ORIGINAL ARTICLE

Journal Section

Mitigating Distributed Denial of Service Attacks in Satellite Networks

Muhammad Usman[1] | **Marwa Qaraqe**[1] | **Muhammad Rizwan Asghar**[2] | **Imran Shafique Ansari**[3]

[1]Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University (HBKU), Education City, 34110 Doha, Qatar

[2]School of Computer Science, The University of Auckland, 1142 Auckland, New Zealand

[3]James Watt School of Engineering, University of Glasgow, G12 8QQ, UK

Correspondence
Muhammad Usman, Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University (HBKU), Education City, 34110 Doha, Qatar
Email: musman@hbku.edu.qa

Funding information

Satellite communication is becoming a complementary technology in future 5G and beyond networks due to their wider coverage. Similar to any terrestrial network, security has become a major concern in satellite networks. Due to a long distance between ground stations and satellite transponders and due to its inherited broadcast nature, satellite communication has certain limitations such as high bit error rate, high link delays, power control, and large round trip delays. The aforementioned limitations make security techniques proposed for terrestrial networks more challenging in satellite settings. Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks have become one of the most popular security threats in both the terrestrial and satellite networks. In this article, we present a DDoS mitigation technique that can be employed at the Ground Station (GS) end in satellite networks. In particular, we simulate Internet Control Message Protocol (ICMP) echo request (ping) flooding across a satellite network and propose a proactive mitigation technique by restricting the number of echo requests a network entity can generate. The simulation results demonstrate that DDoS attacks can be mitigated in satellite networks without affecting the Quality of Experience (QoE) of legitimate users.

Abbreviations: DDoS, Distributed Denial of Service.

KEYWORDS
DoS attack, Distributed DoS attack, Satellite communication, ICMP, Internet Protocol, Packet flooding

1 | INTRODUCTION

Satellites allow communication between geographically dispersed systems by establishing a wireless communication link between them. These satellites are widely utilized in various communication fields, such as the Internet, radio, telephone, television, and military are a few to name with many others. With their inherited nature of wider coverage and lower deployment costs, satellite communication is supposed to become an integral part of the fifth generation (5G) of cellular networks [1]. A growing area of interest in 5G is Vehicle-To-Vehicle (V2V) communication that exploits the potential of satellite communication in 5G [1]. Inspired by the wider coverage of satellite networks, there are some applications of satellite communication in the future Internet-of-Things (IoT) as well [1].

With the advent of integrating satellite communication and 5G cellular networks with the aforementioned applications, it has become vital to investigate the security of these satellite-based networks. The inherited nature of wider coverage and communication broadcast makes satellite networks more vulnerable to cyber attacks. Additionally, the adversaries are utilizing more sophisticated tools to attack different network entities, especially satellite networks.

One of the main attacks in satellite networks is Denial-of-Services (DoS) or Distributed DoS (DDoS) attack, which may target a satellite transponder to take advantage from its inherent weakness of a single point of failure. DoS and DDoS attacks are a major concern in commercial satellite networks wherein the communication infrastructure is poorly equipped with security measures. Further, such attacks can easily target Network Operations Center (NOC) *a.k.a.* command and control system for satellite Ground Station (GS) due to the development of more sophisticated attack tools and weak security measures in satellite networks. Keeping in view the importance of satellite communication infrastructures in 5G, DDoS attacks have become a prime security concern for a satellite GS, especially NOC.

In this article, we highlight various different possibilities of DoS and DDoS attacks on satellite GSs and propose solutions to mitigate those attacks. In particular, we simulate a DDoS attack in a satellite network using Internet Control Message Protocol (ICMP) based echo requests (ping) flooding. We consider a scenario wherein a network entity at NOC of a GS is compromised by an adversary, which utilizes its resources to launch ping flooding causing congestion over legitimate satellite links. As a mitigation strategy, we introduce a rate limiting technique that restricts the number of echo requests a network entity can send or receive from a set of communication nodes. Our simulation results demonstrate that satellite GSs can be protected by mitigating DDoS attacks without hampering the Quality of Experience (QoE) of legitimate users.

