Cyber Security with Radio Frequency Interferences Mitigation Study for Satellite Systems

Gang Wang[a], Sixiao Wei[a], Genshe Chen[*a], Xin Tian[a], Dan Shen[a], Khanh Pham[b], Tien M. Nguyen[c], and Erik Blasch[d]

[a]Intelligent Fusion Technology, Inc. Germantown, MD 20876;
[b]Air Force Research Lab, Kirtland AFB, NM, 87117;
[c]The Aerospace Corporation, CA, 90245;
[d]Air Force Research Lab, Rome, NY, 13441.

ABSTRACT

Satellite systems including the Global Navigation Satellite System (GNSS) and the satellite communications (SATCOM) system provide great convenience and utility to human life including emergency response, wide area efficient communications, and effective transportation. Elements of satellite systems incorporate technologies such as navigation with the global positioning system (GPS), satellite digital video broadcasting, and information transmission with a very small aperture terminal (VSAT), etc. The satellite systems importance is growing in prominence with end users' requirement for globally high data rate transmissions; the cost reduction of launching satellites; development of smaller sized satellites including cubesat, nanosat, picosat, and femtosat; and integrating internet services with satellite networks. However, with the promising benefits, challenges remain to fully develop secure and robust satellite systems with pervasive computing and communications. In this paper, we investigate both cyber security and radio frequency (RF) interferences mitigation for satellite systems, and demonstrate that they are not isolated. The action space for both cyber security and RF interferences are firstly summarized for satellite systems, based on which the mitigation schemes for both cyber security and RF interferences are given. A multi-layered satellite systems structure is provided with cross-layer design considering multi-path routing and channel coding, to provide great security and diversity gains for secure and robust satellite systems.

Keywords: Cyber security, radio frequency interferences, SATCOM, GNSS, multi-layered satellite system, cross-layer design, multi-path routing

1. INTRODUCTION

Satellite systems provide great benefits to human daily life, including television broadcasting, global position navigation, and weather forecasting, etc. To ensure satellite systems function properly, they are composed of space segment, terminal segment, and ground segment, where satellites are monitored, adjusted, and configured, all the operations of which rely on reliable communication link and security ensured data. For the satellite communications (SATCOM), it has characteristics including large area coverage, high capacity, and flexibility with transparent transponders, which thus has great potential to provide affordable ubiquitous network access services. However, it is exactly these characteristics which could make SATCOM vulnerable to interference [1][2], and system performances could be greatly degraded. It is thus required to enhance the SATCOM link performance while not sacrificing much throughput for reliable communications. Besides, the satellites, terminals, and infrastructures need to maintain their robustness against manipulation which leads to security issues.

*Corresponding Author: gchen@intfusiontech.com; phone: (001)301-515-7261; fax: (001)301-515-7262

Sensors and Systems for Space Applications IX, edited by Khanh D. Pham, Genshe Chen, Proc. of SPIE
Vol. 9838, 98380K · © 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2224632

In [3], a SATCOM link with hybrid automatic-repeat-request (HARQ) protocol has been evaluated in a two-stage Markov modeled channel; however radio frequency interferences (RFI) and security issues are not considered. In [4], commercial SATCOM link performances were evaluated in the condition of interferences, where the forward error correction (FEC) schemes apply concatenated Reed-Solomon coding and convolutional coding. In the up-to-date SATCOM standards, advanced channel coding schemes are often employed, including concatenated low-density parity-check (LDPC) and Bose, Ray-Chaudhuri, Hocquenghem (BCH) codes, and turbo coding. In [5][6], the SATCOM link performances of waveform applied in Digital Video Broadcasting - Satellite - Second Generation (DVB-S2) standard and Digital Video Broadcasting - Return Channel via Satellite (DVB-RCS) standard are evaluated in the condition of various RFIs, where however the security issues are not addressed.

For satellite systems, cyber security issues can be classified into three attributes: availability, confidentiality, and integrity. For *availability*, in a satellite communication network, the communication services must be available for legitimate users to access at any time. Many attacks, especially denial-of-service attack, aim to prevent the user from accessing communication channels or other portions of the network [7][8]. For *confidentiality*, it refers to maintaining the secrecy of information by preventing access to unauthorized users. Inside attack is one famous malicious threat with related to the confidentiality [9]. Adversaries first compromise some network components and then imitate legitimate users or servers to access the further information. For *integrity*, it is defined as protecting user data from modification, deletion, and/or injection [10]. This type of threat is extremely dangerous. In satellite systems, once ground stations or satellites are compromised, the adversaries could easily manipulate any sensitive information result in services crash or systems fail [11][12], even the information flow wireless channel is enhanced to be robust of interferences. Therefore, investigating cyber security in satellite communication network is important.

