Federation Among Remote Military Data Stores In Austere Environments

Steve Mazza
School of Systems Engineering
Naval Postgraduate School
Monterey, CA 93943
Email: spmazza@nps.edu

***Abstract*—Transportable computing and some degree of network connectivity have been a necessary component of US military operations at least since the advent of the personal computer in the 1980s. Subsequent ubiquity of laptop computers and, more recently, hand held devices such as the smart phone have exacerbated the situation by allowing the need for data and the locus of computing power to be increasingly distributed and fragmented. Through model design and discussion we address some aspects of one potential solution to this fragmentation through federation of data stores. In particular, we show that we can guarantee eventual consistency of data, even in austere environments. Furtherore, we show that this state can be achieved in time proportional to $O(Klog(n))$ where n is the number of nodes in the network.**

I. Introduction

Transportable computing and some degree of network connectivity have been a necessary component of US military operations at least since the advent of the personal computer in the 1980s. Subsequent ubiquity of laptop computers and, more recently, hand held devices such as the smart phone have exacerbated the situation by allowing the need for data and the locus of computing power to be increasingly distributed and fragmented.

Consequently, there exists a significant and growing problem related to the decentralization of computing in the United States military. Due to the increasing distribution of computing power and data storage, there is now an acknowledged need to implement some form of federation [1] in order to maintain data concurrency. This is especially true in theaters of operation that are characterized as austere environments and for which communications are assumed to be disconnected, intermittent, or limited (DIL), and where connections to a centralized data store are impractical or impossible.

II. Problem Space

United States involvement in military operations over the past fifteen years has been in operationally challenging environments. Lack of existing infrastructure to provide necessary operational support has been a primary challenge to sustaining long-term presence necessary to achieve our national security goals. We focus on the challenges associated with fighting in an asymmetrical conflict while operating in an environment in which the transmission of electronic data is challenging at best.

A. Motivation

Is this answered in the Introduction? If not (or possibly even, if) elaborate here on the distribution (diffusion) of computing and storage. Also, comment on the commonality of the need for federation as a service to a) protect and manage bandwidth as an Organizational resource, and b) prevent independent implementation by multiple systems, which would result in redundant and potentially conflicting services. We view bandwidth as a resource and treat it similar to ammunition and food.

B. Questions

Here is what we intend to address:

- Can we guarantee eventual consistency of data, if even statistically?
- In what sort of time can we expect to achieve consistency?
    - I think it should approach $O(log(n))$, maybe with some constant, K, based on the likelihood that small-world networks will develop. $O(Klog(n))$
    - Elapsed time, based on number of time steps and the average duration of each step.

III. Model Design

We have an interesting situation in that the physical organization of the network is highly structured, as prescribed by military doctrine, which favors a top-down, hierarchical task organization with a relatively fixed number of nodes at each echelon. We generalize this as a tree structure in the classical sense, having no closed loops. We then augment this structure by introducing some loops that connect nodes both laterally and across echelons to represent various opportunities for data delivery and synchronization scenarios not uncommon to actual operational threads.

A. Bandwidth and Connectivity

Where this graph structure becomes particularly interesting is in the implementation of the edges. Due to limited resources in most all theaters of operation[1] we model the probability of connectivity and bandwidth as an edge weight that tends to

[1] Recent theaters of operation include Iran, Iraq, and Afghanistan.

follow an inverse power law proportional to the distance of any node, $\mathscr{N}_k$, to the root node, $\mathscr{N}_0$.

We allow creation of the graph model dynamically by using the inverse square of the distance law of gravitational attraction to approximate both bandwidth and the probability of connectivity within the constraints of our graph model. We assume distance, d, as the graph distance between any two given nodes, $\mathscr{N}_i$ and $\mathscr{N}_j$ such that $d(\mathscr{N}_i, \mathscr{N}_j)$ is the geodesic distance with $0 < d \leq \epsilon(v)$, where $\epsilon(v)$ is the graph diameter. We construct the graph following this basic model but also apply a constant, K, to allow a correction for accuracy, given the particular constraints of any specific setting.

B. Undirected Graph

While the traditional flow of information in a military hierarchy follows a top-down model, we implement an undirected graph. We feel this is in keeping with the stated specific desire that each soldier become a sensor on the network [2]. A direct result of this is that information will naturally flow naturally both up and down the traditional chain of command. An unintended consequence is that, due largely to task re-organization, general officer and staff mobility, and transient network connections, it may also flow laterally within a structural organization and even across formations. We will further see how this occasional lateral flow of information facilitates our desired end state of achieving consistency of data across the network by creating temporary ad hoc small-world networks within the hierarchical military structure.