The rest of the article is organized as follows: Section 2 reviews related work. Section 3 highlights various possibilities of DDoS attacks in a satellite network and provides a comprehensive overview of the problem. The simulated scenario and the details of the system and adversary model are given in Section 4. Section 5 presents the proposed approach to handle DDoS attacks in satellite communication networks. Performance evaluation of the proposed solution is presented in Section 6. Section 7 enlists some of the advantages and limitations of the proposed system. Finally, Section 8 concludes the article and discusses possible future directions.

2 | RELATED WORK

Addressing security issues in satellite communication has gained much attention in recent years. The literature on satellites network security can be divided into two broad categories, namely, (i) Physical Layer Security (PLS) based solutions, and (ii) cryptography-based solutions.

2.1 | PLS-based Solutions

There are some works in the literature that focus on incorporating PLS in the satellite links [2, 3, 4, 5, 6, 7, 8, 9]. The authors in [2] investigate the eavesdropping in Non-Geostationary Orbit (NGSO) satellite communication systems. In particular, the authors focus on the downlink scenario and estimate secrecy capacity and secrecy outage probability in the presence of a fixed eavesdropper. In addition, Li *et al.* [3] explore the secrecy performance of multi-antenna Land Mobile Communication (LMS) systems in the presence of multiple eavesdroppers. They investigate the secrecy outage probability over Shadowed-Rician fading channels. On the other hand, the authors in [4] focus on solving the confidentiality problem in multi-beam satellite systems using XOR network coding protocol. The authors maximize the sum secrecy rate using semi-definite programming together with 1-D search. Inspired from PLS, the authors in [5] propose an algorithm to minimize the total transmit power in a scenario wherein the legitimate receivers are dispersed throughout multiple beams with each receiver surrounded by multiple passive eavesdroppers. Similarly, Bankey *et al.* [6] investigate the secrecy outage probability of a hybrid multi-antenna satellite-terrestrial relay network in the presence of multiple eavesdroppers. Particularly, the authors employ two classic cooperative protocols, *decode and forward* and *amplify and forward* in the presence of both colluding and non-colluding eavesdroppers. A similar kind of work is presented in [7] wherein the authors propose joint beamforming and artificial noise techniques to secure hybrid satellite-terrestrial networks. Working on the similar directions, Gua *et al.* [8] investigate the average secrecy capacity and outage probability of satellite channels with multi-user opportunistic scheduling. Unlike the aforementioned works, the authors in [9] study the secrecy performance of a hybrid satellite and Free-Space Optics (FSO) cooperative systems, under shadowed-Rician fading on satellite links and Gamma-Gamma fading on FSO links.

2.2 | Cryptography-based Solutions

Some works in the literature focus on cryptographic techniques to secure satellite communication [10, 11]. In [10], the authors propose a chaos theory based encryption algorithm for small satellites, such as CubeSats. The results are compared against Advanced Encryption Scheme (AES) and SPECK, in terms of encryption speed. A similar kind of work is presented in [12], where the authors utilize elliptic curve cryptography for satellite communication. In particular, a three-factor authentication protocol is proposed to secure the communications against well-known security attacks. Some works focus on quantum cryptography, a physical layer security technique, to secure a satellite link [13, 14, 15]. For instance, authors in [13] propose a free space key exchange protocol using a weak laser with polarization modulation.

Most of the aforementioned works focus on securing satellite links from the eavesdropper perspective. Very few works exist in the literature that focus on securing satellite communication in scenarios with respect to DoS/DDoS attacks. One such work is presented in [16] wherein the authors investigate the possibility of preventing DoS attacks in the satellite communication. However, the main focus is on reducing power consumption of the Network Control Center (NCC) while preventing DoS attacks.

In this work, we propose a scheme to mitigate DoS/DDoS attacks in the satellite network focusing on defining an upper bound for the number of connection requests on satellite links.