In this paper, we address both satellite systems radio frequency (RF) interferences and security, to provide comprehensive reliable and protected information flow. Due to the open environment nature of RF wireless communications, the complete denial-of-services attack in computer networks could be mitigated in wireless networks. To enhance both RFI mitigation and space segment security, a multi-layer satellites network topology is constructed. The communication protocol stack cross-layer design with joint multiple-path routing and advanced channel coding scheme is further developed to enhance the communication link quality-of-services (QoS). Simulation studies validate the proposed multi-layers cross-layer (MLCL) satellite topology construction and protocol stack design.

The paper is organized as follows. In Section 2, the satellite systems multi-layer scenario and interferences issues are presented. A comprehensive interference model is developed for further SATCOM link performance evaluations. A concatenated advanced channel coding scheme is proposed to enhance transmission link quality. In Section 3, the satellite systems cyber security is addressed and evaluated. The proposed MLCL scheme is developed and evaluated in Section 4. Section 5 provides conclusions and future work.

2. SATELLITE SYSTEM MULTI-LAYER TOPOLOGY

To provide ubiquitous reliable global information access and communications, it is a tendency for satellite systems to integrate all the available resources in the space segment to construct a space backbone network, which includes Geosynchronous Equatorial Orbit (GEO) satellites, Medium Earth Orbit (MEO) satellites, and Low Earth Orbit (LEO) satellites. The multi-layer satellite system topology structure is shown in Figure 1. It highlights that besides the space backbone network, the satellite systems also coordinate with the airborne network layer and terrestrial network layer. Examples of a multi-layered processing include imagery [13] and navigation [14]. Layered sensing requires the ability to correctly locate assets for communication incorporating space situation awareness [15], sensor management [16], and space tracking [17].

While it is easy to gather all the available resources, utilizing them well to achieve large exponential performance gains rather than providing more potential vulnerabilities must be addressed in the global information grid (GIG) environment. There are several ways to achieve this goal, and in this paper, we focus on the *cross-layer design of*

