International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 9 Issue 1 –JULY 2014.

Secure Data Aggregation in Wireless Sensor Networks

[1*] G.R.BhargaviRani, and [2#] K.Srilakshmi

[1] *M.Tech CNIS(Affiliated to JNTU University) GNITS- Hyderabad.*

[2] *Assistant Professor CNIS(Affiliated to JNTU University) GNITS- Hyderabad*

[1]gbr.bhargavi13 @gmail.com

[2]krovvidisrilakshmi@gmail.com

Abstract— The widespread availability of miniature wireless devices such as cell phones, laptops, mobiles has become an indispensable part of our life. Delay Tolerant Networks (DTNs) exploit random contacts between mobile nodes to allow end-to-end communication between points that do not have end-to-end connectivity at any given instant Routing protocols in DTNs often have to make use of so-called knowledge oracles that provide full or partial information about past or future node encounters. In Delay Tolerant Networks (DTNs) the core challenge is to cope with lack of persistent connectivity and yet be able to deliver messages from source to destination. The memory of a DTN node is assumed to be limited to the size of single frame. When large files need to be transferred from source to destination, not all packets may be available at the source prior to the first transmission. In this work, we analyze the replication based routing policies and study their optimization under two hop routing. Piecewise-threshold policies are designed which account for linear block-codes and rateless random linear coding to efficiently generate redundancy, as well as for an energy constraint in the optimization.

Keywords: DTNs, coded packets, Work conserving policies, oppurtunistic connectivity, rateless codes.

I. INTRODUCTION

Delay Tolerant Networks (DTNs) are those network environments where the nodes are characterized by opportunistic connectivity. Routing is one of the major components which significantly affect the performance of DTNs. DTNs represent a class of networks where there will be no existence of well-defined path between two communicating nodes. Due to wide-range applications of DTNs such as Inter-planet satellite communication networks, WSNs, VANETS, and military battlefield networks they are receiving increasing attention in both academia and industry. The design of routing strategies is a core step to permit timely delivery of information to a certain destination with high probability. As relay nodes need to be involved in ensuring successful delivery, it becomes crucial to design efficient resource allocation and data storage protocols.

DTNs exploit random contacts between mobile nodes to allow end-to-end communication between points that do not have end-to-end connectivity at any given instant. This is obtained at the cost of replications of data and hence of energy and memory resources. In basic scenario, where the packets are held by the source, it is optimal to use all opportunities to spread packets till some time σ depending on the energy constraint, and then stop. In such "Spray-and-Wait" policy, a general arrival of packets is assumed.

In this work, we focus on the general arrival of packets at source and two-hop routing. The conditions for optimality are considered for optimality in terms of probability of successful delivery and mean delay. Even though work-conserving policies are the best without energy constraint, but are outperformed by piecewise-threshold policies when there is an energy constraint. The copies of coded packets are generated both with linear block codes and rateless coding.

In the case of non-overwriting, the higher efficiency of piecewise-threshold policies compared with work- conserving policies by developing a heuristic optimization of the thresholds for all flavours of coding considered. When overwriting is allowed, WC policies may be suboptimal when an energy constraint is enforced.

II. EXISTING SYSTEM

Several satellites need to receive several data packets that may need retransmission due to channel errors. The packet level forward error correction (FEC) builds on Reed– Solomon codes, to transmit H additional packets, so that upon receiving any K of the $K+H$ packets, all stations are able to decode correctly the K information packets. The further proposed work involves the combination of both acknowledgment-

based retransmission protocols and FEC. In DTNs the framework is designed to be different since the challenge is to overcome frequent disconnections. Reed Solomon codes are used to verify the probability of successful delivery within a given time limit. In this scheme,

Each time the source meats a relay node, it chooses a frame i for transmission with probability u^i. In a simple scenario, the source has initially all the frame and u^i are fixed in time. It was shown in [1] that the transmission policy has a threshold structure: use all opportunities to spread frame till some time σ and stop, termed similar to "Spray and Wait" policy.