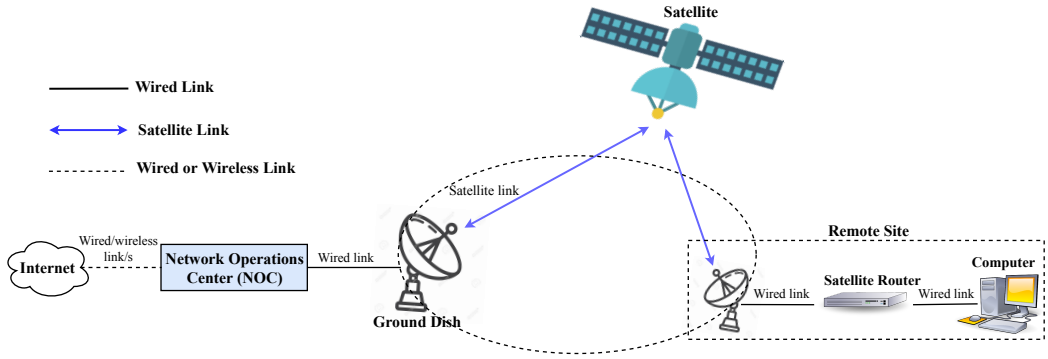

FIGURE 1 A simple satellite-based communication system: The data from satellite to the Internet flows through Network Operations Center (NOC), which is responsible for all the network management and control. The NOC and remote sites are vulnerable to cyber attacks wherein an adversary can take the control of Ground Station (GS) and flood the satellite link with bogus packets in order to create congestion.

3 | PROBLEM STATEMENT

Due to wider coverage and their inheritance broadcast nature, satellite networks are widely utilized in the scenarios wherein conventional wired and wireless terrestrial networks cannot be deployed, such as disaster relief and providing remote areas an access to the Internet [17]. A block diagram of a typical satellite network is presented in Fig. 1. The NOC provides the management and control functionalities in satellite networks wherein a satellite dish behaves as a network entity to transmit and receive information from the satellite. Being a key component of the satellite network, if an adversary gets the control of the ground station, it can be easily utilized to generate DoS attack and block the satellite communication with other ground stations by flooding traffic on the satellite links. Additionally, the remote site depicted in Fig. 1 is another potential source of DoS/DDoS attacks in case it is compromised by an adversary.

3.1 | DoS/DDoS Attack Types

The primary aim of a DoS/DDoS attack is to exhaust the resources of network nodes and the communication links between them using bogus traffic in order to make them unavailable for any legitimate traffic. The key resources in a network include disk space, memory, CPU time, and network bandwidth. In the context of a satellite network, the ground stations can be easily targeted by adversaries. Actually, an adversary can generate a number of bogus packets to consume a significant portion of memory and disk space thereby utilizing a significant portion of bandwidth between the ground station and the satellite link.

Similar to terrestrial networks, satellite networks can be subject to three most popular types of DoS/DDoS attacks

[18], namely, (i) Type of Service (ToS) floods, (ii) Synchronization (SYN) floods, and (iii) ping floods.

3.1.1 | ToS Floods

In ToS floods, an adversary gets the control on Explicit Congestion Notification (ECN) and Differentiated Services (DiffServ) flags by foraging the ToS of an IP packet header. In particular, an attacker spoofs the ECN field to reduce the throughput of individual connections between the clients and the server utilizing satellite links, hence causing the server to be unavailable for legitimate requests. Furthermore, the attacker can use the DiffServ flag to prioritize attack traffic over legitimate traffic, hence intensifying the effect of DoS attacks.

3.1.2 | SYN Floods

In SYN floods, an adversary utilizes the half-open Transport Control Protocol (TCP) connections in a network to overflow the network resources. In TCP, a half-open connection is the one for which a server is waiting for an ACK message from the client after a client sends a SYN message. In fact, for every SYN received from a client, the server sends a SYN-ACK message and waits for the final acknowledgment from the client. Meanwhile, the server maintains a database of all the connections for which the server is waiting for the acknowledgments. As the resources of a server are finite, it can be intentionally made exhausted by creating a large number of open connections, hence making the server resources unavailable for legitimate traffic.

