Applying a space-based security recovery scheme for critical homeland security cyberinfrastructure utilizing the NASA Tracking and Data Relay (TDRS) based Space Network

Harry C. Shaw, Brian McLaughlin, Frank Stocklin, Andre Fortin, David Israel
Exploration and Space Communications Division
NASA/Goddard Space Flight Center
Greenbelt, MD, USA
Harry.C.Shaw@nasa.gov

Asoka Dissanayake, Denise Gilliand, Richard LaFontaine, Richard Broomandan, Nancy Hyunh
Exelis, Inc
McClean, VA
Asoka.Dissanayake@exelisinc.com

***Abstract*— Protection of the national infrastructure is a high priority for cybersecurity of the homeland. Critical infrastructure such as the national power grid, commercial financial networks, and communications networks have been successfully invaded and re-invaded from foreign and domestic attackers. The ability to re-establish authentication and confidentiality of the network participants via secure channels that have not been compromised would be an important countermeasure to compromise of our critical network infrastructure. This paper describes a concept of operations by which the NASA Tracking and Data Relay (TDRS) constellation of spacecraft in conjunction with the White Sands Complex (WSC) Ground Station host a security recovery system for re-establishing secure network communications in the event of a national or regional cyberattack. Users would perform security and network restoral functions via a Broadcast Satellite Service (BSS) from the TDRS constellation. The BSS enrollment only requires that each network location have a receive antenna and satellite receiver. This would be no more complex than setting up a "DIRECTTV™-like" receiver at each network location with separate network connectivity. A GEO BSS would allow a mass re-enrollment of network nodes (up to nationwide) simultaneously depending upon downlink characteristics. This paper details the spectrum requirements, link budget, notional assets and communications requirements for the scheme. It describes the architecture of such a system and the manner in which it leverages off of the existing secure infrastructure which is already in place and managed by the NASA/GSFC Space Network Project.**

Keywords-Cybersecurity; TDRS;cyberattack, Multiple Access

I. INTRODUCTION

Current experiences with cyberattacks occurring during peacetime strongly indicate that future warfare will be conducted via network attacks on US infrastructure. It is possible that a continuous state of cyberwarfare exists now and will continue to exist into the foreseeable future. Nation-states can be attacked by other nation-states as well as rogue actors, terrorist organizations or organized crime organizations. Attackers may have individuals in place ready to facilitate actions to disrupt and interdict networks, both public and private. Additionally, security vulnerabilities in the network infrastructure such as zero-day exploits, improperly installed or non-functional network security features, and social engineering attacks all increase the likelihood that attackers can and will damage the national cyber-infrastructre in an initial attack. It is necessary to have multiple strategies to recover from the initial attack and then re-establish secure network communications. Such a recovery may require that networks flush out existing data such as access control lists, X.509 certificates, PKI information and sensitive metadata and then re-establish themselves with uncompromised data. In the case of Windows Server Active Directory users, they may need to do some form of Active Directory restoral. In this paper, we will describe the Space Network infrastructure, layout a strategy for establishing a security recovery system within the confines of the Space Network, a concept of operations for re-establishing network security, and modeling results that support the concept of operations. Examples of institutions that the security recovery concept would be applicable to include:

- Institutions without an archive of critical security restoral information
- Institutions whose archives may be at risk of being compromised (e.g. public Cloud-based archives)
- Remote locations without secure access to the archive (e.g. remote power grid stations and facilities

For example, Windows Server Active Directory (AD) Certificate Services System State Backup and Restore could be fed via the Space Network. Setting up or restoring Domain Controllers using a certified copy of the AD database that has not passed the tombstone date could be accomplished and users would be required to periodically refresh the archived backups and any tools needed to accomplish restoral. Bare metal restoral

would not be recommended under this concept due to the required data volume (8-12Gbytes [1])

