Towards Energy-efficient and Robust Disaster Response Networks

Vijay K. Shah*[§], Satyaki Roy*[†], Simone Silvestri[§], and Sajal K. Das[†]*

[§]University of Kentucky, Lexington, USA, [†]Missouri University of Science and Technology, Rolla, USA
vijay.shah@uky.edu,sr3k2@mst.edu,silvestri@cs.uky.edu,sdas@mst.edu

ABSTRACT

In the aftermath of a large-scale disaster (such as earthquake), existing communication infrastructures are often critically impaired, preventing timely information exchange between the survivors, responders, and the coordination center. Typically, a temporary network, called Disaster Response Network (DRN), is set up using smart devices, movable base stations and easily deployable cellular antennas. However, such networks are challenged by rapid devices' energy depletion and component failures due to environmental adversities and hardware faults. State-of-the-art literature address energy challenges through intelligent routing, however robustness of DRN against component failures is largely unaddressed. In this paper, we investigate designing a novel network topology for DRNs, which is both energy-efficient and robust against component devices' failures. Specifically, the objective is to construct a sparse structure from the original DRN (termed, Sparse-DRN) while ensuring that there exists a connected tree backbone. Our performance evaluation shows that the Sparse-DRN offers a good trade-off between the energy efficiency and network robustness, while ensuring the QoS requirements i.e., packet delivery and network latency.

KEYWORDS

Disaster Response Network, Robustness, Energy efficiency

ACM Reference Format:
Vijay K. Shah*[§], Satyaki Roy*[†], Simone Silvestri[§], and Sajal K. Das[†]. 2019. Towards Energy-efficient and Robust Disaster Response Networks. In *International Conference on Distributed Computing and Networking (ICDCN '19), January 4–7, 2019, Bangalore, India.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3288599.3295589

1 INTRODUCTION

In the aftermath of a large-scale disaster (e.g., earthquake), the primary communication infrastructures (such as cellular towers) and power sources may be partially or completely damaged [1]. Such communication breakdown and power outage restrict the responders from exchanging situational information like status of survivors, supply chain of goods and damaged roads and buildings. This leads to an asynchronous coordination of rescue/relief operation and ad-hoc decision making in the disaster area, which aggravates the human casualty and economic loss. Thus, a makeshift network is a necessity for bridging the communication gap among the survivors, responders and the coordination center (CC).

Recent reports show that wireless devices such as smart phones and laptops are generally available with survivors in a disaster area. For example, after Nepal earthquake [9], there were approximately 23 million active mobile subscribers in a population of 27 million. Additionally, there are some preexisting *points of interest* (PoIs) viz., evacuation centers, hospitals, police stations etc., equipped with communication devices such as WiFi routers and cellular towers. Various vehicles, called *mobile base stations*, facilitated with communication antennas may also patrol the disaster scene. Keeping this in mind, several research efforts [3, 11, 15] have been directed towards the formation of delay tolerant networks (DTNs) in post disaster scenarios, termed *Disaster Response Networks* (DRNs).

Existing research in DRNs (and DTNs) have mainly proposed routing protocols that focus on achieving high packet delivery at the expense of message replications and forwarding (i.e., flooding message copies), and thereby consuming significant amount of energy [14, 16]. For energy efficiency, intelligent routing approaches have been proposed that focus on reducing the message copy transmissions [1, 13, 15]. Note, in the context of such challenging networks, *energy efficiency can be quantified by the number of message replica transmissions in the network* [15].

Recently, topology control mechanisms have been proposed for DTNs to enhance energy efficiency by providing sparse connectivity (such as, a spanning tree) [2, 4, 6]. However, DRNs are subject to – (i) intermittent connectivity (due to unpredictable node mobility), (ii) defunct smart devices (due to battery depletion in the absence of power infrastructure), and (iii) node failures (due to hardware faults). Keeping these considerations in mind, we infer that energy efficiency and sparse connectivity alone cannot guarantee steady information flow in DRNs. Therefore, it becomes imperative to ensure multiple communication pathways between survivors and the CC such that the steady information exchange between them is ensured, despite node failures. Hence, a DRN topology must be both energy-efficient and robust. Specifically, we define network robustness as *the ability of the network to ensure information flow between the survivors and the CC, despite node failures.*

In this paper, we study the design of a novel DRN network topology, termed Sparse-DRN, which is both energy-efficient and robust against component failures. Specifically, the Sparse-DRN

*Primary co-authors

[1] Almost 800 out of 2600 cellular sites were down after 2015 Nepal earthquake [7].