3.1.3 | Ping Floods

In ping floods, an adversary creates a large number of ICMP echo requests (pings) that are sent to a network node from a range of IP addresses to make it unavailable. Alternatively, in ping floods, an adversary takes control of network nodes and sends a large number of pings originated from multiple servers around the globe thereby flooding the target with bogus traffic, thus making the target unavailable. In both cases, if the network node is a ground station or a satellite, the nodes dependent on it for connectivity will experience a blackout or will encounter a lower QoE.

It is worth mentioning that the effect of the aforementioned DoS/DDoS attacks can be amplified in the satellite networks due to inherited higher latency and broadcast nature of these networks, wherein special satellite equipment can be utilized to overhear the satellite broadcast and act as a legitimate station. In addition, generating these kinds of attacks in a higher latency environment makes the system unavailable for real-time applications such as Voice over IP (VoIP) even if the scale of the attack is manageable.

4 | SYSTEM AND ADVERSARY MODEL

In this section, we present the system and adversary model wherein an adversary gets control of the main ground station (*i.e.*, GS2) and utilizes its resources to launch DDoS attacks across the satellite network. In particular, the system model and the adversary model are discussed separately.

4.1 | System Model

The details of the simulated system are presented in Fig. 2. There are four satellite ground stations (GSs) that are inter-connected via a satellite rotating in a Geostationary Orbit (GEO). One of the sites (*i.e.*, GS2) is a major hub providing Internet access to the other connected remote sites (*i.e.*, GS1, GS3, and GS4) over the satellite links. All other

GSs (*i.e.*, GS1, GS3, and GS4) have satellite routers connected to them over the wired links. The satellite router act as local gateway to connect its local user with GS2.

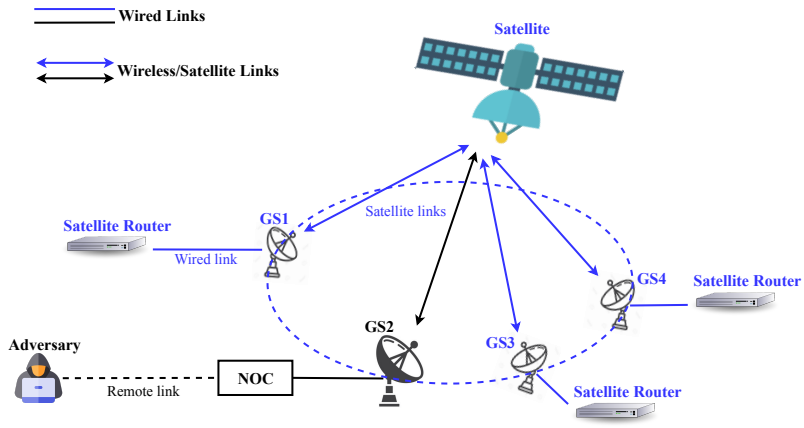

FIGURE 2 The simulated scenario: we consider four ground stations connected to a satellite for communication purposes. An adversary gets control of the main ground station (*i.e.*, GS2) containing NOC and exploits it to send a large number of echo requests utilizing the ICMP protocol. This creates a bottleneck in the satellite network and subsequently decreases the QoE of the legitimate users connected with the GS2. The adversary floods ICMP packets across the network, specifically targeting GS1, GS3, and GS4.

4.2 | Adversary Model

We consider that all the connected entities with GS1, GS3 and GS4 are trustworthy. On the other hand, Some of the network entities attached with GS2 are either not trustworthy or compromised by an adversary. In particular, we consider that an adversary, having information regarding IP address of satellite routers, gets access to GS2. Using GS2, the adversary sends multiple echo requests to all the connected sites utilizing ICMP. ICMP is a network layer protocol, which is generally utilized by network devices to report packet delivery errors to source IP address.