II. TDRS AND THE SPACE NETWORK (SN)

A. *TDRS Relay Constellation*

NASA operates a constellation of relay satellites in geosynchronous orbit to provide continuous coverage for low earth orbiting (LEO) satellites. TDRS constellation allows for a wide variety of spacecraft, balloons, sub-orbital and other vehicles to communicate to the ground regardless of whether or

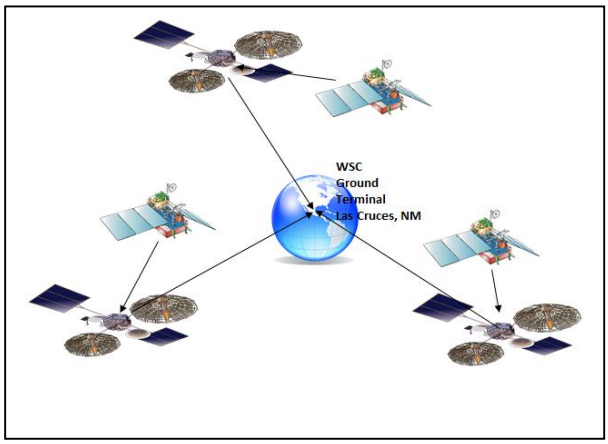

Figure 1. NASA Space Network servicing NASA customers

not the vehicle is over a ground station [2]. All of the vehicle data is returned via Ku-band link to the White Sands Complex (WSC) in Las Cruces, NM. WSC is a secure facility that resides on the White Sands Missile Range. The TDRS spacecraft are operated from WSC. NASA user data that is relayed from user spacecrafts to WSC is transmitted over a closed network to the user mission operation centers. The TDRS relay satellites and the ground stations constitute the NASA Space Network. Figure 1 depicts the basic constellation architecture. Missions such as the International Space Station, Hubble Space Telescope and the Swift Observatory relay data through the SN. In the case of ISS, the links include the data for the hosted payloads, astronaut communications and ISS-related telemetry. Fig. 2 displays the main communications systems of one generation of TDRS spacecraft.

B. *Key Attributes of the Space Network that allow for non-space applications*

Although the TDRS was designed as a relay spacecraft, it can be used in applications other than a space relay. In this paper, two of the attributes that allow this utilization will be discussed. TDRS services are specified as either forward or return services. A forward service originates on the ground from the user mission operations center and a return service originates from the user platform as shown in Fig. 3. Two important attributes are:

- S-band spread spectrum, MA forward service capability. This CDMA capability provides reduced interference for multiple users communicating simultaneously over S-band