Further implemented works deals with techniques to erasure code a file and distribute the generated code-blocks over a large number of relays in DTNs, so as to increase the efficiency of DTNs under uncertain mobility patterns. The benefit of coding is assessed by extensive simulations and for different routing protocols, including two hop routing. Also, there are several allocation techniques; the problem is proved to be NP– hard. In ODE-based models semi-analytical numerical results are reported describing the effect of finite buffers and contact times.

III. PROPOSED SYSTEM

In the proposed work, it is assumed that a network contains N+ 1 mobile node. The communication range for two nodes is assumed to be within the reciprocal radio range also the communications are taken as bidirectional. Let β be the intra-meeting intensity, i.e., the mean number of meetings between any two given nodes per unit of time. Let λ be the inter-meeting intensity. We have $\lambda = \beta N$ .In *a* sparse network, i.e., the density of nodes is constant in *N*, so is λ. A file is transmitted from a source node to a destination node, and decomposed into *K* packets. The source of the file receives the packets at some times $t1 \leq t2 \leq \ldots \leq tK$. The arrival time of the *i*-th packet is denoted by *ti*. In this work, we do not assume any feedback that allows the source or other mobiles to know whether the file has made it successfully to the destination within time τ.

In two-hop routing, we consider two cases: When the source i) can overwrite its own packets in the relay nodes, and ii) when it cannot. The forwarding policy of the source is as follows. If at time *t* the source encounters a mobile, it gives it packet *i* with probability *ui*(*t*) if the overwriting case, and it does so in the non-overwriting case only if the met relay node does not have any packet and is given as $u(t) \leq 1$ where $u(t) = \sum_i u_i(t)$

Let $\widehat{\mathbf{X}}^{(N)}(t)$ be a K dimensional vector whose components are $\widehat{X}_i^{(N)}(t)$, for $i = 1, \ldots, K$. Here, $\widehat{X}_i^{(N)}(t)$ stands for the fraction of mobile nodes (excluding the destination) that have at time t a copy of packet i, in a network of size N. Let $\widehat{X}^{(N)}(t) = \sum_{i=1}^{K} \widehat{X}_i^{(N)}(t)$.

In this work, we consider two classes of forwarding policies.
Class 1: A *work-conserving* (WC) policy if whenever the source meets a node then it forwards it a packet, unless the energy constraint has already been attained.
Class 2: A *piecewise-threshold* policy if the source systematically transmits up to threshold time *si* after receiving packet *i*, and then stops forwarding until the next packet arrives.

The following optimization problems are studied:
• **P1.** Find **u** that maximizes the probability of successful delivery till time τ (over all kinds of policies).
• **P2.** Find **u** that minimizes the expected delivery time.

Policy **u** is called *uniformly optimal* for problem P1 if it is optimal for problem P1 for all $\tau > 0$. The energy constraint is denoted by E(*t*) for the whole network for transmitting and receiving the file during the time interval [0, *t*]. E(*t*) is assumed to be proportional to the number of transmissions that is $X(t) - X(0)$ as because packets are transmitted only to mobiles that do not have any.

We propose an algorithm that has the property to generate a policy **u** which is optimal not just for the given horizon τ but also for any horizon shorter than τ. The auxiliary definitions in this work are as given below:

- $Z_j(t) := \int_{t_1}^{t} X_j(r)dr$. We call $Z_j(t)$ the cumulative contact intensity (CCI) of class j.
- $I(t, A) := \min_{j \in A}(Z_j, Z_j > 0)$. This is the minimum non zero CCI over j in a set A at time t.
- Let $J(t, A)$ be the subset of elements of A that achieve the minimum $I(t, A)$.
- Let $S(i, A) := \sup(t : i \notin J(t, A))$ for i in A.
- Define e_i to be the policy that sends packets of type i with probability 1 at time t and does not send packets of other types.

