TECHNICAL REPORT 1978
February 2009

Advanced Conveyance Security Device System Scalability Assessment

Combined 802.15.4 and IP Network Simulation

Sarah M. Lauff
Douglas S. Hulbert
Ayax D. Ramirez
Russ E. Clement
Stephen L. Childress

SSC Pacific

TECHNICAL REPORT 1978
February 2009

Advanced Conveyance Security Device System Scalability Assessment

Combined 802.15.4 and IP Network Simulation

Sarah M. Lauff
Douglas S. Hulbert
Ayax D. Ramirez
Russ E. Clement
Stephen L. Childress

Approved for public release;
distribution is unlimited.

SPAWAR
Systems Center
PACIFIC

SSC Pacific
San Diego, CA 92152-5001

SSC PACIFIC
San Diego, California 92152-5001

M. T. Kohlheim, CAPT, USN
Commanding Officer

C. A. Keeney
Technical Director

ADMINISTRATIVE INFORMATION

The work described in this report was performed for the U.S. Department of Homeland Security by the Advanced Technology Branch (Code 55430), SPAWAR Systems Center Pacific.

Released by
A. D. Ramirez, Head
Advanced Technology Branch

Under authority of
S. Russell, Head
Electromagnetics and
Advanced Technology
Division

QualNet® is a registered trademark of Scalable Network Technologies, Inc.
OPNET® is a registered trademark of OPNET Technologies, Inc.

LH

CONTENTS

Figures

Tables

EXECUTIVE SUMMARY

With the goal of improving security for shipping containers in the global supply chain, the Department of Homeland Security (DHS) is developing technical requirements for components that comprise the Conveyance Security Device (CSD) System. Working under DHS oversight and with a multi-agency team, Space and Naval Warfare Systems Center Pacific (SSC Pacific) is conducting and documenting field tests, analysis, and demonstrations with Sandia National Laboratories to investigate the capability of potential Advanced Conveyance Security Device (ACSD) technologies to meet container monitoring and communications performance thresholds needed for global implementation of the ACSD systems.

This report demonstrates the capability of a commercially available network simulation package, and uses the star topology to model heterogeneous networks with both wireless and wired subnets to

- predict achievable performance for ACSD technology over various hardware and protocol implementations, and
- corroborate test results from applicable field tests and demonstration efforts.

The report also discusses prospective efforts to employ the simulator to

- develop optimal power-management strategies for battery-operated sensing and wireless communications devices mounted on cargo containers, and
- identify approaches to use the simulator to manage the implementation of particular ACSD systems, assessing factors such as placement of readers, movement of containers, radio frequency (RF) impairments, and potential obstacles to assured and timely ACSD system operation.

1. BACKGROUND

In recent years, industry and government agencies have investigated ways to improve security in the global supply chain in an effort to protect against criminal activity and terrorist attacks. For cargo containers, this effort has included developments to improve mechanical and electronic container seal technology and to develop sensor systems, inspection agreements, and processes to identify and monitor cargo movement at major ports and transit points worldwide. With adequate sensing and reporting capabilities, automated and persistent container security could become integral to the global supply chain.

DHS has developed requirements for components of the Container Security Device (CSD) System to monitor intrusion via the doorway and breaches of ISO 668 Dry Shipping Containers and conveyances while in transit from a point of stuffing, through designated intermediate transit points, and then to termination points within the United States. For shipping containers, the ACSD objectives are intended to align technical requirements to the greatest extent possible with the CSD program while providing for

- detection of container breaches and unauthorized door openings,
- multi-modal tracking capability for inbound cargo shipments, and
- improved interdiction and targeting of cargo across the supply chain.

To track the status of an individual conveyance, the current CSD concept employs a battery-operated security device that resides within the container and that is capable of wireless communications to Readers located at strategic waypoints. These Readers, using well-defined protocols, receive the binary data from the ACSD as the conveyance passes and forwards them to a centralized server referred to as a Data Consolidation Point (DCP) over the public Internet. Because multiple conveyance devices could seek to report simultaneously, a standardized multiple access (MAC) protocol must be enforced to ensure global interoperability. Here, “multiple access” refers to a protocol that offers a large number of reporting nodes a way to send and receive in close proximity and on one radio frequency or a small range of frequencies.

Available standards for MAC protocols are maintained by the Institute of Electrical and Electronics Engineers (IEEE) and include identifiers such as 802.11, 802.15.4, and 802.16. DHS has chosen to enforce the IEEE 802.15.4 standard for the ACSD System, in part because its requirement for relatively low data rates does not appear to impinge on ACSD System performance, yet enables long battery life (months or years) and minimal complexity. When an ACSD is within reliable (low frame error rate) range of a Reader, it is able to transfer its status and data to the Reader after first executing a prescribed association and guaranteed time slot (GTS) request process of messages defined by the IEEE 802.15.4 standard and receive command messages from the DCP.

2. INITIAL SIMULATION TASK

In the summer of 2008, our initial objectives were to choose a simulation tool, exercise the tool, register its outputs against field test results [1], and begin an assessment of IEEE 802.15.4 specifications as a suitable background standard to guide the development of the ACSD System.