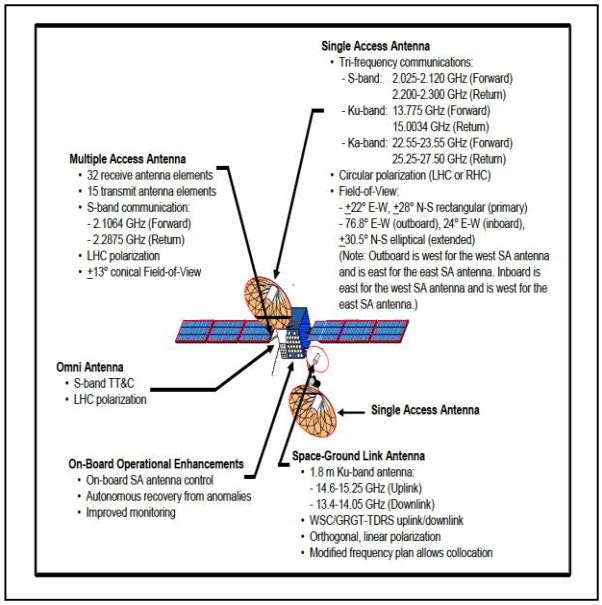

Figure 2. Second Generation TDRS spacecraft

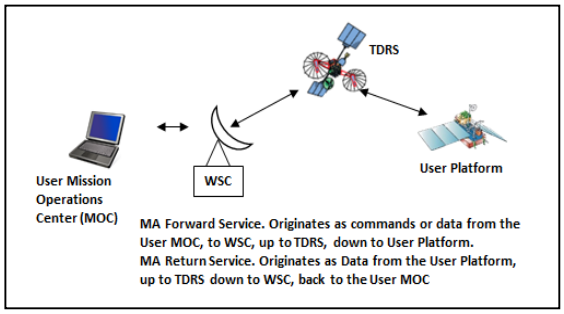

Figure 3.Multiple Access (MA) Forward and Return service definition

- The MA forward service links will close at zero altitude and are possible throughout the CONUS. The forward link is limited to 300 kbps for spread spectrum operation.

III. CONCEPT OF OPERATION

A. *System Elements*

Designated Sites. Designated Sites are locations that have been selected for emergency restart via a TDRS MA forward service. The necessary credientials and data are received over a space link from one or more TDRS spacecraft in view at the time of the emergency. The Designated Sites send their archival information periodically to Emergency Control Center for storage.

Emergency Control Center. The Emergency Control Center (ECC) resides at a physically secure location at WSC. The ECC maintains the users key information such as Certificate Authority data from the System State Backup needed to re-start secure network operations at designated sites. It may also contain other key operational data required by each designated site. From the SN perspective, the Emergency Control Center plays the role of the User MOC in Fig. 3.

Emergency Ground Station. This is the satellite ground antenna and receiver at each designated site. It could be a mobile or fixed site. The requirements for the Emergency Ground Station can be satisfied with Commercial-Off the Shelf equipment and a S-band receive antenna with 0.5m aperture size. There is no return service (no uplink) from the Emergency Ground Station and each site will be provided the coordinates for pointing the antenna. There are no tracking requirements. Given the wide variety of secure network configurations and data required, no standard implementation would be imposed upon the designated sites, except that they are recommneded to have an "air-gapped" satellite receiver and computer system for receipt of the TDRS forward link security data. Air-gapped" is defined as no network or physical link between the computer sysem downloading information from TDRS and any other computer networks. The TDRS link is a one-way half-duplex link. The Emergency Ground Station plays the role of the user platform each with a unique CDMA code.

Restoral Message Virtual Private Network. This is a dedicated, demonstrably secure, encrypted network of one-way network traffic from Emergency Ground Stations and the Emergency Control Center. The only traffic permitted on this network are Emergency Ground Station status messages and ack/nack messages confirming/denying successful data reception from the Emergency Ground Station to the Emergency Control Center over the TDRS MA forward service. Traffic between Emergency Ground Stations and any other network noded should be prohibited (or highly restricted)

B. Basic Concept of Operations

- A cyberattack on elements of the national infrastructure occurs and the network infrastructure is taken off-line.
- The Designated Sites start-up the Emergency Ground Stations and sends an encrypted message indicating on-line status
- Upon receipt of proper authorization, the Emergency Control Center creates a MA forward message queue for transmission of restoral basis data to all the designated sites and notifies the SN.
- Using a new service concept called MA Fast Forward, the SN schedules one or more TDRS spacecraft for MA forward and transmits the restoral information to each Emergency Ground Station. The SN will operate single forward links via the appropriate TDRS spacecraft(s) to Emergency Ground Stations until the MA forward message queue is empty.
- Using the VPN, the Emergency Ground Stations, acknowledge receipt of restoral data back to the Emergency Control Center. If no acknowledgement is received, another MA forward service is scheduled with the SN at the next opportunity.
- The downloaded data from the MA forward link now residing at the Emergency Ground Station is physically moved to the computer network requiring restoral.

It is anticipated that the volume of critical data to be downloaded would be on the order of 500 Mbytes per user as packetized files. Users could utilize successive downloading events to retrieve their files, if necessary.