ICDCN '19, January 4–7, 2019, Bangalore, India
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6094-4/19/01…$15.00
https://doi.org/10.1145/3288599.3295589

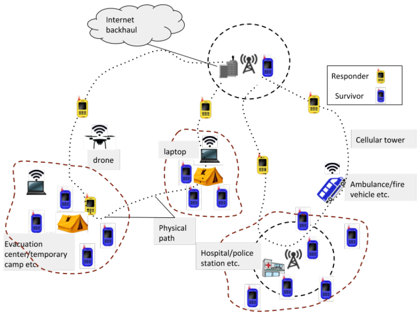

Internet backhaul
Responder
Survivor
Cellular tower
drone
laptop
Ambulance/fire vehicle etc.
Physical path
Evacuation center/temporary camp etc.
Hospital/police station etc.

Figure 1: A post-disaster scenario.

is a sparse structure, constructed by extracting a connected tree backbone structure from original DRN, followed by the addition of a pre-specified number of randomly chosen links (See Section 3). Our experimental evaluation shows that the Sparse-DRN offers a good trade-off between energy efficiency and network robustness, while ensuring both packet delivery and network latency.

2 NETWORK MODEL AND ASSUMPTIONS

This section discusses the key components of a representative post-disaster scenario (See Fig. 1), followed by network model.

2.1 Key Components

Survivors. The affected individuals equipped with smart devices, such as smart phones and laptops, which are capable of short-range peer-to-peer (P2P) communication. A survivor has an application installed (for instance Surakshit [8]) on his device that allows him to (a) establish P2P communication via WiFi-Direct or Bluetooth (ad-hoc mode), and (b) exchange situational or rescue/relief related information in forms of text, image, audio and video clips. A survivor, either static or mobile, usually remain confined within the boundary of his respective PoI (explained below), and rarely leaves the PoI (due to unsafe outside environment [13]).

Points of Interest (PoIs). Certain geographical locations such as schools, parks, hospitals, preexisting evacuation centers, temporary camps, shelter points etc., where the survivors gather in the aftermath of the disaster. The location of PoIs are fixed.

Information dropbox (IDB). Each PoI is equipped with a dedicated Information dropbox (IDB), which may be a laptop, a WiFi/cellular antenna or a customized equipment (like a kiosk [10] or consumer premise equipment [12]). The IDB has the following capabilities: (i) two wireless communication technologies - (i.a) short-range P2P technology to communicate with the resident survivors, and (i.b) long-range technology (such as, WiFi or GSM/LTE) to communicate with other IDBs, patrolling responders or the coordination center directly (explained below), (ii) storage capability to temporarily store the messages collected from survivors or patrolling responders. The locations of IDBs are fixed.

Responders. Members of rescue and relief teams, medical teams, disaster response teams, police and fire vehicles, who periodically or aperiodically patrol one or more PoIs in the disaster area. These responders are also equipped with short-range P2P enabled smart devices (or long-range cellular or WiFi antennas).

Coordination Center (CC). The base station that coordinates the entire rescue/relief operations in the disaster area, and can communicate with outside world (if required) over Internet backhaul. All the data generated at the survivors' end are eventually delivered to the CC for processing and analysis, based on which appropriate future measures are taken for efficient recovery operations.