We chose a particular event simulator, one with modeling details that include departure and arrival times for each communications packet as it traverses the nodes of a network under study. This discrete event simulator registers variations in packet arrival patterns with respect to changes in factors such as propagation environment, media access protocol, buffer sizes, and routing protocols. Among available candidates, QualNet® was our choice. QualNet is known for accuracy, clarity of display in real time, and ability to scale up to large networks. Its facility with large networks is based on code designed to run on single- or multi-core processors: “The QualNet simulation engine is extremely scalable and can accommodate high-fidelity models of networks of thousands of nodes. QualNet makes good use of computational resources and models large-scale networks with heavy traffic and mobility in reasonable simulation times” [2]. Another simulator that we could have chosen was OPNET®. While both OPNET and QualNet are discrete event simulators with strong track records, QualNet was more compelling in the simplicity of its wireless networking interface and in the convenience of training and consulting services from its parent company, Scalable Network Technologies, Inc.

2.1 VARIATIONS IN THROUGHPUT WITH RANGE

Our first exercise was to create a simple 802.15.4 star topology scenario in the simulator to find the maximum range of the Reader to ACSD and how the maximum range changes based on the propagation limit and velocity of the ACSD as it passes the Reader. For this simulation, the variables were 10-mW transmission power, 0-dB antenna gain on the transmitting antenna, and 5-dB antenna gain for the receiving antenna. The antenna height for both the transmitting and receiving antenna is 0.3 m. We use 10 mW for transmission power because it satisfies power limitations on commercial equipment for a large number of countries.

Vehicle speed does not have technical issues such as Doppler errors due to the nature of 802.15.4. Speed does affect time-in-coverage and thus network discovery time. For this example, a single data frame of 64 bytes was sent with a frequency of 2.4 GHz at 250 kb/s. The ideal situation is for the ACSD to continuously be in the line of sight of the Reader, which would give a propagation limit of -92 dBm to -96 dBm. However, most instances of transmitting will not be line of sight. Therefore, lower propagation limits have been provided to show the differences the amount of loss makes. These lower propagation limits also address the issue of link budget. In Table 1, DNR stands for "Did Not Receive," which means the propagation limit was too low (-46 dbm) at velocities of 10 m/s, 15.7 m/s, 10 m/s, and 25 m/s for the data to be read. As represented in Table 1, the propagation limit seems to be the variable that affects the range the most. Using a free-space model of propagation loss, the data in Table 1 lead to a conclusion that ACSD requirements for range and relative velocity are easily satisfied under our targeted operational conditions. However, QualNet engineers have developed more complex models of environmental effects that might be incorporated into our simulations to more accurately assess RF impairments within ACSD systems.

Table 1. Maximum separation (meters) vs. propagation limit and relative velocity.

Propagation Limit	**Velocity 0 m/s**	**Velocity 5 m/s**	**Velocity 10 m/s**	**Velocity 15.7 m/s**	**Velocity 20 m/s**	**Velocity 25 m/s**
-96 dBm	106	106	106	106	106	105
-95dBm	100	100	100	100	100	100
-94 dBm	94	94	94	94	94	93
-93dBm	89	89	89	89	89	88
-92dBm	84	84	84	84	84	83
-86 dBm	59	59	59	59	59	59
-76 dBm	33	33	33	32	32	32
-66 dBm	18	18	18	18	18	18
-56 dBm	10	10	10	10	9	9
-46 dBm	3	3	DNR	DNR	DNR	DNR
-36 dBm	1	DNR	DNR	DNR	DNR	DNR
-26 dBm	DNR	DNR	DNR	DNR	DNR	DNR

2.2 SHIPPING SCENARIO

The shipping scenario focuses on an ACSD requirement to initiate and complete data transfer to a Reader while moving at 15.7 m/s with respect to the Reader [3]. Within the scenario, an ACSD moves into and out of the range of a Reader as data flows from the ACSD, to the Reader, to a DCP; then, an acknowledgement returns over the same two hops. See Figure 1.

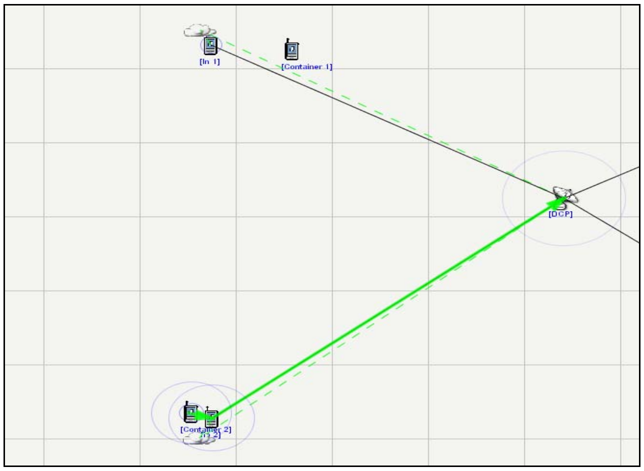

Figure 1. Single CSD-to-Reader range scenario.

Since distance and propagation limit are factors in the success of collecting data, we decided to use a propagation limit of -92dBm. From this, it was determined that a container moving 16.6 m/s with a closest point of approach (CPA) of 10 m was able to send all of its data. In addition, a second container moving at 10 m/s had a successful exchange while traversing a CPA of 60 m, which shows that the devices do meet specified requirements.

2.3 REPORT AND ACKNOWLEDGEMENT WITHIN 2 SECONDS

One requirement expressed in more than one source [1, 3] is that report and acknowledgement data must successfully traverse a loop from the ACSD to the Reader, then to the DCP, and back along the reverse two-hop path within 2 seconds.