The algorithm for for equalizing the less populated packets at each point in time is given as below:

A1 Use $\mathbf{p}_t = e_1$ at time $t \in [t_1, t_2)$.
A2 Use $\mathbf{p}_t = e_2$ from time t_2 till $s(1,2) = \min(S(2,\{1,2\}), t_3)$. If $s(1,2) < t_3$ then switch to $\mathbf{p}_t = \frac{1}{2}(e_1 + e_2)$ till time t_3.
A3 Define $t_{K+1} = \tau$. Repeat the following for $i = 3, ..., K$:
A3.1 Set $j = i$. Set $s(i,j) = t_i$
A3.2 Use $\mathbf{p}_t = \frac{1}{i+1-j}\sum_{k=j}^{i} e_k$ from time $s(i,j)$ till $s(i,j-1) := \min(S(j,\{1,2,...,i\}), t_{i+1})$. If $j = 1$ then end.
A3.3 If $s(i,j-1) < t_{i+1}$ then take $j = \min(j : j \in J(t,\{1,...,i\}))$ and go to step [A3.2].

Algorithm 1: Algorithm for equalizing the less populated packets

The algorithm first strives to increase the CCI of the latest arrived packet; trying to increase it to the minimum CCI which was attained over all the packets existing before the last one arrived. The process is repeated until the packet arrives. Rateless erasure codes are a class of erasure codes with the property that a potentially limitless sequence of coded packets can be generated from a given set of information packets. Information packets, in turn, can be recovered from any subset of the coded packets of size equal to or only slightly larger than *K*.

C1 Use $\mathbf{p}_t = e_1$ at time $t \in [t_1, t_2)$.
C2 Use $\mathbf{p}_t = e_2$ from time t_2 till $s(1,2) = \min(S(2,\{1,2\}), t_3)$. If $s(1,2) < t_3$ then switch to $\mathbf{p}_t = \frac{1}{2}(e_1 + e_2)$ till time t_3.
C3 Repeat the following for $i = 3, ..., K-1$:
C3.1 Set $j = i$. Set $s(i,j) = t_i$
C3.2 Use $\mathbf{p}_t = \frac{1}{i+1-j}\sum_{k=j}^{i} e_k$ from time $s(i,j)$ till $s(i,j-1) := \min(S(j,\{1,2,...,i\}), t_{i+1})$. If $j = 1$ then end.
C3.3 If $s(i,j-1) < t_{i+1}$ then take $j = \min(j : j \in J(t,\{1,...,i\}))$ and go to step [C3.2].
C4 From $t = t_K$ to $t = \tau$, use all transmission opportunities to send an RLC of information packets, with coefficients picked uniformly at random in $\mathbb{F}_q$.

Algorithm 2: Algorithm for RLC of information packets

In each sent packet, a header is added to describe what are the coefficients, chosen uniformly at random, of each information packet. The decoding of the *K* information packets is possible at the destination if and only if the matrix made of the headers of received packets has rank *K*.

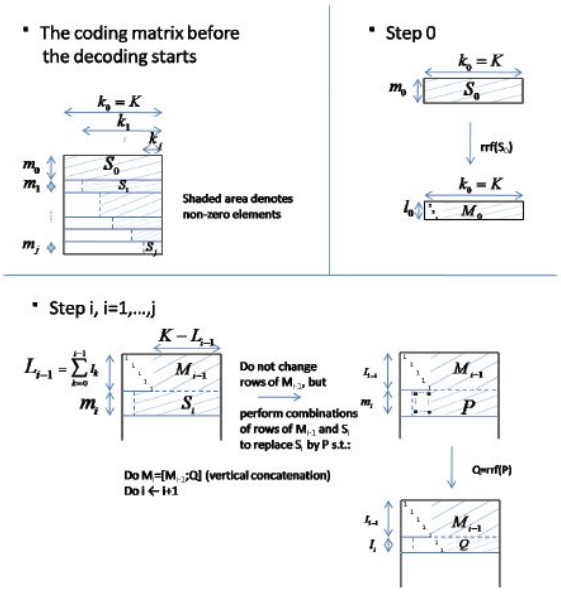

Fig 1: Decoding Process for forwarding policy

Given any forwarding policy $u(t)$, it is optimal for P1 and P2 to send coded packets resulting from RLCs of all the information packets available at the time of the transmission opportunity with probability $u(t)$. For any policy $u(t)$, the probability of successful delivery of the entire file is given by