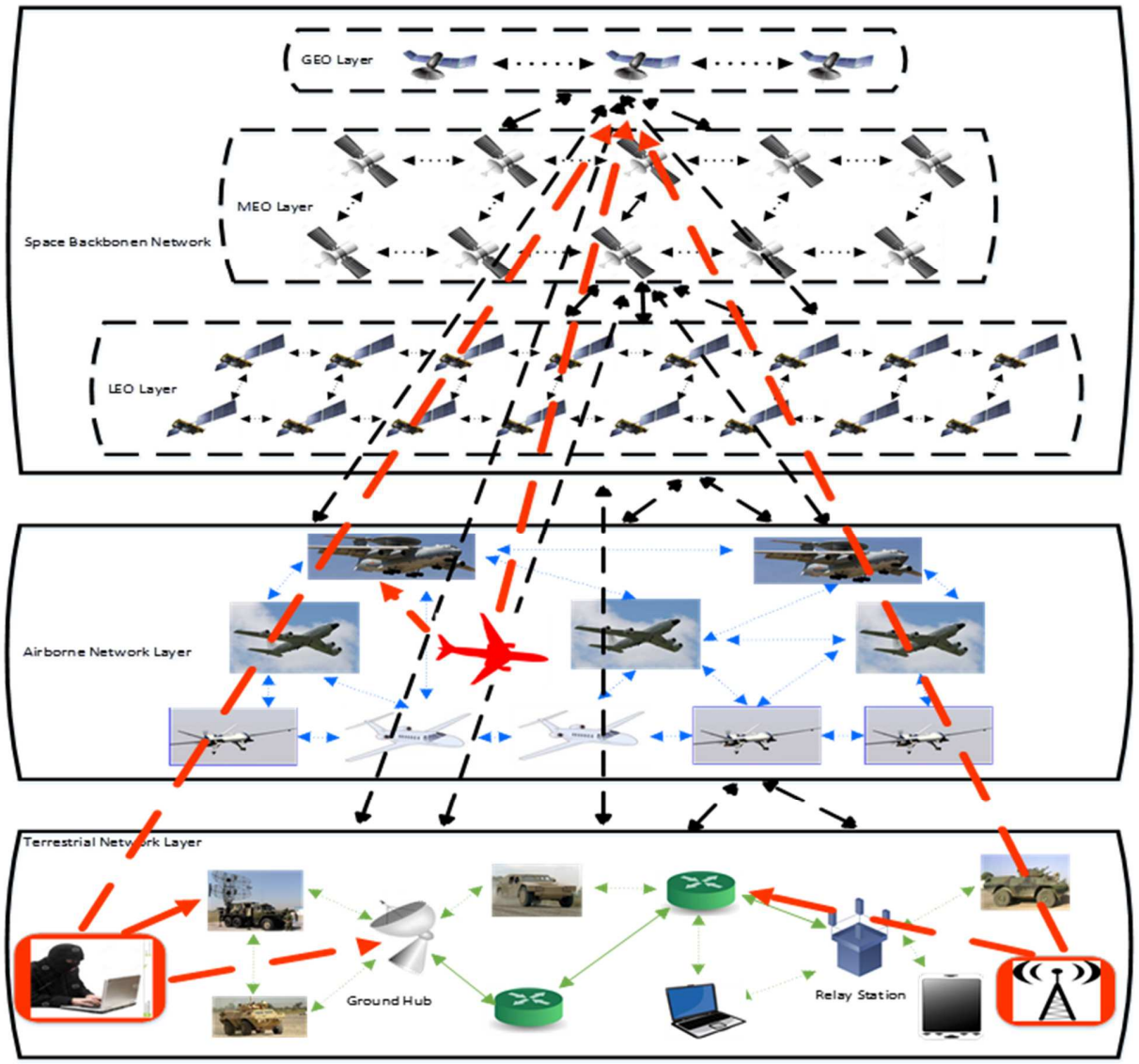

Figure 1. Satellite System Multi-Layer Topology Scenario

multi-path routing and advanced channel coding scheme. Since all the techniques development and performance evaluations are based on an accurate comprehensive interferences analysis; therefore, the satellite systems interference sources are analyzed, based on which a comprehensive interference model is developed. To clarify the various RFIs, we categorize them into two types, which are unintentional interferences and intentional interferences.

2.1 Unintentional Interferences

There are three types of *unintentional interferences*, which are (1) system malfunction and maloperation, (2) radio frequency signal channel propagation, and (3) external sources coming from other legal radio systems.

System internal unintentional interferences, such as malfunction and maloperation, could arise from both space and ground sources. For the satellite, it could be poor system design such as payload antennas are not set well, the circuits of electric boards are not hardened, manufacturing processing errors, or electronic components are exposed to solar flares,

etc. This kind of poor system design could cause the internal interferences among satellite components. Equipment failure from both satellite and ground controllers, such as the electronic components and clock drift, can also cause unintentional interferences for communication. Other sources include human error and malfunction could also cause unintentional interferences. To this list should be added is *physical attacks* where the electric components of the satellite could be destroyed by others, resulting in unintentional interferences.

Another type of unintentional interferences is the wireless propagation channel, resulting in *radio frequency* (RF) signal distortions. It includes multipath fading (LEO and MEO), Doppler effects, ionosphere effects, weather, and tropospheric delays. The multipath fading depends on carrier frequency, transmission data rate, and communication area surroundings, etc., where reflected signals can cause confusion to the recipient at the time of information recovery. The Doppler effect is caused because of the relative movement between the transmitter and receiver, with surrounding objects, which introduces signal frequency domain shifting and time domain phase rotation. The ionosphere effect and tropospheric delay arises when a satellite communicates with objects in airborne network layer and terrestrial network layer, where the ionosphere effect depends on frequency caused by the region of the atmosphere between 50 and 1000 km above the surface of the earth. The tropospheric delay is frequency independent and caused by the surface of the earth and 50 km above.

There are numerous *external unintentional interference* sources for SATCOM, caused by other legal radio communication systems, such as ultra wideband radar, personal electronic devices, and other devices operating in the adjacent and the same spectrum due to crowded and saturation of SATCOM operating frequency bandwidth. Moreover, the unintentional RFI can be also from other satellites in the same network, due to antenna mispointing, small separation angle, etc [18].

2.2 Intentional Interferences

There are mainly three types of *intentional interferences* for SATCOM, which are (1) spoofing, (2) meaconing, and (3) jamming. For *spoofing*, it is a deceptive signal transmission in the same frequency of SATCOM as the information signal. The spoofing is intended to deceive or to saturate the SATCOM receiver without it recognizing the interference effect, since the receiver treats the spoofing signal as real, however it is not. For *meaconing*, it consists of receiving the SATCOM signal, delaying it, and broadcasting the signal in the same frequency as the real signal to confuse the airborne system and users. For *jamming*, it emits signal with enough power and characteristics to prevent the receiver to acquire and track the information within the area SATCOM covered.