The first objective was to determine how many containers could send their data to the DCP simultaneously and still have the data collected in under 2 seconds using the star topology. There are two methods to determine this. In the first method, each ACSD communicates with a separate Reader, and then these Readers contend for access to the DCP; see Figure 2.

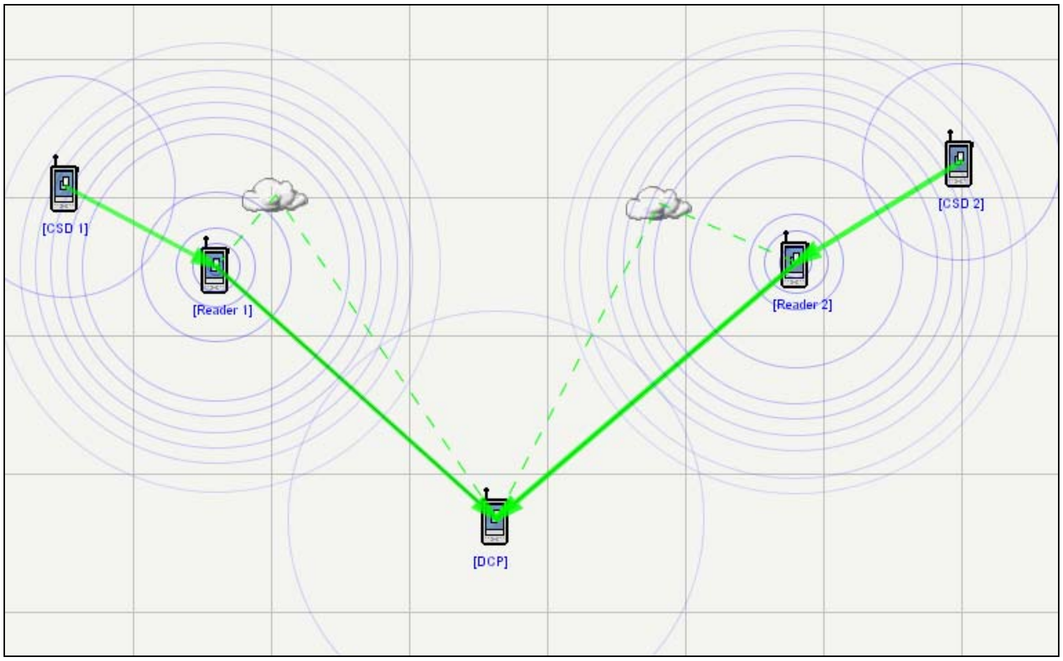

Figure 2. Multiple CSD-to-Reader range scenario.

For this scenario, data transfers from ACSD to Reader are over 802.15.4 wireless links, while Reader-to-DCP transfers are over a wired Ethernet connection at 100 Mbps. To estimate the total duration of a transaction involving multiple nodes, the average time was taken. Table 2 gives the results for different data rates and number of contending ACSDs. These times also include network discovery, which is the dominant element in latency. Each discovery time in Table 2 is an average over several runs. Figure 3 plots and interpolates the data from Table 2.

Table 2. Durations of the report-acknowledge sequence (seconds).

Wireless Link Rate CSD Count	20 kb/s	40 kb/s	100 kb/s	250 kb/s
1	2.577	1.0984	0.2837	0.166
5	2.8122	1.1092	0.3434	0.2287
10	3.1252	1.153	0.3716	0.2941
15	3.9063	1.5969	0.6062	0.5812
20	4.4466	3.2988	1.3909	1.3905