2.2 Network Model

Due to the mobility of survivors and responders, intermittent connectivity and failure of communication devices, the DRN can be modeled as a time-evolving graph. As discussed in Section 2.1, the survivors tend to confine their movement to their respective PoIs because the outside environment is unfavorable. As a consequence, the DRN topology, though time-evolving, remains largely unchanged for a considerable duration of time, defined as a timeslot (in the order of several minutes). Note that in the rarest of events, few survivors leave their respective PoIs. To make a realistic representation of DRN, we consider the total time duration T, say 12 hours, to be divided in to H distinct and equal time slots, $\{1, 2, \ldots h \ldots H\}$. At a given time slot h, let DRN be represented by an undirected graph $G^h = (V^h, E^h)$, where V is the set of nodes comprising survivors, IDBs, responders, and the CC, and E is the set of communication links. Let $e^h(u, v) \in E^h$ denote that nodes u and v have come in the communication range for a prespecified duration of time (in order of few minutes) within the current time slot h. Our proposed approach for the construction of the Sparse-DRN topology (as discussed in Section 3) is applied independently at each time slot [2], therefore, we drop h from all the notations from here onwards.

3 SPARSE-DRN TOPOLOGY

In this section, we briefly discuss a simple mechanism for the construction of Sparse-DRN topology in a real post-disaster setting, followed by the details of the proposed algorithm.

3.1 Sparse-DRN topology construction

As mentioned in Section 2.2, the DRN is a time-evolving graph and the total time T is split into H slots. At the beginning of each timeslot, the CC periodically broadcasts a *Hello* packet. On receiving the Hello packet, each survivor and IDB sends a *Response* packet of format <*survivor/IDB ID, loc-coor*> to the CC. The CC waits a prespecified duration of time (in order of few minutes) from the start of each time slot, in order to receive the *Response* packets. Then, the CC invokes the proposed algorithm (explained below), which utilizes the location of the survivor and IDB nodes to generate a list of neighbors each node can communicate with, and broadcast them. Finally, on receiving its respective neighbor list, every node restricts data forwarding only to those nodes specified on the neighbor list, thus constructing the sparse-DRN topology.

3.2 Algorithm Overview

Here, we discuss the details of the proposed algorithm for the construction of the Sparse-DRN topology. Our algorithm is based on the theorem explained below.

Theorem 3.1. *The cardinality of simple paths between any survivor to the CC always increases with the addition of a new non-parallel link in the connected DRN topology* $G(V, E)$.

[2] Since the duration of each time slot is considerably high, it is reasonable to construct Sparse-DRN at the beginning of each time slot.

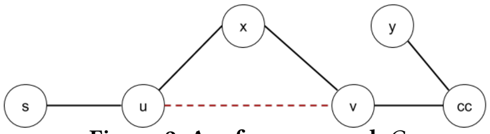


Figure 2: A reference graph G

Proof. Consider a connected DRN topology G. Since G is undirected, there exists a path from each survivor to CC. From graph G in Fig. 2, let $P(s, cc) =< s, u, x, v, cc >$ be a simple path from a survivor s to coordination center cc. Now we introduce a new link $e(u, v)$ to G, which in turn, creates a new path between node s and cc, i.e., $P(s, cc) =< s, u, v, cc >$, and hence proves the theorem. □

Algorithm description. The inputs to the algorithm are (1) Original DRN topology G and (2) a control parameter X ($0 \leq X \leq 1$) that dictates the graph density of the Sparse-DRN.

The algorithm operates in two steps. First, it constructs the spanning tree structure $S(V_s, E_s)$ which acts a backbone for the resultant Sparse-DRN topology. The key insight behind this step is to obtain the potentially most energy-efficient DRN topology and ensure that there exists at least one path from each survivor to the CC. Then, in the second step, in order to introduce multiple communication paths (as shown in Theorem 3.1), we iteratively add a pre-specified $X.(|E| - |E_s|)$ number of additional links to the spanning tree backbone. The time complexity of the algorithm is $O(|E|log|V|)$.

