INCREASING INFRASTRUCTURE SURVIVABILITY THROUGH RELIABLE SERVER POOLS

Mariusz A. Fecko[1], **M. Ümit Uyar**[2], **Jianliang Zheng**[2], **Phill T. Conrad**[3], **Sunil Samtani**[1]

[1] Applied Research Area
Telcordia Technologies, Inc.
Morristown, NJ 07960, USA

[2] Electrical Engineering Department
City College of New York
New York, NY 10031, USA

[3] Computer Science Department
Temple University
Philadelphia, PA 19122, USA

1 Introduction

Future Combat Systems will rely on battery-powered devices and wireless sensor nodes deployed in mobile ad-hoc networks. In this environment, applications such as collaborative planning, mobile command and control, situational awareness, remote login and file transfer, voice over IP (VoIP), will place increasing demands on reliable transport protocols and persistent sessions. Traditional client-server communications will experience lossy and intermittent conditions that disrupt and often abort traditional reliable transport protocol connections.

In mobile ad-hoc networks, client-server connections need to be persistently maintained for military applications even as links and nodes migrate or become disabled during times of severe network stress. This research investigates increasing availability and survivability of the battlefield infrastructure by allowing a pool of redundant information sources to be viewed as a single transport endpoint. In other words, servers that can provide equivalent functionality are pooled together; when a particular server becomes unavailable, or network QoS degrades, a client can transparently switchover to another server in the pool.

There are many promising applications of the reliable server pools in a battlefield environment. Consider a mobile soldier accessing a database of enemy locations. The soldier need not break and restart a session should enemy fire make that database unreachable. Instead the session would transparently continue with a redundant backup database. Another potential application of reliable server pooling is Agile Commander, an infrastructure for mobile command and control aided by continuous battle planning and event control systems. To better satisfy the requirement of graceful degradation for the C2 applications, various server components of Agile Commander could be replicated on multiple pool elements. The client-side software can then help adaptive C2 applications to switchover (in other words, relink communications autonomously) between mobile databases/proxies, deployed on server pools. Reliable server pools can also be used to increase availability of servers distributing autoconfigurable IP addresses and authentication keys for self-configuring subnets, and providing situational awareness on a battlefield (Section 3).

With the focus on fixed-infrastructure networks, the IETF rSerPool Working Group is developing new lightweight protocols. We believe that these protocols offer sound signaling solutions with respect to server (de)registration and client requests for server pooling service. Unless our extensive evaluation proves otherwise, we plan to reuse these components of the IETF architecture. We are currently focusing on other critical aspects of the provisioning of server pooling services in the FCS environment.

2 Research issues

The IETF approach is a best-effort architecture, with no QoS or service differentiation aspects. Our enhanced architecture provides these protocols with the distributed server selection beyond the originally defined simple schemes such as round-robin or least-recently-used. The architecture also enables the server selection to be broader than client-side selection schemes. In the longer-term, the QoS-based server selection and the dynamic management of pool membership in wireless networks with high mobility will introduce QoS and service prioritization concepts to reliable server pooling.

2.1 Dynamic reconfiguration

In a dynamic approach to pool management, the reliable server pool has to be re-configurable based on route and topology changes in the network and servers failure and recovery. The reliable server pool should be dynamically auto-configured to adjust to these changes. According to our scheme, each node can potentially be a server, and this willingness to be a server is indicated as a degree of readiness, which depends on the server load and current battery life. The degree of readiness can be defined as the number of associations that a server is willing to sustain at a certain level of quality. A server may belong to different server pools at varying degrees of readiness. Server pools can be formed and taken down dynamically. They may also merge or split depending on certain parameters such as network connectivity, link state, mobility, failures, traffic load and utilization.

2.2 Distributed server selection

Given the FCS environment's fast changing characteristics, traditional approaches to server selection based on past measurement data, dynamic probes, and server evaluation based solely on the applications estimates are most likely to be inadequate. In addition, in the resource-constrained environment, the IETF's best-effort policy to

offer the server pool resources may lead to the degradation of service to the already existing sessions, impair the ability to perform successful switchovers or start new sessions, and result in a very high number of unsuccessful session attempts when the network resources are stressed. We are investigating fundamentally different approaches to server selection, with intelligent management of server resources that may become overloaded.

