M. Walsh. "Gartner: mobile to outpace desktop web by 2013," Online Media Daily, January 2010.

[4]. L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," Communications Magazine, IEEE, vol. 44, no. 11, pp. 134–141, Nov. 2006.

[5] Handbook of Wireless Networks and Mobile Computing, 1st ed, John Wiley & Sons, Inc., Ivan Stojmenović, New York, USA, 2002, pp. 325-346.

[6] N. D. Lane, E. Muluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," Communications Magazine, IEEE, vol. 48, no. 9, pp. 140–150, Sept. 2010.

[7] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications

Technical Committee (MMTC) ELetter, 2011.
[8] M. Conti, and M. Kumar, "Opportunities in opportunistic computing," IEEE Computer, vol. 43, no. 1, pp. 42–50, Jan. 2010.