In this article, we assume that the adversary utilizes ICMP flooding (ping flooding) to launch DDoS attacks across the network. In particular, having information about the connected ground stations with the satellite, the adversary targets GS1, GS3, and GS4 with the aim of potentially blocking the legitimate communication over satellite links. The adversary floods ICMP echo requests to all GSs, which in return sends echo response frames, overwhelming GS2 and potentially blocking the communication of GS2 with any other GS. In addition, as GS2 is the major hub for GSs to communicate with the Internet, overwhelming it potentially blocks Internet access to all the remote sites associated with it.

The frequency of ping requests is increased gradually in order to make the effect unnoticed in the beginning. In addition, the attacker does not fully block the communication of GS2, rather it tries to decrease the QoE of legitimate

users by sending a large number of ICMP echo requests and hence decreasing the throughput of the legitimate link. The network administrator may not detect the attack in the beginning assuming that the decrease in the QoE may be due to legitimate reason(s), such as bad weather conditions.

5 | PROPOSED SOLUTION

One of the straightforward solutions to prevent DDoS attacks is to disable the ICMP support from all the network entities connected through satellite links. However, this solution has a number of limitations. First of all, it will deactivate a number of other ICMP-based protocols and functionalities utilized for network management and diagnostics. For instance, it will deactivate the error-reporting functionality, *i.e.*, the sender node will not be able to send/receive any error in case its IP packet has not reached the intended destination. In addition, it will disable a useful protocol, ICMP Router Discovery Protocol (IRDP), which is used to discover the presence of routers across a network.

The other limitation of disabling ICMP is that even if its functionality is not enabled across the routers, the adversary will still be able to flood the satellite link in case it is not blocked on any of the connected routers with the satellite link, such as a remote site. In particular, any network entity with ICMP enabled can be a potential source of ping flooding, causing congestion over satellite links. The user will still feel a decrease in the QoE for the applications connected over the satellite links.

As a mitigation strategy to prevent DDoS attacks in satellite networks, we propose to limit the number of ICMP connections a network entity can send or receive. In particular, we monitor the behavior of the network, *i.e.*, how many echo requests a network entity sends or receives from a set of IP addresses in the normal condition while the network is not under a DoS attack. We flag this as normal behavior of the network and any violation from this is flagged as an abnormality and ICMP packets are not entertained in such a scenario. It is important to note that this monitoring of behavior does not mean the profiling of a user's traffic based on its IP address. However, the term "normal" means an estimation of the average number of ICMP requests a network entity may handle. This kind of information can be easily retrieved from the network even if the IP address allocation is dynamic across the networks. The case of dynamic IP allocation does not prevent to estimate a threshold for the average no. of ICMP requests for each entity over a specific period of time. In fact, the network entity can be uniquely represented by its IP address, MAC address or any other information unique to it, such as its user name, *etc.* In particular, all the ICMP packets passing through NOC are monitored to prevent DoS/DDoS attacks. In case a large number of ICMP echo requests are observed passing in or out of the NOC, they are blocked by the routers at NOC. It is worth mentioning that for the current work, the proposed solution is implemented in NOC. However, it can be easily generalized to any remote site connected with a satellite network.

Note that our solution helps to prevent both kinds of ping flooding, *i.e.*, (i) a network entity within NOC sends a large number echo requests to different GSs whose replies overwhelm the communication link of GS2, and (ii) a large number of spoofed network devices send ICMP requests to a target network entity in GS2 to overwhelm its network and computational resources. During the case of a network entity sending a large number of echo requests to different GSs, the NOC will not only block the echo request beyond a certain limit but also their replies coming from the GSs. On the other hand, for the other scenario, the ICMP request originating from different entities are blocked at the NOC and no reply is sent to the source IPs. It is important to note that we block the ICMP requests from specific IP addresses only (that potentially triggers DDoS attacks), which will not affect the legitimate ICMP traffic generated from the legitimate users across a satellite network. There can be some cases, when the corrupted network entity, such as a BS, has legitimate nodes attached to it. However, even in those cases blocking the corrupted network entity from generating ICMP requests does not affect the attached legitimate entities, which have their own public IP address. This is due to the reason that our proposal blocks the ICMP requests originated from the corrupted node only not all the

ICMP packets passing through a node as transit.

