Adaptive Resilient Tactical Network Management

R. G. Cole, S. Kumar[†], A. Mishra[†], and B. Awerbuch[†]*

**JHU Applied Physics Laboratory, Baltimore, MD; and*
[†]JHU Department of Computer Science and Engineering, Baltimore, MD

Our objective is to develop an enhanced verification and validation capability for configuration management of devices and information networks, building upon the Internet Engineering Task Force's (IETF's) NETCONF[1] protocol and the YANG[2] modeling language. A more robust validation and a new verification capability for configuration management can greatly improve the overall reliability of computer networks by reducing misconfiguration causing service interruptions. Network scenarios that will benefit from these improved verification and validation methods include the following:

- Wired Networks—Often these networks support separate out-of-band management networks and manual repair to maintain a robust management capability. Our work will result in higher service reliability and lower operating costs.
- Wireless Mobile Ad Hoc Networks (MANETs)—Often wireless MANETs necessarily perform configuration management over the wireless channel. Misconfiguration can isolate the nodes from the network and force manual reconfiguration.
- Disruption-Tolerant Networks (DTNs)—The autonomous operation of remote vehicles demands a more resilient configuration management model to mitigate misconfiguration.

Standards-based configuration management relies on the IETF's Simple Network Management Protocol (SNMP)[3] for management protocol exchanges and Structure of Management Information version 2 (SMIv2)[3] for managed device modeling (i.e., management information base or MIB). SNMP does not support a means to specify general validation checks, and it has no means to specify verification of running configuration. Hence, most operators rely on manual methods (or scripting) to manipulate device configuration through out-of-band access. This option is not viable for management of tactical or critical network services requiring high reliability and performance, such as those anticipated in MANET and DTN deployments. The IETF is developing a new configuration management protocol, NETCONF. NETCONF allows limited validation checking of configuration, but it does not allow[1] the server to perform methods to verify proposed configuration changes to running configuration on remote devices.

Our research program was initiated to address these shortcomings. We have developed a software-defined radio (SDR) packet radio network platform based on the GNU Radio open-source software program (see Fig. 1). We are using this testbed to prototype and evaluate our methods to improve current configuration management. We have developed a network layer and management software (NETCONF client and servers) in the Practical Extraction and Report Language (PERL) as a means to perform rapid prototyping of our research ideas. We

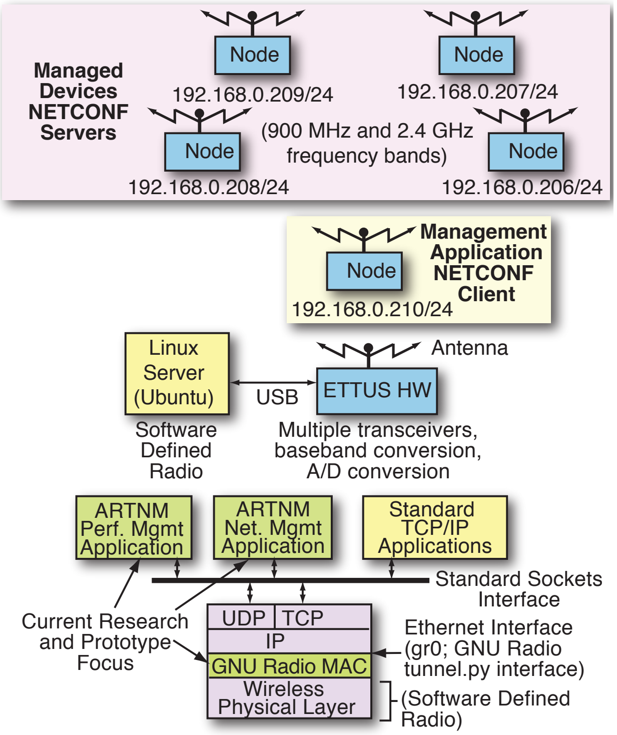
Managed Devices NETCONF Servers
Node
192.168.0.209/24
Node
192.168.0.207/24
Node
192.168.0.208/24
(900 MHz and 2.4 GHz frequency bands)
Node
192.168.0.206/24
Management Application NETCONF Client
Node
192.168.0.210/24
Linux Server (Ubuntu)
Antenna
USB
ETTUS HW
Software Defined Radio
Multiple transceivers, baseband conversion, A/D conversion
ARTNM Perf. Mgmt Application
ARTNM Net. Mgmt Application
Standard TCP/IP Applications
Standard Sockets Interface
Current Research and Prototype Focus
UDP
TCP
IP
GNU Radio MAC
Wireless Physical Layer
Ethernet Interface (gr0; GNU Radio tunnel.py interface)
(Software Defined Radio)

Figure 1. GNU Radio prototyping network.