There are several types of *jamming* including broadband jamming, partial-time partial-band jamming, narrowband jamming, swept jamming, follower jamming, and smart jamming. The broadband jamming interferes the entire SATCOM frequency bandwidth. It is effective however requires large power to interfere the whole bandwidth, which in turn makes the jammer easy to be detected and located, and then mitigated. The partial-time partial-band jamming relaxes the large power requirement of broadband jamming, while sacrificing some effectiveness, by placing interference energy across multiple but not all channels in the spectrum domain used by SATCOM sometimes. The narrowband jamming places all of the jamming energy into a single channel, thus can be easily mitigated by SATCOM sensing and frequency re-allocation. To increase the effectiveness of narrowband jamming, the swept jamming signal is swept in time across the whole frequency band of interest. To further improve the effectiveness of narrowband jamming, the follower jamming attempts to locate the frequency of SATCOM transmitter went, identifies the signal as the one of interest, and jams at the new frequency. Besides the traditional jamming types, the smart jamming is gained a lot of interest, which attempts to disrupt portions of SATCOM digital signals, selecting only those portions necessary to deny communications [18], such as denying the control message by analyzing the traffic pattern. It attempts to effectively interfere the signal of interest, while greatly reducing its own energy consumption, making itself low probability of detection and lengthening the working lifetime.

2.3 Interferences Mitigation

After analyzing the interferences types of SATCOM, effective interference mitigation techniques are summarized in this subsection. Interferences mitigation can be categorized into four strategies, which are (1) regulatory protection, (2) RFI

localization and characterization, (3) protected waveform design and receiver interferences mitigation, and (4) authentication and encryption.

The *regulatory protection* strategy manages and assigns the appropriate spectrum for SATCOM. The assignment seeks to eliminate the possibility of the existence of the unintentional RFI, including the RFI from the same network and other legal radio communication systems. For the *spectrum interference localization and characterization*, the RFI can be determined as unintentional or intentional by localization of RFI sources and RFI waveform characteristic analysis in time and frequency domain. Therefore, corresponding techniques can be further employed. For unintentional RFI, different organizations can be contacted for RFI mitigation [19]; such as a coordination among different communication systems could be executed to mitigate the RFI among each other. For intentional RFI, the protected waveform and authentication can then be adaptively utilized.

For the *protected waveform design and receiver interference mitigation*, there are many techniques can be utilized. At transmitter, several techniques could be effective, including direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), time-hopping spread spectrum (THSS), advanced channel coding with interleaver over a larger number of symbols, directional antenna, beamforming, power control, and joint source-channel-network coding [20]. At receiver, effective techniques include interference nulling, front-end filtering, pulse blanking, and effective synchronization. Besides physical layer techniques, dynamic spectrum access (DSA) and dynamic resource management (DRM) with multipath routing could also be effective for interference mitigation [21-28]. For the authentication and encryption, this strategy can mitigate spoofing and meaconing intentional RFI. It includes angle-of-arrive discrimination, polarization discrimination [29], and cryptographic authentication.

The unintentional and intentional RFI for SATCOM are included in the communication link model, which is described as follows. Suppose the communication transmit-receive pair is separated with distance d. The information bits at the transmitter are divided into frames. In each frame, there are L uncoded information bits and L_0 overhead bits. The information bits and overhead bits are encoded with a channel encoder with coding rate r. For a system with M-ary modulation scheme, the number of symbols in each frame is $L_s = (L + L_0)/(rlog_2 M)$, where L is chosen in a way such that L_s is an integer. Therefore, considering both intentional and unintentional interference, the received signal samples in discrete-time at receiver can be represented as

$$y_m = \sqrt{E_r} h_m^{(TR)} x_m + \sqrt{E_I} h_m^{(IR)} k_m + z_m + n_m, m = 1,2,\cdots, L_s, \quad (1)$$

where E_r and E_I are the average received symbol energy from transmitter and synchronized aggregated RFI nodes respectively; $x_m \in S$ is the m-th modulated symbol at transmitter, with S being the modulation alphabet set with the cardinality $M = |S|$, k_m and z_m are the unknown synchronized interference and rest overall interference signal during the m-th symbol period, y_m, $h_m^{(TR)}$, $h_m^{(IR)}$, and n_m are the received sample, the fading coefficient between transmitter and receiver, the fading coefficient between the aggregated RFI node and receiver, and additive white Gaussian noise (AWGN) with single-sided power spectral density $N_0 = 2\sigma^2$, respectively. The z_m can be modeled as a Gaussian random variable with mean μ and variance $2\alpha^2$, which is quite flexible to model many weak interferes with varied μ and $2\alpha^2$ values [30]. It is assumed that the transmitter and aggregated RFI node transmit each signal to receiver undergoes different path, therefore providing the independent path fading of $h_m^{(TR)}$ and $h_m^{(IR)}$.