C. TDRS Multiple Access Fast Forward (MAFF)

The current TDRS MA system requires a modification to permit the rapid fulfillment of forward services to multiple users. This is because the system was designed to handle multiple return users, (typically science data from multiple spacecraft), but only individual forward service users (typically commands from the MOC to the user spacecraft and instruments). This asymmetric service model can be modified to permit a rapid succession of forward services to multiple users. This design modification is called MA Fast Forward [3]. MA Fast Forward provides the following additional capabilities:

- Provides new SN Operational capability which enhances the MA forward (MAF) service by removing the need of user scheduling
- Enables rapid access to MAF service by the user (science & emergency events etc.)
- Enables reduction in SN & Customer operational constraints
- Improves the SN network service utilization (rapid utilization of unused times)
- Provides a potential reduction in MAF inter-service time.

The service will utilize TDRS Unscheduled Time (TUT) and thus does not interfere with any scheduled MAF users. All other TDRS services (Single Access Forward and Return, and Multiple Access Return) are not affected.

This concept allows for an efficient utilization of an existing space communications asset without impacting other users. If insufficient TUT exists for a given situation, then NASA science users could be bumped down in the priority list in favor of providing scheduled services. The implementation of a MA Fast Forward service for a homeland security network recovery is depicted in Fig. 4. Operators are provided to manage the network and data, and provide a human-in-the-loop to resolve problems in real time. Note that all network connections are one-way. The Emergency Ground Stations transfer one-way status and acknowledgement data to the Emergency Control Center. Operators at the Emergency Control Center use that information to plan MAF services to transmit restoral data to the Designated Sites via the Emergency Ground Stations. It is the responsibility of the Designated Sites to get the data to restoral points within their networks.

D. IT Cybersecurity Threat/Recovery Scenario

A bad actor has identified your operations as a target of interest. The bad actor has worked with sympathetic and opportunistic actors to slowly unroll a spear-phishing campaign against your organization. Unaware employees and system users slowly provide the bad actor the information they need not only to compromise your operational system but also, over time, poison the integrity of your backup system. As a response to halt the attack is quickly devised it becomes clear that the integrity of critical assets on your system have been

compromised and will need to be restored as quickly as possible.

While the online backups are deemed unusable for recovery and the confidentiality, integrity, and availability of your network remains unknown, your team begins the work to isolate and restore critical parts of the infrastructure. While a full restore from connected backups is not possible and off-site storage will take some time to provide safe restore media, the critical infrastructure of keys, seeds, and other core information deemed essential to your organization is remotely stored on the isolated Emergency Control Center systems at the White Sands Complex. A transmission of this critical information to your organization's air-gapped, secure, ground station at both your primary site and your backup site is scheduled across one or more upcoming TUT periods. Rapidly, your organization has fundamental information needed to begin a rebuild of your system without relying on your compromised network and IT infrastructure.

E. Emergency Ground Station Requirements

The Emergency Ground Station requires an antenna and receiver system capable of closing the link with the TDRS MA forward service. This service has link characteristics as shown in table 1. [4]

TABLE I. TDRS MA FORWARD LINK REQUIREMENTS

Feature	Value
Customer service links/satellite	1
Frequency	2106.4 MHz
Polarization	Left Hand, Circular
RF Channel BW (3 dB, minimum)	6 MHz
Max Data Rate	300 kbps
Modulation	Spread Spectrum Unbalanced Quadriphase Shift Keying (SS-UQPSK). Spread Spectrum Binary Phase Shift Keying (SS-BPSK).

Using the assumptions shown in table 2, the required link characteristics can be satisfied with a link budget as shown in table 3. All link characteristics and budgets were calculated by the NASA/GSFC RF Analysis Group utilizing their standard tools for analyzing all missions that could utilize TDRS services.