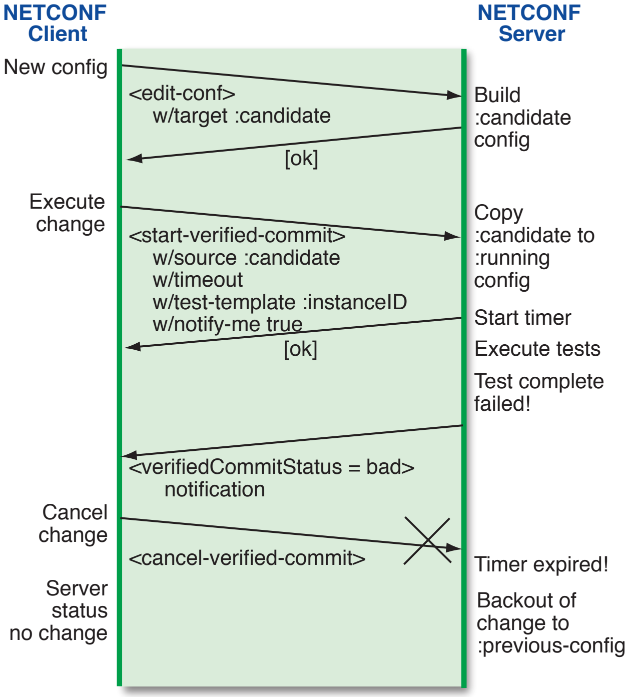
NETCONF Client
NETCONF Server
New config
<edit-conf> w/target :candidate
Build :candidate config
[ok]
Execute change
<start-verified-commit> w/source :candidate w/timeout w/test-template :instanceID w/notify-me true
Copy :candidate to :running config
Start timer
[ok]
Execute tests
Test complete failed!
<verifiedCommitStatus = bad> notification
Cancel change
<cancel-verified-commit>
Timer expired!
Server status no change
Backout of change to :previous-config

Figure 2. Example of robust verify and backup.

have developed and prototyped the following improved methods:

- Generalized validation checking through syntax, constraints, and policy documents
- Generalized verification testing by explicitly involving the managed device and defining means to specify the verification tests and associated acceptance criteria
- Generalized verification testing by defining methods that allow simultaneous network-wide configuration management

Figure 2 shows an example of our more robust configuration management capabilities. Here the client requests that the server (the remote managed device) reconfigure aspects of its network interface and follow up with a set of active measurements to determine the correctness of the new configuration. The server reports these results back to the client, which is responsible for issuing the final commit to the server. In the event of failure of measurements, or failure of connectivity, the server is designed to always back out to the previous correct state. This process is illustrated at the bottom of the diagram in Fig. 2.

We will continue our experiments and investigations of this new technology. Future focus areas include developing more autonomy in remote device management; new, network-wide, upgrade capabilities; and more efficient transport and operations bundling for operations over DTN networks.

For further information on the work reported here, see the references below or contact robert.cole@jhuapl.edu.

[1] Enns, R., (ed.), *NETCONF Configuration Protocol*, Internet Engineering Task Force (IETF) RFC 4741, http://rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=4741&type=http&file_format=pdf (Dec 2006).

[2] Presuhn, R., Case, J., McCloghrie, K., Rose, M., and Waldbusser, S., *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*, Internet Engineering Task Force (IETF) RFC 3416, http://rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=3416&type=http&file_format=pdf (Dec 2002).

[3] McCloghrie, K., Perkins, D., and Schoenwaelder, J., *Structure of Management Information Version 2 (SMIv2)*, Internet Engineering Task Force (IETF) RFC 2578, http://rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=2578&type=http&file_format=pdf (Apr 1999).