3. SATELLITE SYSTEM CYBER SECURITY STUDY

In this section, the performance of the security resiliency improvement is investigated using the multi-layer satellite system topology. To comprehensively evaluate the security performance of system, we use *metasploite*[1] to simulate a false data injection attack as an example to demonstrate the impact of security resiliency.

[1] Accessed at https://www.metasploit.com/

Specifically, an adversary is configured via metasploit to randomly compromise the ground stations or satellites for launching a class of false data injection attack. These attacks may result in the failure of the core measuring components and misleading the essential information, such as available bandwidth information and packet routing information. Generally speaking, false data injection attack refers to a *disruption*, in which an adversary injects forged bandwidth information into satellite network routing messages aim to disturb the routing process of data transmission. For example, the adversary may claim a higher or lower bandwidth than the satellite link could truly provide. Once ground stations or satellites receive the manipulated bandwidth information will be assigned improper amount of data packets, which may result in congestion or high delay situation.

In our simulation, we demonstrated a false data injection data by compromising ground stations and forging a higher available bandwidth information. With the packet size fixed at 1000 bytes, reducing the packet arrival interval can achieve a similar effect to increasing the number of users. Both single layer and multi-layers satellite system are evaluated and compared for their effectiveness of system security.

In Figure 2, it shows the relationship between throughput and number of users in terms of false data injection attack for both single layer and multi-layers satellite system. During the simulation, an adversary launched a fake available bandwidth information (2.0 Mbps) with regards to a true available bandwidth (1.5 Mbps). The throughput of multi-layers satellite system appears to be much higher than single layer. This is expected because more routes can be applied in multi-layers system and the congested packets will be automatically detour via other available links by choosing suitable routing algorithms. The end-to-end delay versus number of users in terms of false data injection attack is shown in Figure 3. Once false data injection attack is launched, the end-to-end delay will not have any influence before network becomes saturation. When more than 45 users are added into the satellite system, the attack will cause the end-to-end delay to increase rapidly. The results highlight that there is nearly no impact on a multi-layers satellite system because the multi-layers design provides higher security capacity by the comparison with single layer system.

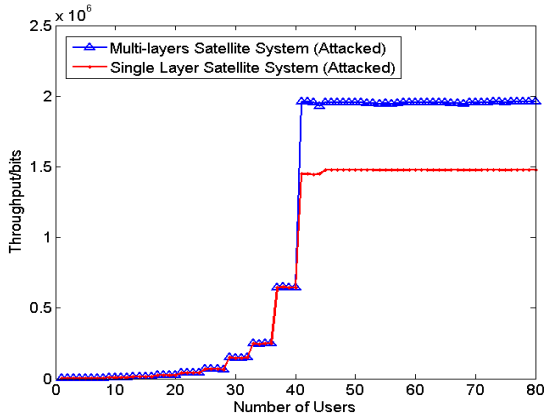

Figure 2: Throughput vs. Number of Users in False Data Injection Attack

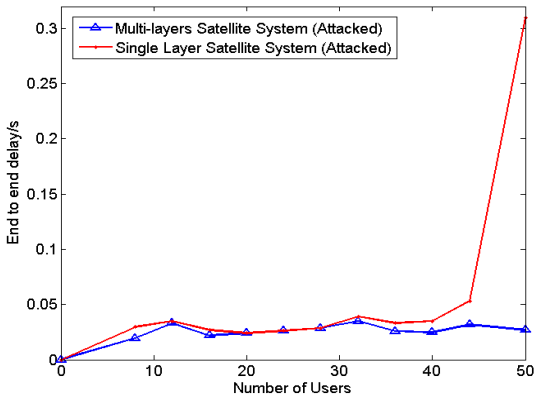

Figure 3: End-to-end Delay vs. Number of Users in False Data Injection Attack

4. MULTI-LAYER SATELLITE SYSTEM CROSS-LAYER DESIGN

Besides the multi-layer satellite system topology development in multi-layers cross-layer (MLCL) design, the cross-layer of multi-path routing with *advanced channel coding* design is utiized. The interaction of physical layer and network layer provides great benefits for the satellite network traffic flow, where appropriate traffic is distributed in each routing path for load balancing to avoid network congestion as well as security, and adaptive waveform transmission strengths each transmission successful probability for the RFI mitigation for the loaded traffic. There are two popular powerful schemes for the channel coding, which are *LDPC coding* and *turbo coding*. The two coding schemes have been compared in numerous literature, and each has been applied in various commercial communication