One possible approach is based on prioritized server resources allocation. Finding the optimal server allocation policy is inevitably complicated. To overcome this problem, some recent research efforts resulted in the formulation of two suboptimal, but significantly simpler approaches to dynamic resource allocation for prioritized classes of users: virtual partitioning (VP) and upper limit (UL) policy. Both these approaches achieve a high multiplexing gain when the service request load is light (converging to the best-effort policy), and offer a good isolation of resources for underutilized or high-priority classes when the resources are severely overloaded.

3 Application to situational awareness system

Consider a hypothetical distributed system providing situational awareness. Such a system might include data reporting elements (DREs) —vehicles reporting their GPS coordinates, direction and velocity, fuel level—and data display elements that provide personnel at various echelons with displays of the battlefield appropriate to their mission, rank, and authorization. In addition, several levels of relay agents may be deployed to avoid single points of failure by providing failover and redundant gathering of information. First level relay elements RE-1s (e.g., orange sensors) gather data directly from DREs (e.g., blue and green sensors), and aggregate data together into a more useful and compact form for transmission to RE-2s and higher. For example, individual positions of enemy vehicles within a battle group would be summarized into a bounding polygon with the number of vehicles present. This aggregate data then would be reported to RE-2.

In such a system, each DRE establishes a persistent on-the-move session with RE-1. Using reliable server pooling protocols, DRE "x" locates both a primary RE-1 "a" and a secondary RE-1 "b." DRE "x" then maintains its session with "a" and sends updates to "a" as needed. Meanwhile, "a" periodically updates "b" with sufficient state to allow seamless failover of "x"'s data-reporting session to "b." Once failover occurs, the reliable server pool protocols should identify a new RE-1 for "x." Similarly, at each level, the RE-(k) would establish a persistent on-the-move session with both a primary and a secondary RE-(k+1). The session between RE-(k) and RE-(k+1) uses the same reliable server pool selection protocols and failover protocols as described above for the session between DREs and RE-1. Similarly, data display elements would establish persistent on-the-move sessions with REs at the level appropriate to the detail of the display needed, with both a primary and secondary element chosen by the reliable server pool protocols.

4 Evaluation in multi-layer wireless system

A fundamental question is whether a lightweight, best-effort approach, such as the one provided by IETF rSerPool protocols, is sufficient for ad hoc networks. This issue becomes more critical under stress conditions imposed by the battlefield wireless environment. Therefore, the reliable server pooling architecture must be analyzed and evaluated in a multi-layer wireless system with many interacting components, including transport protocol (SCTP), ad hoc routing protocols (AODV, MAODV), MAC protocols, realistic mobility and radio propagation models, and failure models. The main research issue is to address reliable server pooling performance and scalability with respect to these components of a wireless system.

Realistic and comprehensive analytical models for a multi-layer wireless system are likely to be intractable. In this case, effective simulation becomes the most feasible alternative. NS-2 is chosen as the network simulation tool. The NS-2 Simulation Testbed models include the IETF rSerPool protocols, namely, Endpoint Name Resolution Protocol (ENRP) and Aggregate Server Access Protocol (ASAP). To enable both unicasting and multicasting for communication between server pool elements (PEs), users (PUs), and registrar agents (ENRP servers), MAODV was integrated into the testbed. Dynamic and proactive selection of Home Servers and PEs in FCS environment, failure detection and handling in FCS environment, sharing session states (to facilitate switchover) and special cases of switchover in wireless environment are among the main topics for NS-2 Simulation Testbed.

Among the capabilities of our NS-2 Simulation Testbed are movement pattern selection (frequency, speed, etc.), transmission pattern selection (antenna model, transmission range, etc.), multicast/unicast among PEs, PUs and ENRP servers, pool name resolution, pool (de)registration, PE failure detection by timers, ENRP server failure detection, application transparent switchover (due to failures, PE deregistrations, etc.), ENRP home server hunt for PEs and PUs, and home server and PE selection based on different policies.

The initial results show significant differences between designs for wired (the IETF architecture) and wireless environments. For example, the constant movements of nodes dominate the communication failures in a wireless environment. This type of failure is different from a typical wired network failure (e.g., node hardware failure, operating system failure, or severe link/route failure).

A set of metrics to be extracted and analyzed in experiments focus on the tradeoffs between performance, control traffic overhead, and gains from the increased server availability. The metrics include the number of data and control packets transmitted per data packet delivered, time between session failures, time between PE's reregistration with a new ENRP server, PE utilization, rejection ratio of new sessions, number of switchovers per session, and success ratio of switchovers (i.e., percentage of sessions "rescued" thanks to the deployment of reliable server pools).