$$P_s(\tau) = \sum_{j=0}^{K-1} \sum_{k_1>\cdots>k_j} \sum_{l_0=K-k_1}^{K} \cdots \sum_{l_i=K-k_{i+1}-L_{i-1}}^{K-L_{i-1}} \cdots$$

$$\sum_{l_j=K-L_{j-1}}^{k_j} \sum_{m_0=l_0}^{\infty} \cdots \sum_{m_j=l_j}^{\infty} \prod_{i=0}^{j} f(l_0,\ldots,l_i,m_i)\,,$$

with $L_i = \sum_{j=0}^{i-1} l_j$, $f(l_0,\ldots,l_i,m_i) = P(m_i)\binom{m_i}{l_i}\prod_{r=0}^{l_i-1}\left(1-\frac{1}{q^{K-L_{i-1}-r}}\right)$, where

$$P(m_k) = \exp(-\Lambda_k)\frac{\Lambda_k^{m_k}}{m_k!}\,, \quad \Lambda_k = \lambda\int_0^{\tau} Y_k(t)\,dt\,,$$

$$Y_k(t) = (t \geq t_{k+1})\lambda\int_{t_k}^{\min(t,t_{k+1})} u(v)\exp\left(-\lambda\int_0^{v} u(s)\,ds\right)dv\,.$$

In order to recover the *K* information packets, the matrix which has to be full-rank is composed of the *Si*, for $i = 0, \ldots, j$. rrf(*M*) denote the reduced row form of any matrix *M*, i.e., the matrix resulting from Gaussian elimination on M, without column permutation.

The decoding complexity of random network codes ($O(K3)$) may not be a problem in the DTN context as the decoding by progressive/incremental Gauss-Jordan elimination as the packets arrive at a slow rate can limit the

Computational burden per time unit. Our work holds also for multi-hop routing as the optimality condition relies up on the concavity of the function $\zeta(h) = 1 - \exp(-\lambda h)$. the case of multi-packet memory can be derived,

IV. CONCLUSION AND FUTURE WORK

In the implemented work, the problem of optimal transmission and scheduling policies in DTN with two-hop routing under memory and energy constraints . In this work, we have considered two cases: when the source can or cannot overwrite its own packets, and for WC and non WC policies. The implemented work is based on fixed rate systematic erasure codes and rateless random linear codes. in the overwriting case, we show that work-conserving policies are the best without any energy constraint.

The future scope of this work can be extended for multi-packet memory for the total buffer. This work can also be extended for multi-hop routing.

V. REFERENCES

[1] [1] Eitan Altman, Lucile Sassatelli, and Francesco De Pellegrini, Dynamic Control of Coding for Progressive Packet Arrivals in DTNs, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 2, FEBRUARY 2013.

[2] E. Altman, F. De Pellegrini, and L. Sassatelli, “Dynamic control of coding in delay tolerant networks,” in Proc. 2010 IEEE INFOCOM, pp.1–5.

[3] Y. Lin, B. Li, and B. Liang, “Efficient network-coded data transmissions in disruption tolerant networks,” in Proc. 2008 IEEE INFOCOM, pp. 1508–1516.

[4] Y. Wang, S. Jain, M. Martonosi, and K. Fall, “Erasure-coding based routing for opportunistic networks,” in Proc. 2005 ACM SIGCOMM Workshop Delay-Tolerant Netw., pp. 229–236.

[5] D. S. Lun, M. M´edard, and M. Effros, “On coding for reliable communication over packet networks,” in Proc. 2004 Annual Allerton Conf. Commun., Control, Comput., pp. 20–29..