C. Shortcuts

We intentionally allow the occasional introduction of shortcuts on our graph. These shortcuts model the transit of information over non-traditional routes within the network. Shortcuts are an important part of this network model in that they intermittently create small-world type situations within an otherwise hierarchical, acyclical network model. These shortcuts come in two general types that have similar effect but which arise from different circumstances.

1) Lateral Movement of Data: Data at rest on computing devices[2] in transit between Companies or Battalions is an example of how a situation can arise. When this results in the opportunistic exchange and synchronization of data between nodes that are otherwise separated by much larger geodesic distances, it constitutes an instance of an unintended consequence of an increasingly distributed and mobile computing environment.

2) Hierarchical Movement of Data: The establishment of temporary connectivity from one echelon to another, which bypasses the standard chain of command can also result in a hierarchical movement of data. Such situation may exist if, for example, a Company Commander required a Sat-Com link to a Division asset or if that Commander (or his staff) travels to Division HQ. In both cases we are creating network cycles in the form of temporary links that transcend the hierarchical structure of the graph and connect nodes tat are otherwise separated by much larger geodesic distances.

IV. Disaster Recovery

An event in which a node suffers catastrophic loss of data, a disaster recovery scenario, can be evaluated with epidemic modeling. In both cases there is a non-trivial healing function which occurs over some t time steps and which is affected by the network topology [3]. In the former case, the disaster recovery *heals* similar to a standard S-I-R model. The failed node is analogous to the infected state (for example in a cellular automata). As the data propagates back, the infected node transitions to a recovered state. All nodes on the network are assumed to be susceptible.

As with all data flow on the network, the rate of propagation of data to the failed node is determined by bandwidth and probability of connectivity, both of which are functions of geodesic distance to the root node.

V. Related Work

Possibilities for additional, related work include:

- Individual datum may have different levels of importance, and consequently there may be the need to address QoS issues on the network.
- Security has been summarily ignored for the sake of this discussion, but must be implemented in a way that satisfies the needs of the military organization.

VI. Conclusion

The conclusion goes here.

The following is just a collection of citations that may (or may not) be used in this paper. I have collected them here in order to ensure they not get misplaced. [4] [5] [6] [7] [8] [3] [9] [10] [11] [12]

References

[1] T. M. Takai, "Cloud computing strategy," Department Of Defense, Tech. Rep., 2012.

[2] *ES2: Every Soldier is a Sensor*, 2003.

[3] A. Ganesh, L. Massoulié, and D. Towsley, "The effect of network topology on the spread of epidemics," *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, 2005.

[4] P. Hui, J. Crowcroft, and E. Yoniki, "Bubble rap: Social-based forwarding in delay tolerant networks," *Mobile Computing, IEEE Transactions on*, 2011.

[5] C. Liu and J. Wu, "Scalable routing in cyclic mobile networks," *Parallel and Distributed Systems, IEEE Transactions on*, September 2009.

[6] A. Vahdat and D. Becker, "Epidemic routing for partially-connected ad hoc networks," Department of Computer Science, Duke University, Tech. Rep., 2000.

[7] T. Gross, C. J. D. D'Lima, and B. Blasius, "Epidemic dynamics on an adaptive network," *Physical Review Letters*, 2008.

[8] S. C. Fu and G. Milne, "Epidemic modelling using cellular automata," *Proc. of the Australian Conference on Artificial Life.*, 2003.

[9] G. Bent, P. Dantressangle, P. Stone, D. Vyvyan, and A. Mowshowitz, "Experimental evaluation of the performance and scalability of a dynamic distributed federated database," *Proc. 3rd Ann. Conf. International Technology Alliance*, 2009.

[10] G. Bent, P. Dantressangle, D. Vyvyan, A. Mowshowitz, and V. Mitsou, "A dynamic distributed federated database," *Proc. 2nd Ann. Conf. International Technology Alliance*, 2008.

[11] A. Toce, A. Mowshowitz, and P. Stone, "Hyperd: A hypercube topology for dynamic distributed federated databases," *Proceedings of the Fifth Annual Conference of ITA*, 2011.

[12] J. Sonnenberg, "Disconnected, intermittent, limited (dil) communications management technical pattern," Harris Corporation, Tech. Rep., December 2009.

[2] While these are traditionally ruggedized racked computers, increasingly they will be tablets, smart phones, and other end user devices (EUDs).