4 PERFORMANCE EVALUATION

This section presents a comparative analysis of both energy-efficiency and network robustness for the following three topologies:

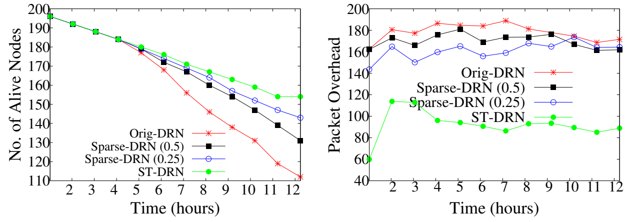
- Orig-DRN - Original network formed due to communication among survivors, IDBs, responders, and CCs, equipped with either smart devices or cellular/WiFi antennas or both.
- ST-DRN - A spanning tree constructed by removing surplus edges from original DRN.
- Sparse-DRN - Proposed topology (discussed in Section 3) corresponding to threshold variable $X = 0.25$ and 0.5, denoted by Sparse-DRN (0.25) and Sparse-DRN (0.5), respectively.

4.1 Post-disaster Setting

We consider a disaster area of 3×3 square kilometers, which comprises one CC, 50 responders, and 5 PoIs (and IDBs), each with $25 - 35$ survivors (which adds up to 200 nodes). The PoIs and the unique CC are randomly placed in the disaster area. A unique IDB and the survivors are randomly placed in the vicinity of a certain PoI (within a radius of $300 - 500$ meters). The responders travel back and forth between the CC and the prespecified set of PoIs. The survivors and responders have P2P communication technology with transmission range of 50 meters, the CC has long-range cellular antenna with range of 500 meters. The IDBs are equipped with both the communication technologies. (These settings are in accordance with the network model discussed in Section 2.)

4.2 Energy efficiency and QoS Analysis

We use Opportunistic NEtwork (ONE) simulator [5] to analyze the energy efficiency and QoS (in terms of packet delivery ratio and network latency) of the proposed Sparse-DRN topology against other topologies. The simulation duration is 12 hours and the duration of each time slot is taken as 1 hour.



(a) (b)

Figure 3: (a) Number of alive nodes and (b) Message overhead vs Simulation time

Table 1: Edge Count for different network topologies (with 200 nodes) at the start of simulation

DRN Topology	Orig-DRN	Sparse-DRN(0.5)	Sparse-DRN(0.25)	ST-DRN
Number of links	739	407	322	199

All the experiments, unless otherwise stated, are performed with the following parameters:

Network traffic model: Each survivor generates messages at a rate of 1 packet every 35 - 45s. A packet size is taken from the interval [0.5 - 1] MB and TTL (time-to-live) is 2 hours.

Energy expenditure model: The energy consumed in data transmission/reception and scanning other devices are 1.2 J/s and 0.3 J/min, respectively. Each survivor node has a finite initial energy of 100 J (Other nodes have a high initial energy of 1000 J). Besides, all nodes have a buffer storage of 1 GB.

Node failure model: We consider the failure of 2% randomly selected survivors, IDB and responders (except CC) after every 1 hour. Note that in the interest of fair comparison, the same nodes are failed for all the topologies.

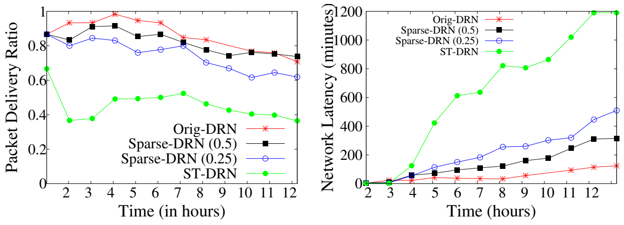
Node mobility model: Survivors either remain static or move in the vicinity of their respective PoIs (where they reside) with an average speed of 5 Km/hr. However, they may rarely move to other neighboring PoIs. In our experiments, we consider that 10% survivors may move to other PoIs at each time slot. The average speed of responders is taken as 10 Km/hr. The PoIs, IDBs, and the CC remain fixed for the entire simulation duration.

Routing Model: We utilize the epidemic routing protocol [16] since it guarantees the QoS requirements, which are the primary requirements of any DRN topology.