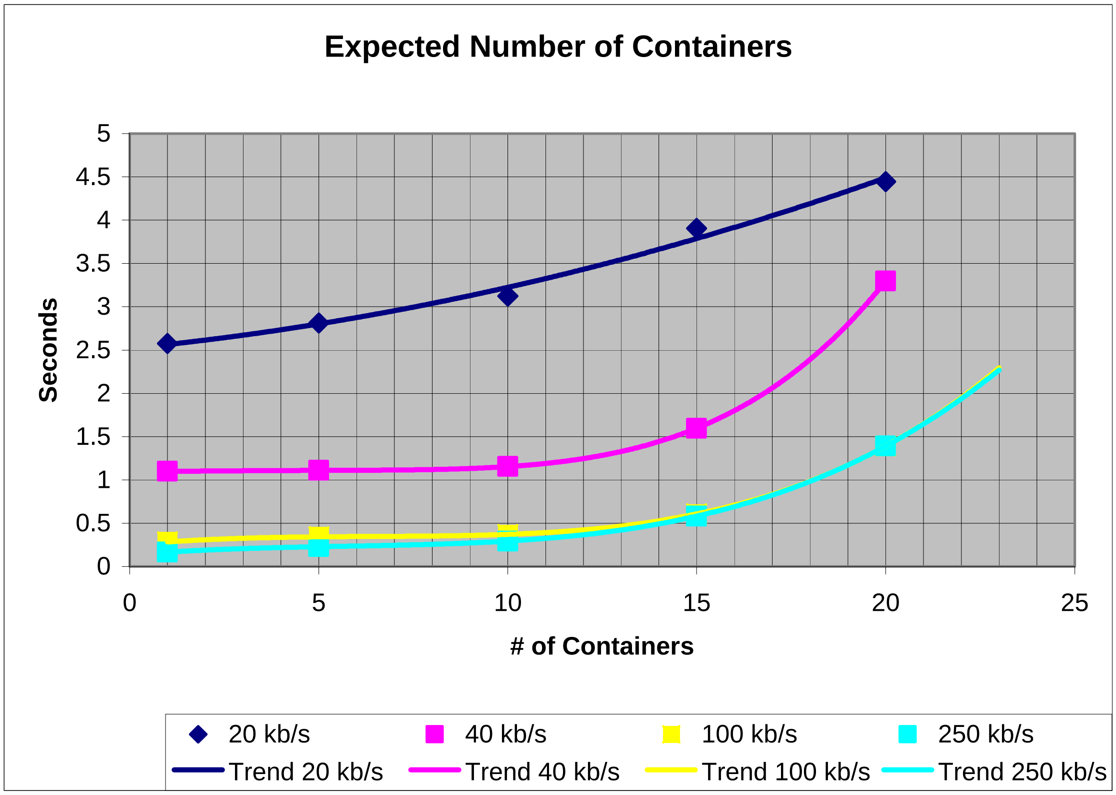

Figure 3. Interpolated duration of the report-acknowledge sequence.

For this analysis, the propagation limit did not affect the data. The table and graph clearly show that the larger the data rate is, the less time it takes. Also, we can see that using more containers increases the amount of time needed for data to be transferred. A data rate of 20 kb/s will never transfer information in less than 2 seconds. A data rate of 40 kb/s seems feasible as long as there are fewer than 15 containers sending at the same time. Obviously, the data rates of 100 kb/s and 250 kb/s are the best choices. The graph shows that the 100 kb/s and 250 kb/s data rates should reach the 2-second mark when about 22 containers are sending their data simultaneously. It should be noted that these times do vary based on the speed of the Ethernet connection, routing protocol, and even the distance between the ACSD and Reader. These data are important because they show, for each data rate, the number of containers that can transfer data simultaneously and still keep to the requirements.

In the second method, multiple ACSDs can try to send to the same Reader, and then the Reader sends the data to the DCP (see Figure 4). This follows the star topology, where the ACSDs do not share data with each other.

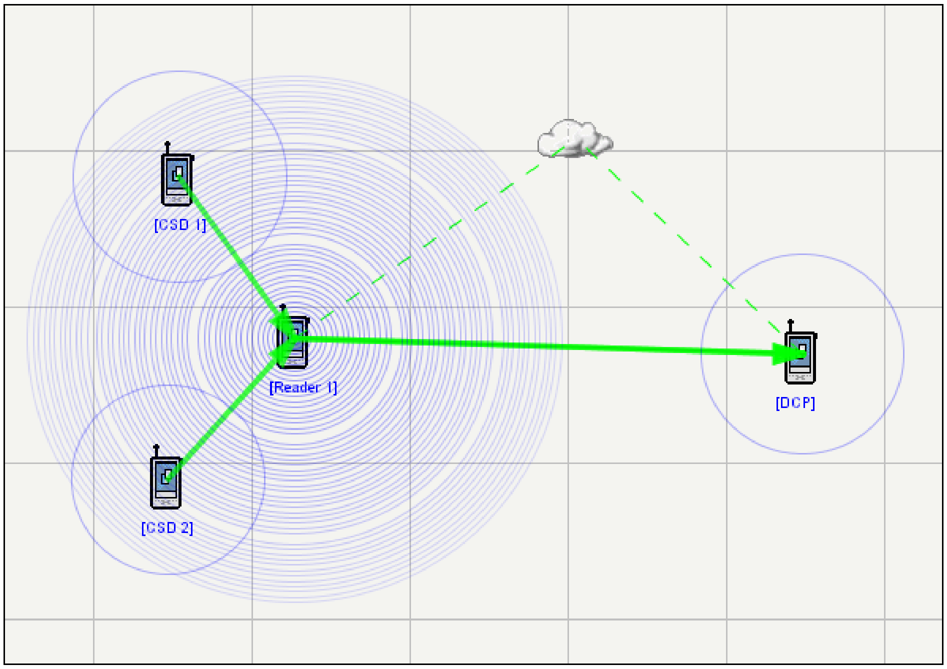

Figure 4. Multiple CSDs-to-reader scenario.

For two ACSDs to send data through a single Reader, they must first compete for time with the Reader. Non-beacon-enabled networks use a carrier sense multiple access (CSMA) protocol to transmit data. For beacon-enabled networks, data can be sent two ways: slotted CSMA and GTS. The time between beacons is divided into 16 sections in which there is a Contention Access Period and a Contention Free Period, as shown in Figure 5.