6 | PERFORMANCE ANALYSIS

This section reports performance evaluation of the proposed solution presented in Section 5. The aim is to prevent DoS/DDoS attacks in the satellite network presented in Fig. 2 without placing computation and communication burden on the satellite links. The scenarios presented in Fig. 2 are implemented in MATLAB[1]. Four legitimate satellite GSs are connected with a satellite rotating in Geostationary Orbit (GEO). For simulation purposes, we place the satellite at a distance of 36,000 kms from GSs [19, 20], wherein GSs are placed randomly within an area of radius of 1000 kms (Area 3,142,857 km^2). It is important to note that 1000 km radius is the considered range only, where we place the GSs. It, by no means, represents the total coverage area of a GEO satellite. It is worth mentioning that the MATLAB implementation of our work is based on the open-source library[2]. As the focus of this article is simulating DDoS attacks and its mitigation, we do not explicitly explain the physical layer characteristics of such a system, rather we analyze the network layer performance under DDoS attacks.

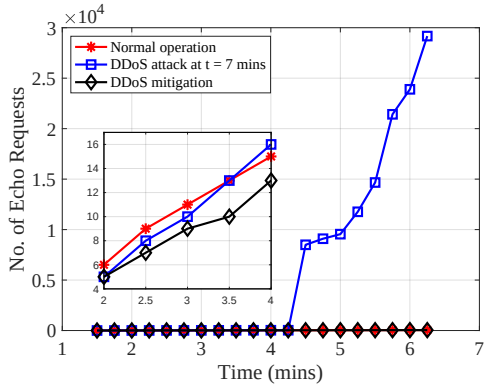

FIGURE 3 The cumulative number of ICMP echo requests passing through NOC in the normal operation and in the presence of DDoS attacks: we consider on average 2-3 echo requests/minute sent from an IP or received by an IP as normal and anything beyond this is regarded as abnormality. The x-axis represents the simulation time while the y-axis represents the cumulative number of echo requests with the passage of time. At t=7 minutes, a compromised network node in NOC starts sending a large number of echo requests to a number of remote sites (GS1, GS3, and GS4). The attack subsequently decreases the QoE, if not handled properly. It can be noted that our solution prevents the DDoS attack and keeps an average number of connections in the normal range.

The simulations results are presented in Fig. 3, Fig. 4, and Fig. 5. Particularly, Fig. 3 presents the cumulative number of echo requests sent from a network entity in the case of normal operations, DDoS attacks, and attack mitigation in action. reviNormal operation is the duration of the simulation when the network is not under any DDoS attack. Particularly, 2-3 echo requests/minute are considered as normal and any number beyond this is considered as a DDoS attack. It can be noticed from the graph that the adversary gradually increases the number of echo requests starting from the time t=7 minutes targeting network entities attached with GS1, GS3, and GS4. This subsequently decreases the QoE at the legitimate user's end. Applying the mitigation technique keeps the number of echo requests in the normal

[1] https://www.mathworks.com/products/matlab.html

[2] https://www.mathworks.com/matlabcentral/fileexchange/54875-geostationary-satellites-tracking

range and does not allow the compromised entity to send a large number of echo requests. In case the compromised entity still tries to send the ICMP requests, they are blocked at NOC, preventing them to penetrate in the satellite links. In addition, the source IP can be blocked entirely to send any IP traffic until the issue is resolved and the compromised entity is rescued.