Performance Metrics: We compare the Sparse-DRN against the other topologies in terms of the following performance metrics:

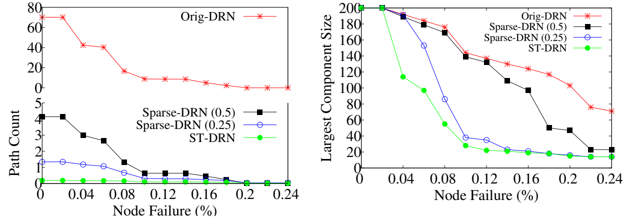
- *Energy Efficiency* – total number of alive nodes in the DRN,
- *Packet Delivery Ratio (PDR)* – fraction of total unique messages received at the CC to the total generated messages at the survivor nodes,
- *Network Latency* – average delay incurred in delivering all generated messages to the CC.

Energy Efficiency. We study the energy efficiency of the Orig-DRN, Sparse-DRNs and ST-DRN for 12 hours of simulation. We know that Sparse-DRNs possesses intermediate graph density to Orig-DRN and ST-DRN (See Table 1). Since energy consumption is quantified by the number of message replica transmissions in the network, Sparse-DRN (0.25) and Sparse-DRN (0.5) have lower energy consumption than Orig-DRN and higher than ST-DRN (as shown in Fig. 3(a)). This result is further corroborated by the packet overhead curve as shown in Fig. 3(b).



(a) (b)

Figure 4: (a) PDR and (b) Network latency vs Simulation time



(a) (b)

Figure 5: (a) Path Count and (b) Largest component size vs Perc. of Node Failures

Packet Delivery Ratio. Fig. 4(a) shows that Orig-DRN, owing to its high graph density, has a high PDR in the initial stages of the experiment. After 6 hours of simulations the Orig-DRN suffers from the death of energy constrained survivor nodes, making the PDR lower or comparable to Sparse-DRN. This is because Sparse-DRN, due to its energy efficiency, does not suffer badly from node deaths and are able to support high packet delivery for longer periods.

Network Latency. Fig. 4(b) shows that Orig-DRN and Sparse-DRNs exhibit lower network latency compared to ST-DRN, due to the existence of higher number of communication paths between each survivor and the CC; notwithstanding the node failures (See Fig. 5(a)). For the similar reason, the Sparse-DRN (0.5) outperforms the relatively sparser Sparse-DRN (0.25).

4.3 Network Robustness Analysis

Through graph experiments, we evaluate the robustness of Sparse-DRN against Orig-DRN and ST-DRN in terms of the following *robustness metrics* – (i) *path count*, and (ii) *size of largest connected component*. For the graph experiments, we consider the same post-disaster setting (as discussed in Section 4.1) and extract the DRN (i.e., Orig-DRN) topology formed at each time slot (i.e., 1, 2, . . . 12) hours. Furthermore, we remove the same 2% failed nodes (from above simulation experiments) for all topologies.

Path count. The multiplicity of paths from any survivor node to the CC reflects the robustness of the network, by ensuring steady information flow in the event of node failures. In our experiments we only consider paths of length less than 6 as we observe that the average hop count was 6 (also counting the number of all possible simple paths between a pair of nodes is a NP-Hard problem [17]). As shown in Fig. 5(a), Orig-DRN renders the highest path count owing to its high graph density. Sparse-DRN exhibits better average path count than ST-DRN because it possesses greater number of paths from survivor to CCs, despite random node failure.

Size of largest connected component. We gauge the connectivity of network by the *size of largest connected component* after node failure. Fig. 5(b) shows that Orig-DRN exhibits the highest connectivity i.e. largest size of connected components because of its high graph density. ST-DRN exhibits poorer connectivity compared to Sparse-DRN because it is the sparsest topology.

5 CONCLUSION AND FUTURE WORK

In this paper we investigated the construction of a novel network topology for disaster response networks, called sparse-DRN, which is energy-efficient yet robust against node failures. Sparse-DRN is a subgraph of the original DRN topology which is constructed by augmenting a connected backbone structure with a prespecified number of randomly chosen links (from the original DRN.) Our graph and simulation experiments demonstrate that the idea of Sparse-DRN is a step in the direction of achieving trade-off between the energy efficiency and network robustness, while ensuring the QoS requirements. In the future, we would like to come up with an intelligent algorithm for constructing a network topology that optimizes the conflicting trade-off between energy efficiency and network robustness in DRN. Moreover, we would also like to investigate the optimal value of control parameter X, for a given objective of energy efficiency, network robustness, and QoS requirements.