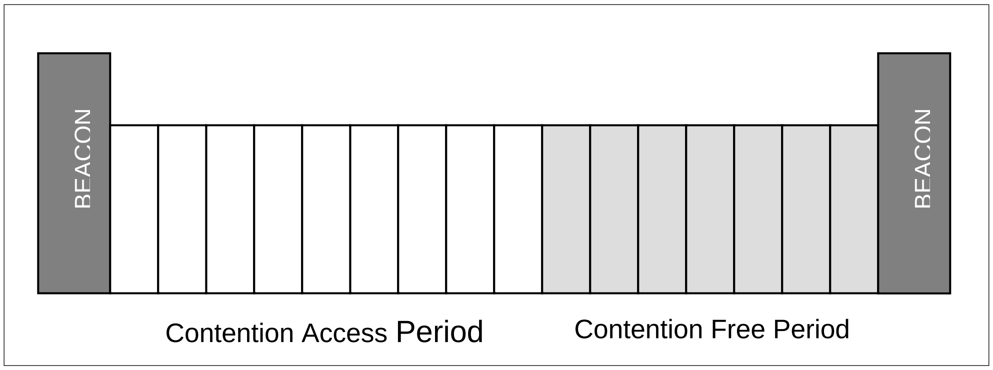

Figure 5. Beacon frame slot allocation.

The slotted CSMA lies in the Contention Access Period, while the GTS portion lies in the Contention Free Period. Note that the 802.15.4 specification allows for variable apportioning of available time slots to these two periods within the beacon frame. The Reader can choose how much time should be allotted to each section. In the slotted CSMA, the ACSD will send the data at the beginning of a time slot. If contending ACSDs choose the same leading edge of a time slot to send their data, their packets collide (interfere) with one another at the input to the Reader. When a collision occurs, each ACSD chooses a random number of time slots before attempting to re-send its packets, called a back-off period. This method allows algorithms for generating random numbers to mediate contending flows, but the lack of a centralized decision process necessarily decreases collective throughput. “If there is a Contention Free Period, all contention-based transactions must be completed before the first allocated slot begins” [4].

GTS protocols differ from the other protocols in that they allot a dedicated set of time slots in each beacon frame. The protocol requires that each ACSD with a message to send first contact the Reader to request GTS. Then, the Reader will respond back with a specific time in which the ACSD can send data. The GTS protocol may take longer to transmit data because of all of the requests and responses, but it guarantees contention-free access to the channel.

Since QualNet does not have the option of modeling GTS, this second method cannot be fully completed. QualNet can send data in either slotted or unslotted Carrier Sense Multiple Access with Collision Assurance (CSMA-CA). With CSMA-CA, a station wishing to transmit must first listen to the channel to check for any activity on that channel. If no other stations are transmitting, then it will transmit. If the channel is busy, then it must wait. Once the channel is clear, the station will send out a signal telling all others not to transmit and then sends its packet. The slotted CSMA-CA is very similar to the Contention Access Period of the GTS. With both of these protocols, the data will always be sent; it is just a question of how long it takes for all of the data to be sent. Table 3 gives the time it takes for a certain number of ACSDs to send their data to the Reader using unslotted and slotted CSMA-CA at a frequency of 2.4 GHz. Since GTS only allows for a maximum of seven ACSDs to be reserving slots to send in, these two tables only look at the rates for a maximum of seven containers sending. Also given are the best and worst case scenarios for slotted and unslotted. In QualNet, slotted CSMA-CA is known as beacon-enabled mode, while unslotted CSMA-CA is known as non-beacon-enabled mode. For this scenario, the amount of time for the Reader to send to the DCP is not included because it is negligible.

Table 3. Slotted and unslotted CSMA-CA simulation (seconds).

# of CSDs	Slotted CSMA/CA		Unslotted CSMA/CA		
	Best Case	Worst Case	Polling	Not Polling	Worst Case
1	0.05	0.05	0.06	0.07	0.07
2	0.08	0.08	0.13	0.13	1.34
3	0.12	0.12	0.32	0.9	1.37
4	0.14	0.15	0.57	1.03	1.37
5	0.17	0.17	0.96	1.89	4.13
6	0.20	0.39	1.08	1.92	5.13
7	0.24	0.79	1.64	2.33	5.38

In reference to polling, QualNet states: “This parameter specifies the polling time (in seconds) used by an RFD to check for pending data in non-beacon enabled scenarios. This parameter is optional. If this parameter is not specified, the default behavior is not to poll" [5]. Both sets of data are included for informational purposes.

Even though QualNet’s beacon-enabled mode does not exactly match the requirements for a correct sending, the results indicate that a large difference exists between the number of ACSDs that can be read in non-beacon-enabled mode to the number in beacon-enabled mode.

From looking at this information compared to the results of separate Readers above, it seems that having one Reader collect data from multiple ACSDs and then sending to the DCP would be the most efficient way to meet the requirements of sending data within the 2 seconds and would be cost-appropriate.

2.4 LATENCY RESULTS FROM FIELD TESTS BY SSC PACIFIC AND SANDIA NATIONAL LABORATORIES

Another way that we tested the 2-second rule was by using the experimental data provided by Sandia to see if data could be sent over an intricate path in the required time. In September of 2007, SSC Pacific and Sandia conducted an experiment in which data were sent from Albuquerque, New Mexico, to San Diego, California. The goal of this research was to use QualNet to simulate the events that occurred during this experiment and determine if the data collected from QualNet were comparable to the data collected from the Sandia experiment.

In this experiment, data were first sent from a microprocessor to an antenna (the ACSD). From there the antenna sent the data wirelessly, using 802.15.4, to a Reader, which then transferred the data to a controller. The data were then sent to one network and then through the Internet to another network. Finally, the data were sent to the San Diego DCP, which sent an acknowledgement back to the original microprocessor. Figure 6 is a diagram from the latency document [1] of the route.