standards. However, in this paper, instead of adopting one coding scheme for a selected scenario, we develop the concatenated turbo/LDPC coding for enhanced communication link design in severe RFI environment.

A simulation study is conducted to evaluate the network resource utilization of MLCL satellite system. Consider a mixture network, which consists of multiple types of satellites and ground stations. Specifically, one GEO satellite, 4 MEO satellites, 11 LEO satellites and 10 ground stations are implemented via network simulator. The parameters we used are listed in following Table 1. In our simulation scenario, terminals are configured to emulate sources and destinations are ground stations on Earth. All the satellites are moving on their default orbits (different layers satellites are running on different altitudes) and all the associated parameters keep consistent while simulation runs. The handoff time of each satellite is defined as 10 time slots, which represents 10 ms. Once the simulation starts, one source node (a user) begin to transmit packets to a destination node (another user) via MLCL satellite system. The packet size and intervals are increased as time elapses, representing the increasing demand of users.

Two metrics are considered to evaluate the effectiveness of our MLCL satellite system: (i) *Throughput* is defined as the successful data delivery rate during data transmission over the network; (ii) *End-to-end delay* is defined as the average time taken for a single packet to be transmitted from the source to the destination over the network. Though these two metrics, QoS network performance such as traffic transmission rate and congestion status is determined. To better evaluate the performance of multi-layers satellite system, we conduct two simulation schemes to make the comparison. In first scheme, the source and destination node we established will only communicate through ground stations and one GEO satellite. All the traffic data will be transmitted through one upload link and download link. In second scheme, we keep using the same source and destination node as first scheme but they are allowed to communicate via multi-layers satellite system, including all the GEO, MEO and LEO satellites. To accurately assess the network performance between two schemes, the bandwidth of both schemes are denoted as the same while simulation runs. Throughput and end-to-end delay are compared and evaluated from each scheme. The simulation was run around 150 times for both two schemes and compute the average performance metric values.

Table 1: Multi-layers satellite system simulation parameters

	GEO Satellite	MEO Satellite	LEO Satellite	Ground Station
Altitude	36000 km	10000 km	780 km	0 km
Planes	1	1	1	N/A
Plane	1	4	11	10
Up/Download Bandwidth	1.5 MB/s	1.5 MB/s	1.5 MB/s	10 MB/s
Inclination	15 degree	55 degree	86.4 degree	N/A
Inter-plane Separation	N/A	15 degree	31.6 degree	N/A
Elevation Mask	180 degree	40 degree	8.2 degree	N/A

In Figure 4, it shows the relationship between throughput and number of users for two schemes. As shown, more users are increased to using the network resource as time elapses. With the fixed packet size (e.g., 1000 bytes), the decline of packet arrival intervals can achieve a similar effect as the increase of the number of users. However, the throughputs are not increasing once around 45 users are created in both two schemes. This represents that the upload or download link can only allow around 45 users using the network simultaneously. Eventually all the throughputs reach the bandwidth limit as the number of users increases. Figure 4 demonstrates that the multi-layers satellite system can achieve higher throughput by the comparison with single layer when more than 45 users are accessing the network. This is expected because multi-layers satellite system allows more routes to transmit the traffic packets while users are increasing. The congested packets could be detoured via another idle transmission link. In Figure 5, it illustrates the end-to-end delay versus the number of users for both single layer and multi-layers satellite systems. The trend of end-to-end delay in multi-layer satellite system is a performance much lower than that of single layer. This is because multi-layers structure can provide multiple routes to avoid the congestion and re-route the packets to other satellite links with idle bandwidth.