6 ACKNOWLEDGEMENT

This work is partially supported by NATO grant G4936 and Intelligent Systems Center (ISC) at Missouri S&T, Rolla.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine. 2006. MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks.. In *IEEE Conference on Computer Communications (INFOCOM)*.

[2] H. Chen, K. Shi, and C. Wu. 2016. Spanning tree based topology control for data collecting in predictable delay-tolerant networks. *Ad Hoc Networks* 46 (2016), 48–60.

[3] K. Hazra, V. K. Shah, M. Bilal, S. Silvestri, S. K. Das, S. Nandi, and S. Saha. 2019. A Novel Network Architecture for Resource-constrained Post-disaster Environments. In *accepted in Conference on Communication Systems and Networks*.

[4] M. Huang, S. Chen, Y. Zhu, and Y. Wang. 2013. Topology control for time-evolving and predictable delay-tolerant networks. *IEEE Transactions on Computers (TOC)* 62, 11 (2013), 2308–2321.

[5] A. Keränen, J. Ott, and T. Kärkkäinen. 2009. The ONE simulator for DTN protocol evaluation. In *Int'l conf. on simulation tools and techniques (ICST)*. 55.

[6] F. Li, S. Chen, M. Huang, Z. Yin, C. Zhang, and Y. Wang. 2015. Reliable topology design in time-evolving delay-tolerant networks with unreliable links. *IEEE Transactions on Mobile Computing (TMC)* 14, 6 (2015), 1301–1314.

[7] [Online]. 2018. GSMA Report: Disaster Response Nepal Earthquake Response and Recovery Overview., Last accessed on Sep 15, 2018.

[8] [Online]. 2018. https://itsforkit.github.io/uploaded/Surakshit Software Data Sheet.pdf". Last accessed on October 14, 2018.

[9] [Online]. 2018. https://www.ushahidi.com/blog/2015/04/25/supporting-online-volunteer-response-to-the-nepal-earthquake/, Last accessed on Sep 15, 2018.

[10] A. Pentland, R. Fletcher, and A. Hasson. 2004. Daknet: Rethinking connectivity in developing nations. *IEEE Computer* 37, 1 (2004), 78–83.

[11] S. Saha, S. Nandi, P. S. Paul, V. K. Shah, A. Roy, and S. K. Das. 2015. Designing delay constrained hybrid ad hoc network infrastructure for post-disaster communication. *Ad Hoc Networks* 25 (2015), 406–429.

[12] V. K. Shah, S. Bhattacharjee, S. Silvestri, and S. K. Das. 2017. Designing Sustainable Smart Connected Communities using Dynamic Spectrum Access via Band Selection. *ACM International Conference on Systems for Energy-Efficient Built Environments (BuildSys)* (2017).

[13] V. K. Shah, S. Roy, S. Silvestri, and S. K. Das. 2017. CTR: Cluster based topological routing for disaster response networks. In *IEEE International Conference on Communications (ICC)*. 1–6.

[14] T. Spyropoulos, K. Psounis, and C. S. Raghavendra. 2005. Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In *ACM SIGCOMM workshop on Delay-tolerant networking*. 252–259.

[15] Md Y. S. Uddin, H. Ahmadi, T. Abdelzaher, and R. Kravets. 2013. Intercontact routing for energy constrained disaster response networks. *IEEE Transactions on Mobile Computing (TMC)* 12, 10 (2013), 1986–1998.

[16] A. Vahdat and D. Becker. 2000. Epidemic routing for partially connected ad hoc networks. *Technical Report CS-200006, Duke University* (2000).

[17] Douglas R White and Mark Newman. 2001. Fast approximation algorithms for finding node-independent paths in networks. (2001).