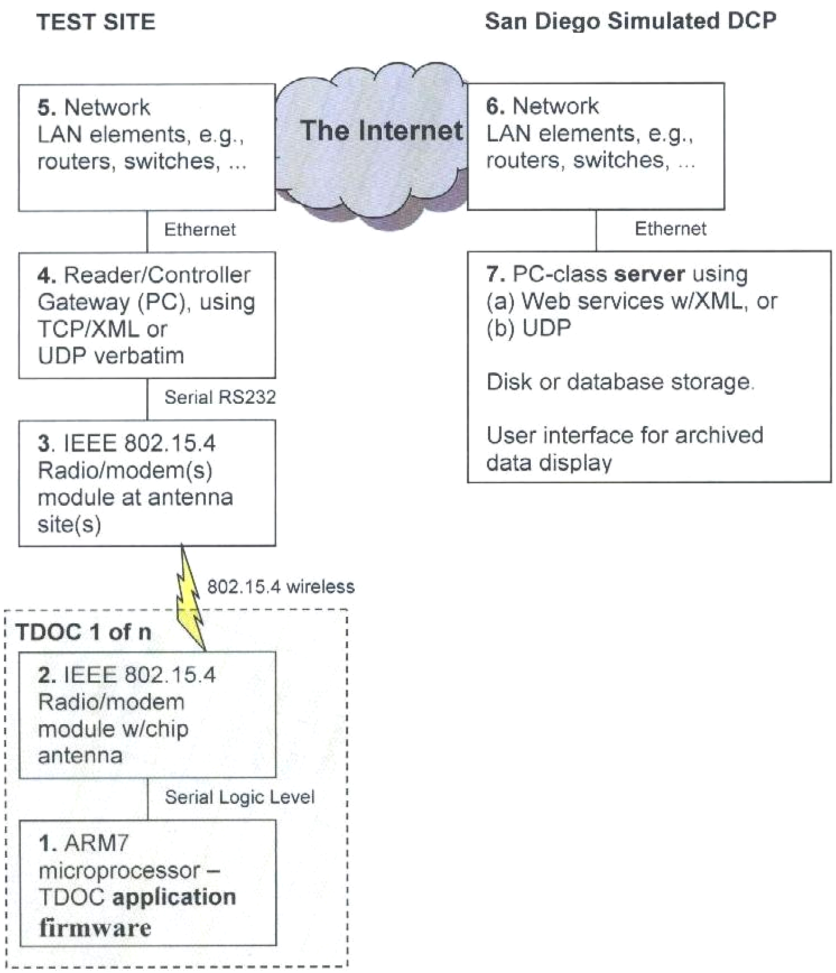

Figure 6. Concept model for latency test.

This first section of data looks at the transmission times for sending a single packet of 74 bytes from the microprocessor to the DCP, and then having the DCP send an acknowledgement packet of 16 bytes back. In Table 4, the first column indicates what step in the transmission is being taken. The document, AODV B, and AODV nB columns give the amount of time it took for the data to transmit over the steps. AODV B is the scenario created with the AODV routing protocol and using beacons. AODV nB is the same scenario but non-beaconing. Finally, the “% Error” column tells how far off the data are based on

% Error= 100 x (estimated-actual)/actual

where the document is the actual and the QualNet simulations provide the estimated. The total sections at the bottom indicate the round-trip time for data to be sent.

Table 4. QualNet comparison to the Sandia test.

	Document (s)	**AODV B (s)**	**Error (%)**		**AODV nB (s)**	**Error (%)**
Encrypt	0.01					
Step # 1 1 -> 2	0.0405	0.0552	36.29		0.0552	36.29
Step # 2 2 -> 3	0.0024	0.0068	183.33		0.0048	100.00
Step # 3 3 -> 4	0.0405	0.0552	36.29		0.0552	36.29
Step # 4 4 -> 7	0.1566	0.1566	0.00		0.1566	0.00
Step # 5 7 -> 4	0.1566	0.1562	0.26		0.1562	0.26
Step # 6 4 -> 3	0.0405	0.041	1.23		0.041	1.23
Step # 7 3 -> 2	0.0024	0.0215	795.83		0.5016	20800
Step # 8 2 ->1	0.0405	0.041	1.23		0.041	1.23
Total 1	0.1668	0.2207	32.31		0.6988	318.94
Total 2	0.48	0.5335	15.31		1.0116	110.63

Total 1 - excludes Wakeup, Network Discovery, and Internet.

Total 2 - excludes Wakeup and Network Discovery.

Figure 7 shows the QualNet comparison to the Sandia test.