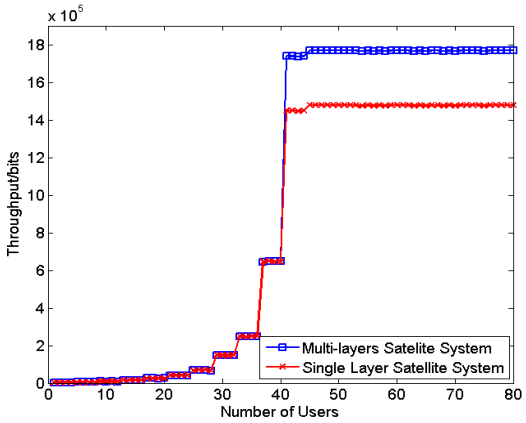

Figure 4: Throughput vs. Number of Users

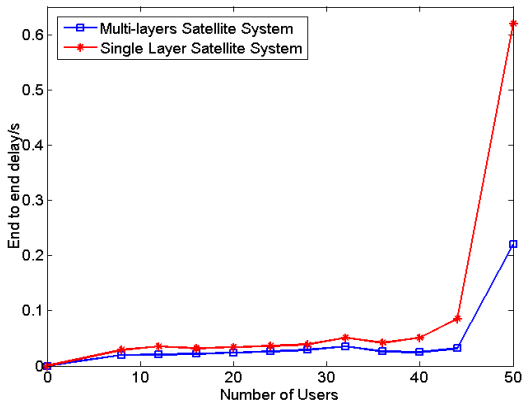

Figure 5: End-to-end Delay vs. Number of Users

5. CONCLUSIONS

In this paper, a multi-layer cross-layer satellite systems topology construction and protocol stack design is developed to address the system both RFI mitigation and security capabilities. The RFI mitigation ensures the link information flow reliability, while security ensures the flowed information data are integrate and from legacy users. With the comprehensive RFI mitigation and security investigations, satellite systems are able to provide ubiquitous reliable services. In addition, for the RFI mitigation, the comprehensive satellite systems interferences are investigated, based on which an interference model is developed for link performance evaluations. With the multi-layer satellite systems topology construction, a cross-layer design of multi-path routing and enhanced concatenated turbo/LDPC advanced channel coding scheme is also developed. The results demonstrate that the RFI mitigation and security are not isolated. For instance, if the ground station is compromised, the designed RFI mitigation communication protocol stack could be useless, since the ground station could stop working due to the hacking which thus result in large network congestion. The RFI mitigation capability even makes situation worse while it ensures the compromised ground station manipulated data reliable flow in the satellite systems. Besides the RFI mitigation capability and security, it also shows our developed MLCL to improve satellite network QoS performances and capabilities, including increased throughput and reduced delay, by utilizing well all the available resources in space backbone network.

Future work includes using the multi-layer approach in space situation awareness toolsets which include space object tracking and location, sensor management, and network topology reconfiguration. Techniques such as cloud computing for big data analytics [31] and coordination with air platforms [32] would be incorporated.

REFERENCES

[1] “Backyard satellite jammers concern US air force,” News in Science, (2000).
[2] Bercovici M. W., [FCC Narrowbanding Mandate: A Public Safety Guide for Compliance], (2006).
[3] Schodorf, J. B. and Gouker, M. A., “Performance evaluation of a hybrid ARQ protocol implementation for EHF SATCOM on the move systems,” IEEE Military Communications Conference, (2001).
[4] Ezers, R. and Farserotu, J., “Performance evaluation of commercial SATCOM modems with respect to interference and nuisance jamming,” IEEE Military Communications Conference, (1995).
[5] Wang, G. et al., “Performance evaluation of SATCOM link in the presence of radio frequency interference,” IEEE Aerospace Conference, (2016).