TABLE II. TDRS MA FORWARD LINK ASSUMPTIONS

Ground Terminal Altitude	0 km
Minimum Ground Terminal Elevation Angle	5°
Frequency	2106.40625 MHz
TDRS MA EIRP	34 dBW (1st Gen. TDRS)
MA Information Rate	262.5 kbps
MA Symbol Rate	300 ksps
Modulation	SS-BPSK
Antenna Gain	18.25 dBi (Assumed for a 0.5 meter dish with 55% efficiency)
Pointing Loss	0.5 dB (Assumed)
Passive Loss	1 dB (Assumed)
LNA Noise Temperature	100 ˚K (Assumed)
System Temperature	199.4 ˚K Referenced at LNA (Assumed Tant = 50˚K)
Polarization	LHCP
Polarization Loss	0.1 dB (Assumed)
Data Format	NRZ-L
Command Coding	Rate 7/8 LDPC
Command Req. E_b/N_0	3.85 dB (BER=10-5)
User Implementation Loss	3 dB
Propagation Effects	0.5 dB (Assumed; rain and atmospheric attenuation)

Given the assumptions above for range of 41,130.9 km and a coded symbol rate of 300 ksps (kilosymbols per second) which provides an information rate of 262.5kbps, the link budget shown in table 3 applies using a 0.5 meter aperture antenna.

Table III. TDRS MA Forward Link Budget

	Parameter	Value	Tol	Remarks
1	Relay Network EIRP-dBw	34	-	
2	Free Space Loss-dB	191.2	-	Note B
3	Polarization Loss-dB	0.1	0.01	Note A
4	Propagation Loss-dB	0.5	*	Note A
5	Rfi Loss-dB	*	-	Note B
6	Dynamics Loss-dB	*	*	Note B
7	User G/T-dB/K	-6.25	-	Note A
8	Boltzman Constant	-228.6	-	Note B
9	User Received-P/N0-dB-Hz	64.55	-	Sum 1 Thru 8
10	Carrier/Total Power Ratio-dB	0	-	Note A
11	User Required Acquisition-P/N0-dB-HZ	61.04	3	Note A
12	User Acquisition Margin-dB	3.51	-	9+10-11
13	Command/Total Power Ratio-dB	0	-	Note A
14	User Implementation Loss-dB	3	1	Note A
15	Received Command-P/N0-dB	61.55	-	9+13-14
16	Command Data Rate-dB-Hz	54.19	-	Note A
17	User Received Eb/N0-dB	7.36	-	15-16
18	User Required Eb/N0-dB	3.85	1	Note A
19	Effective User Command Margin-dB	3.51		17-18

NOTE A: PARAMETER VALUE FROM USER PROJECT-SUBJECT TO CHANGE.
NOTE B: FROM CLASS ANALYSIS IF COMPUTED

The link budget was computed with NASA/GSFC CLASS link analysis tool assuming Low Density Parity Check (LDPC) Rate 7/8 forward error correction coding [5]. This link can be satisfied with positive margin using commercial off the shelf equipment and a 0.5 meter satellite dish. This can be accommodated in a variety of fixed and mobile ground station configurations.

IV. NETWORK SIMULATION RESULTS AND DATA DELIVERY CAPABILITY

A. *Definition of an Event*

Data is downloaded to a site during an event. An event consists of the user acquiring the TDRS MA forward signal and receiving the downloaded data in packet form.

B. Simulation Approach

The RF analysis group undertook a series of simulations to analyze the performance of MAFF for spacecraft users. These

results are directly applicable to the ground based security restoral scenario. The ground based scenario is a simplified subset of a space-based scenario. The ground elements are at fixed locations, and from the TDRS perspective, the view is much more constant than for low earth orbiting satellites.

For the purposes of this paper, the simulation configuration for up to 32 ground-based Designated Sites receiving MAFF is shown in fig. 5. Two TDRS spacecraft in the east and two TDRS spacecraft in the west covering the 32 sites in the CONUS enclosed in the polygons. The simulation uses TDRS Unused Time (TUT) for a period of 7 days. Events are queued up and run to completion (i.e. all users with data in the queue are serviced, however long that takes). In the simulation, all four TDRS unused time are used to maximize the available time for the MAFF service. The average delay is the time to complete an event (5 min, 15 min etc.) as shown in table IV. "Av" is the average delay considering all users, "Max" maximum value of average delay for the selected user set, "-" indicates average delay > 10 hrs. Average delay vs. number of users takes into account all four TDRS (in seconds). Data buffer length and time-to-live are parameters that can be adjusted according to needs; for the current simulation, these two have been adjusted to ensure there is no data loss. Table IV summarize the results, which are for the worst case service (lowest priority events, unscheduled service, simple FIFO queuing), for up to 8 users. Simulations for up to 32 simultaneous users have been performed.