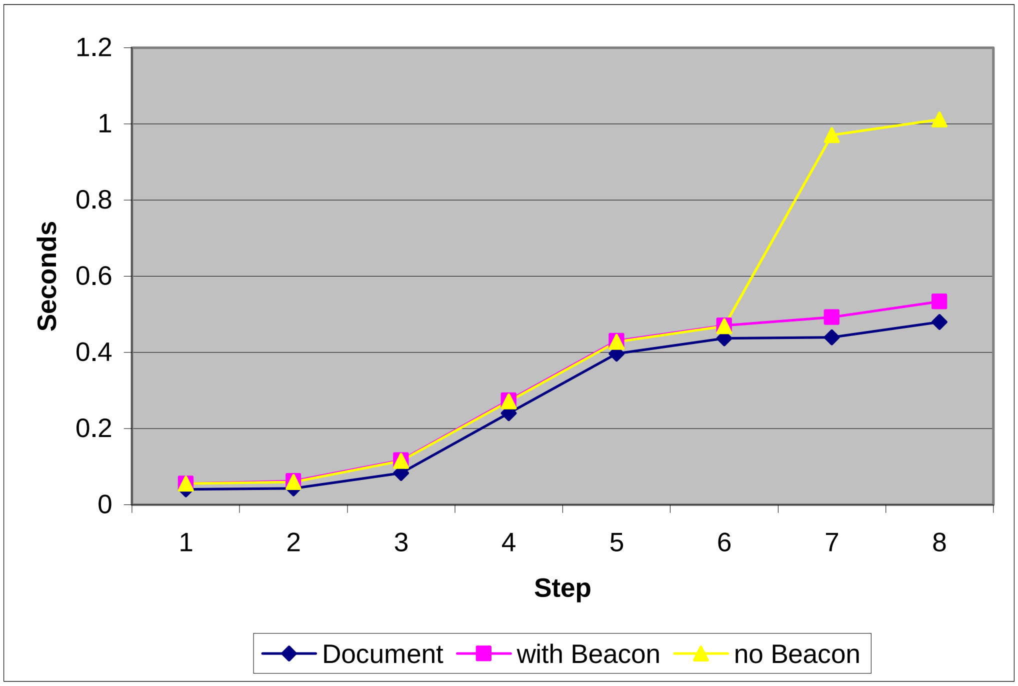

Figure 7. QualNet comparison to the Sandia test.

These first two totals do not include initial network discovery because it can vary dramatically depending on whether it is in beacon or non-beacon mode and how many channels must be scanned. However, from these data it seems that the AODV B is within a reasonable amount of error from the Sandia data. Note that the non-beacon-enabled mode was actually very close until the Reader had to relay the acknowledgement back to the ACSD. This, and this alone, is the reason the non-beacon-enabled mode is so off at the end. This large increase also agrees with the previous idea that non-beacon-enabled mode is not beneficial because it is not as reliable.

This next section of data looks at the network discovery times. As stated above, the times recorded are very different because of the varying parameters. The first three rows of Table 5 give the amount of time a Reader would spend on a channel based on whether it is beacon-enabled or not. The next four rows provide the Sandia data for network discovery. A1 is to be read as the amount of time it takes for network discovery for the Reader to scan 16 channels in beacon mode. Note that for these data, the times for network discovery are not for the time of total network discovery, but only the time it takes for the 802.15.4 portion to complete its share of network discovery. Finally, the columns provide the values and how they were found.

Table 5. Sandia's channel time (seconds).

Lab Data	Value		Equation	
Beacon interval	0.06144			
Channel dwell time (for beacon):	0.13828		0.06144*2+ .0154	Beacon interval and the typical 802.15.4 return time
Channel dwell time (no beacon):	0.01636		.001536+.001	Time per a channel plus tuning delay
A1. 16 channels w/ beacon	2.21248		0.13828*16	Channel dwell time *16
A2. 4 channels w/ beacon	0.55312		0.13828*4	Channel dwell time *4
B1. 16 channels, no beacon	0.2624		16*(0.01636)	Channel dwell time *16
B2. 4 channels, no beacon	0.0656		4*(0.01636)	Channel dwell time *4

With the QualNet data, the number of channels being scanned is not specified. However, by finding QualNet's values for network discovery time and comparing them with the Sandia data, given in Table 6, we attempted to determine the number of channels being scanned. The row labeled "2 nodes, with beacon" indicates the data when only looking at the network discovery times between the ACSD and Reader. The row labeled "All nodes/7" gives the average network discovery time per node.

Table 6. Attempt to discover QualNet’s channel time (seconds).

QualNet Data	Value		Equation	
A. 2 nodes, with beacon	0.06403		.02295+ .01283+ .01283+ .01543	Time the nodes come into contact during network discovery
All nodes/ 7, with beacon	0.169095		(2.183665-1.0)/7	(Discover end time- discovery start time)/7
B. 2 nodes, no beacon	0.30767		.25447+ .02275+ .01864+ .30767	Time the nodes come into contact during network discovery
All nodes/7, no beacon	0.249473		(2.746309-1.0)/7	(Discover end time- discovery start time)/7

Unfortunately, the QualNet data do not exactly match the data from Sandia. The amount of time for discovering with a beacon is extremely small compared to that of Sandia. However, by looking at the non-beaconed network discovery, it seems that QualNet data are the most similar to those of a 16-channel non-beaconed scan.

The Test Report on CSD-DCP Latency [1] shows that using beacons for network discovery takes more time than not using beacons. In QualNet, however, it seems that network discovery with beacons takes less time. We feel that the major difference between Sandia’s data and QualNet’s data for discovering with beacons is due to the fact that QualNet does not have GTS, which is an integral part of the beaconing system. Without GTS, QualNet seems to be automatically discovering its network and, therefore, causing the amount of data with beacons to be very small.

3. CONCLUSIONS

The CSD/DCP round trip latency is determined primarily by the following:

1. Network discovery time in the ACSD, where this depends on the choice of beaconed superframe/GTS versus beacon-request, and how many RF channels must be scanned. Reference [3] details this.
2. Latency of the wide area network connecting the DCP.
3. In the ACSD program’s at-portal-only connectivity assumption, and driven by battery life constraints, network discovery time, and low-power-sleep time strategies must be appeased.