[6] Wang, G., Chen, G., Shen, D. et al., “Spread spectrum design for aeronautical communication system with radio frequency interference," IEEE/AIAA Digital Avionics Systems Conference, (2015).
[7] Yu, W., Wei, S., Shen, D., Blowers, M., and Blasch, E. P., “On detection and visualization techniques for cyber security situation awareness,” in Proceedings of SPIE, 9-17, (2013).
[8] Yu, W., Wei, S., Ma, G., Fu, X., and Zhang, N., “On effective localization attacks against internet threat monitors,” IEEE International Conference on Communication (ICC), (2013).
[9] Zhang, H., Wei, S., Ge, L., Shen, D., Yu, W., Blasch, E. P., Pham, K. D., and Chen, G., “Towards an integrated defense system for cyber security situation awareness experiment,” SPIE, 946908–8, (2015).
[10] Wei, S., Ge, L., Yu, W., Chen, G., and Pham, K., “Simulation study of unmanned aerial vehicle communication networks addressing bandwidth disruptions,” in Proceedings of SPIE, 10–17, (2014).
[11] Bhattarai, S., Rook, S., Ge, L., Wei, S., Yu, W., and Fu, X., “On simulation studies of cyber attacks against LTE networks,” IEEE International Conference Computer Communication and Networks, (2014).
[12] Xiong, W., Kwon, H. M., Ibdah, Y., Lee, K., and Bi, Y., “Effects of node geometry on cooperative distributed AF wireless relay network,” IEEE International Conference on ICT Convergence, (2011).
[13] Mendoza-Schrock, O., Patrick, J. A., et al., ”Video Image Registration Evaluation for a Layered Sensing Environment,” Proc. IEEE Nat. Aerospace Electronics Conf (NAECON), (2009).
[14] Yang, C. et al.,“Performance-Driven Resource Management in Layered Sensing,” Int’l Conf. on Info Fusion (2009).
[15] Chen, G., Blasch, E., Chen, H., Pham, K., “Multi-agent modeling and analysis for space situation awareness,” SPIE Newsroom, (2009).
[16] Xu, P., Chen, H., Charalampidis, D., Shen, D., G. Chen, et al., “Sensor Management for Collision Alert in Orbital Object Tracking,” Proc. SPIE 8044, (2011).
[17] Tian, X., Chen, G., Blasch, E., Pham, K., Bar-Shalom, Y., “Comparison of three Approximate kinematic Models for Space Object Tracking,” Int’l Conf. on Info Fusion, (2013).
[18] Park, C., Kang, C. et al., “Interference analysis of geostationary satellite networks in the presence of moving non-geostationary satellites,” IEEE Information Technology Convergence and Services, (2010).
[19] United States Strategic Command, Satellite Communications Electromagnetic Interference Resolution, (2007).
[20] Yu, W., Fu, X., et al., “On Effectiveness of Hopping-Based Techniques for Network Forensic Traceback,” Int’l J. of Networked and Distributed Computing, Vol. 1, No. 3, (2013).
[21] Xiang, X. and Valenti, M. C., “Improving DVB-S2 performance through constellation shaping and iterative demapping,” IEEE Military Communications Conference, (2011).
[22] Ding, Y., Li, L, and Zhang, J. K., “Blind transmission and detection designs with unique identification and full diversity for noncoherent two-way relay networks,” IEEE Trans. Veh. Technol., (63), 3137-3146, (2014).
[23] Li, L., Ding, Y., Zhang, J. K., and Zhang, R., “Blind detection with unique identification in two-way relay channel,” IEEE Trans. Wireless Comm., (11), 2640-2648, (2012).
[24] Xiang, X. and Valenti, M. C., “Closing the gap to the capacity of APSK: constellation shaping and degree distributions,” International Conference on Computing, Networking and Communications, (2013).
[25] Wang, G., Pham, K., Blasch, E., Nguyen, T. M., Chen, G. et al., “Optimum design for robustness of frequency hopping system,” IEEE Military Communications Conference, (2014).
[26] Wang, G., Chen, G., Shen, D. et al., “Performance evaluation of avionics communication systems with radio frequency interference," IEEE/AIAA Digital Avionics Systems Conference, (2014).
[27] Xiong, W., Lee, K., and Ibdah, Y., “A regenerative decode-and-forward wireless network with multihop relays under channel uncertainty,” Computer Modeling and Simulation (EMS), (2011).
[28] Shen, D., Chen, G., Wang, G. et al., “Network survivability oriented markov games (NSOMG) in wideband satellite communications,” IEEE/AIAA Digital Avionics Systems Conference, (2014).
[29] Wang, G., Shen, D., Chen, G., Pham, K., Blasch, E., “Polarization Tracking for Quantum Satellite Communications,” Proc. SPIE, Vol. 9085, (2014).
[30] Chen, Y. and Beaulieu, N. C., “NDA estimation of SINR for QAM signals,” IEEE Comm. Letters, (2005).
[31] Liu, B., Blasch, E., Chen, Y., Aved, A. J., Hadiks, A., Shen, D., Chen, G., “Information Fusion in a Cloud Computing Era: A Systems-Level Perspective,” IEEE Aerospace and Electronic Systems Magazine, Vol. 29, No. 10, pp. 16 – 24, Oct. (2014).
[32] Wang, Z., Blasch, E., Chen, G., Shen, D., Lin, X., Pham, K., “A Low-Cost Near Real Time Two-UAS Based UWB Emitter Monitoring System,” IEEE AESS Magazine, Vol. 30, No. 11, pp. 4-11, Nov. (2015).