Table IV. Average event delay (seconds) vs. number of simultaneous users

		Number of Users				
User events/day		***1***	***4***		***8***	
Event duration		Av	Av	Max	Av	Max
5 min	10	389	335	454	255	646
	15	385	402	472	260	598
	20	324	389	457	376	698
15 min	10	461	567	766	454	1311
	15	594	846	966	553	884
	20	507	1188	1297	1105	2373
30 min	10	815	1640	2201	1226	2899
	15	1380	3974	4461	2975	4320
	20	1639	9024	13140	12321	35668
45 min	10	1548	4437	5692	3348	4363
	15	2901	29521	56826	31093	69551
	20	5197	-	-	-	-

C. Performance Optimization

In an actual emergency, the number of users requiring this service is likely to vary as well as the required number of user events/day, event duration. This problem will require development of utilization of optimization algorithms. The MAFF model utilizes historical knowledge of the TDRS Unused Time (TUT) which exists between scheduled user supports. Therefore, one model of performance optimization that can be performed utilizes a variation of the NP-hard Bounded Knapsack problem [6]. In one version, optimization could be expressed for a fixed number of users as shown in Table V. Take the set of the 11 objects in table IV for eight users with event durations of 5, 15, 30, and 45 minutes and 10, 15 or 20 events per day. The knapsack is the available TUT, which in this example is constrained to 12 hours (43,200 sec).

TABLE V. TDRS MA FAST FORWARD UTILIZATION AS A BOUNDED KNAPSACK OPTIMIZATION PROBLEM

i	**Weight (events/day*Av delay)**	**Value (MBytes)**
1	2550	98
2	3900	148
3	7520	197
4	4540	295
5	8295	443
6	22100	591
7	12260	591
8	44625	886
9	246420	1,181
10	33480	886
11	466395	1,329

Items {8}, {9}, and {11} are exceed the 43200 sec knapsack limiit and are forbidden. The combination of {5, 6, 7} has weight of 42655 sec and value of 1624 Mbytes. The goal would be to optimize the knapsack up to the capacity. Such a problem is regularly approached via dynamic programming and evolutionary algorithms.

V. CONCLUSIONS

We have proposed a space-based relay service capable of using existing TDRS and WSC assets for a new, novel purpose: Spacebased network security restoral data services. It would utilize the existing infrastructure of the NASA/GSFC operated Space Network and its TDRS relay satellite constellation. The combination of a secure facilities at WSC, plus secure, encrypted, space links over TDRS, and secure, encrypted, short message, one-way acknowledgments facilitates this concept of operation. This capability can provide an element of the overall strategy for essential network security recovery service in case of national cyberattack with other options having been compromised.

ACKNOWLEDGMENT

NASA/GSFC Exploration and Space Communications Division provided support for this paper.

REFERENCES

[1] A.Waikar, Microsoft Tech Forum, Accessed, October 6, 2014, http://social.technet.microsoft.com/Forums/en-US/dataprotectionmanager/thread/dd37f298-0695-4db5-b9c5-1a56a7e9b067/

[2] D. J. Israel, "Low-cost TDRS communications for NASA's long duration balloon project," Aerospace and Electronic Systems Magazine, IEEE , vol.8, no.2, pp.43-47, February 1993

[3] D.J. Israel, F. Davis, and J. Marquart, "A DTN-Based Multiple Access Fast Forward Service for the NASA Space Network," Space Mission Challenges for Information Technology (SMC-IT), 2011 IEEE Fourth International Conference on, pp.61-65, 2-4 August 2011