The data found through working on QualNet show that the 802.15.4 meets the requirements specified in [6, 3, 7] and is able to mimic the results of experiments. Even though QualNet is a newer simulation tool, it still seems very reliable and efficient for creating simulations. These data have shown that QualNet, with the exception of GTS, is a sufficient tool. The first part of the SSC Pacific/Sandia experiment shows that QualNet can be extremely accurate. The second part shows that there are still parts of QualNet that need to be created in order for our simulations to run perfectly. Two negative aspects of QualNet are the absence of GTS and the fact that the ACSD does not send its information in response to the Reader. Not having GTS makes the times for sending data a bit inaccurate.

Also, the simulations do not follow the exact steps of the specifications. One requirement of the 802.15.4 is that “the ACSD transmits data to the ACSD Reader only in response to beacon assigned GTS assigned to the ACSD” [6]. Since QualNet only has a simple structure for sending information, it does not cover this requirement. Therefore, we need for this part of the program to be created for those data to be correct.

4. REFERENCES

1. SSC Pacific, “CSD Communications Test Report on CSD-DCP Latency and Multi-Lane Portal Wireless Range, Version 1.7,” Space and Naval Warfare Systems Center Pacific (SSC Pacific), San Diego, CA, and Sandia National Laboratories, 15 November 2007.
2. Scalable Network Technologies, Inc., “QualNet Product Families,” http://www.scalable-networks.com/pdf/QualNet Family.pdf.
3. Department of Homeland Security, “Container Security Device (CSD) CSD-to-CSD Reader Interface Control Document (ICD), Version 2.0,” U.S. Department of Homeland Security, Customs and Border Protection, 8 November 2007.
4. Cooklev, T. “Wireless Communication Standards: A Study of IEEE 802.11, 802.15, and 802.16.” Standards Information Network IEEE Press, New York, NY, 2004.
5. Scalable Network Technologies, Inc., QualNet 4.5-Sensor Networks Model Library, Scalable Network Technologies, Inc., Los Angeles, CA, 2008.
6. Department of Homeland Security, “Container Security Device (CSD) Reader-to-Data Consolidation Point (DCP) Interface Control Document (ICD), Version 1.0,” U.S. Department of Homeland Security, Customs and Border Protection, 2 October 2007.
7. Department of Homeland Security, “Container Security Device (CSD) Requirements, Version 4.0,” U.S. Department of Homeland Security, Customs and Border Protection, 9 November 2007.

5. BIBLIOGRAPHY

1. Bagrodia, R, et al, “An Accurate, Scalable Communication Effects Server for the FCS System of Systems Simulation Environment,” *Proceedings of the 2006 Winter Simulation Conference*, 1-4244-0501-7/06 ©2006 IEEE
2. Newton, David, CAPT, USCG. “S&T Stakeholders Conference” (Presentation), www.homelandsecurity.org/StakeholdersMay07/Pl2_Newton.pdf.
3. Petrova, M. “Performance Study of IEEE 802.15.4 Using Measurements and Simulations,” Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE, pp. 487-492.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-01-0188

1. REPORT DATE *(DD-MM-YYYY)*
February 2009

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
ADVANCED CONVEYANCE SECURITY DEVICE SYSTEM SCALABILITY ASSESSMENT: COMBINED 802.15.4 AND IP NETWORK SIMULATION

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS
Sarah M. Lauff
Douglas S. Hulbert
Ayax D. Ramirez
Russ E. Clement
Stephen L. Childress

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
SSC Pacific
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER
TR 1978

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Department of Homeland Security
Washington, D.C. 20528

10. SPONSOR/MONITOR'S ACRONYM(S)
DHS

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

This is a work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction. Many SSC Pacific public release documents are available in electronic format at http://www.spawar.navy.mil/sti/publications/pubs/index.html

14. ABSTRACT

Space and Naval Warfare Systems Center Pacific (SSC Pacific) is conducting and documenting field tests, analysis and demonstrations with Sandia National Laboratories to investigate the capability of potential Advanced Conveyance Security Device (ACSD) technologies to meet container monitoring and communications performance thresholds needed for global implementation of the ACSD systems. This report demonstrates the capability of a commercially available network simulation package, and uses the star topology to model heterogeneous networks with both wireless and wired subnets to predict achievable performance for ACSD technology over various hardware and protocol implementations, and corroborate test results from applicable field tests and demonstration efforts. The report also discusses prospective efforts to employ the simulator to develop optimal power-management strategies for battery-operated sensing and wireless communications devices mounted on cargo containers, and identify approaches to use the simulator to manage the implementation of particular ACSD systems.

15. SUBJECT TERMS

Mission Area: Communications and Networks
Advanced Conveyance Security Device (ACSD)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			S. Lauff
					19B. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	27	(619) 553–7561

INITIAL DISTRIBUTION

84300	Library	(2)
85300	Archive/Stock	(1)
85300	L. Hood	(1)
55430	S. Lauff	(120)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (1)

SSC San Diego Liaison Office
C/O PEO-SCS
Arlington, VA 22202–4804 (1)

Center for Naval Analyses
Alexandria, VA 22311–1850 (1)

Government-Industry Data Exchange
Program Operations Center
Corona, CA 91718–8000 (1)

SSC Pacific
San Diego, CA 92152-5001