[4] Space Network Users Guide (SNUG), Revision 10, August 3, 2012

[5] B. Gioannini, Y. Wong; J. Wesdock and C. Patel, "Bandwidth Efficient Modulation and Coding Techniques for NASA's Existing Ku/Ka-Band 225 MHz Wide Service," Aerospace Conference, 2005 IEEE, pp.1-11, 5-12 March 2005

[6] L. Caccetta, and Araya Kulanoot. "Computational aspects of hard knapsack problems." Nonlinear Analysis: Theory, Methods & Applications, vol. 47, no. 8, pp 5547-5558, 2001

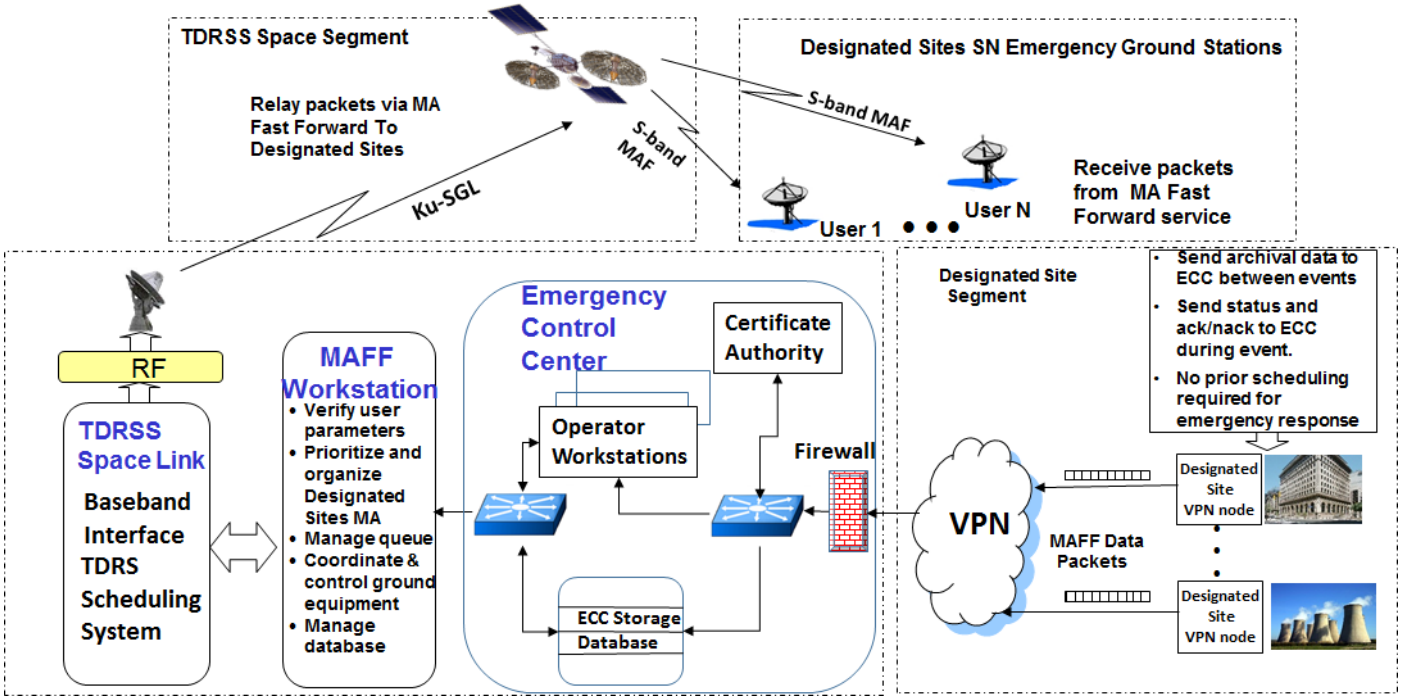

Figure 4. Concept of Operations for Emergency Network Security Restoral

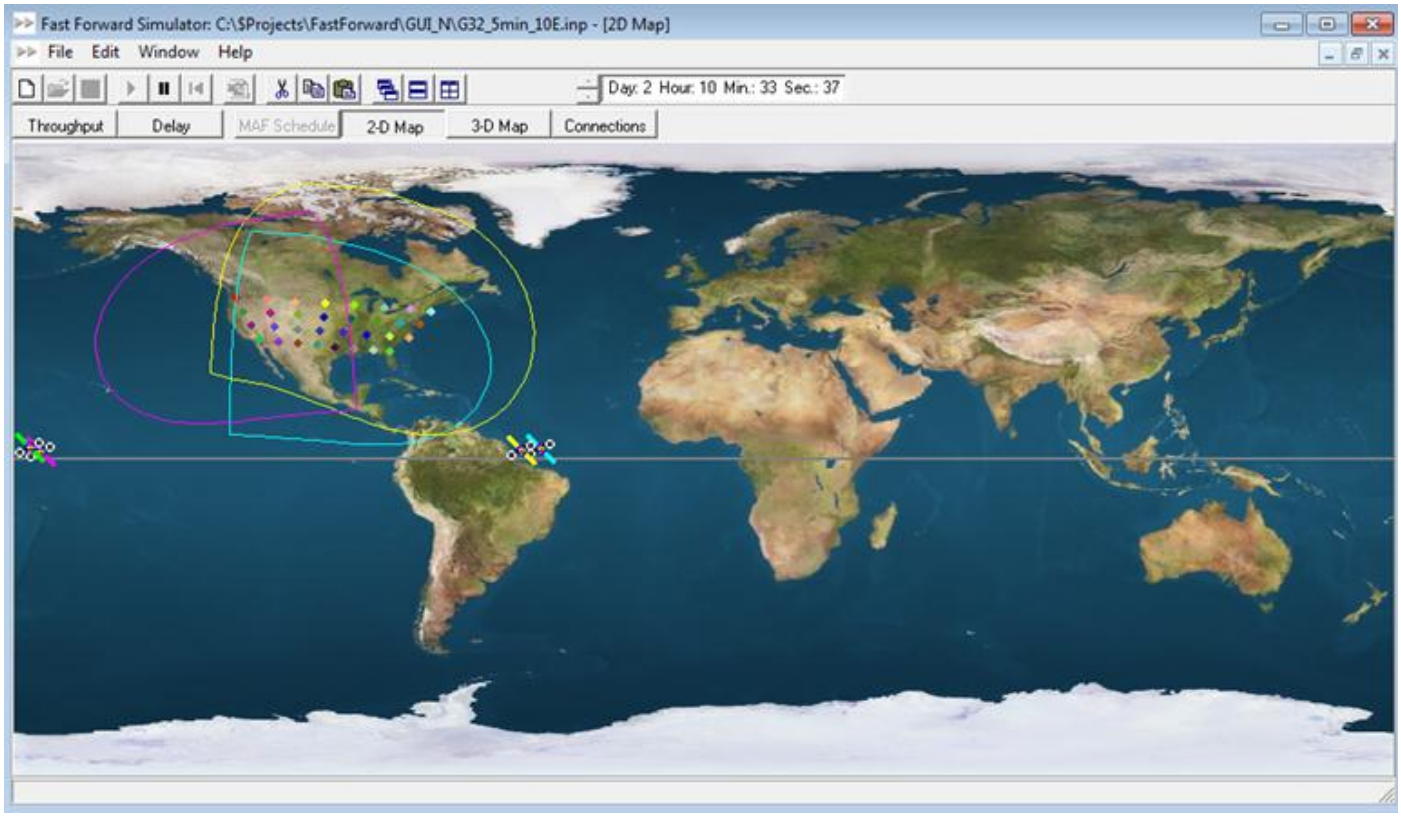

Figure 5. Simulation scenario with 32 Designated Sites serviced by four TDRS spacecraft.