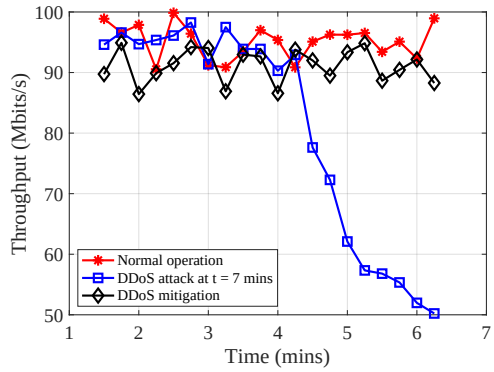

FIGURE 4 The instantaneous throughput observed at GS2: we measure the throughput at GS2 every 30 seconds. At a certain time, t=7 minutes, an adversary joins the network and starts sending a large number of echo requests to potentially overwhelm the satellite link and block the legitimate communication. With the proposed solution, the traffic goes unaffected by the attack and legitimate users experience the same QoE.

Fig. 4 illustrates the instantaneous TCP throughput measured at GS2 for its communication with GS1. It can be observed from Fig. 4 that on an average the TCP throughput between GS2 and GS1 is around 100 MBits/s. It can be noticed that in case of no defense against DDoS attacks, the throughput significantly drops from t=7 minutes onward. It is clearly visible from the graph that applying DDoS mitigation technique, *i.e.*, restricting the number of allowed echo connections helps to mitigate DoS attacks and keep the throughput in the normal range. In fact, the network goes unaffected by the attack and the legitimate network entities do not feel any decrease in the QoE. The only limitation of this solution is that network entities cannot send more echo requests beyond a certain threshold. However, in normal day-to-day activities, they generally do not require to send a large number of echo requests.

Fig. 5 shows the percentage of packet drops at NOC of GS2 during normal operations and under DDoS attacks. It can be observed from the graph that in the case of normal operation a minor percentage of packets are dropped at GS2, which may be due to bad channel conditions. This kind of packet drops does not significantly affect the performance as they are re-transmitted from the transmitter using the Automatic Repeat Request (ARQ) protocol. However, in the case of DDoS attacks, a significant amount of packets are dropped due to the buffer flow and link congestion caused by the generation of a large number of ICMP echo requests. This kind of packet drop cannot be handled by the ARQ protocol but requires special consideration to mitigate the effect of DDoS attacks. Limiting the number of echo requests per IP can certainly prevent this kind of attacks without significantly changing the overall performance of satellite networks.

7 | ADVANTAGES AND LIMITATIONS

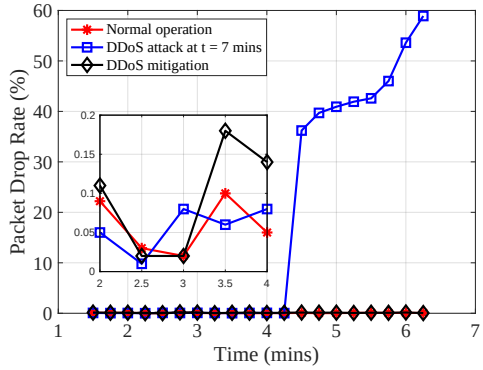

FIGURE 5 The percentage of dropped packets at GS2 with and without DDoS attacks: restricting the number of echo requests from an IP assists in keeping the packet drop rate within the normal range even in the presence of a DDoS attack. In addition, it can be observed that in the case of no defense against DDoS attacks, the packet drop percentage starts increasing from the attack time, *i.e.*, t=7 minutes and reaches around 60%.

7.1 | Advantages

The advantage of our solution is that it blocks the DDoS attack with it is actually happened. As soon as our system identifies that the number of ICMP requests are going beyond a certain limit, it blocks all the subsequent ICMP packets from that particular network node. Another advantage lies in the simplicity of the proposed solution, which makes it faster to implement In particular, the proposed solution does not require any sophisticated cryptographic algorithms, which makes it ideal in the satellite setting, where the link delays are already high. On the other hand, some of the approaches proposed in the literature aim to implement strong authentication mechanisms in the legitimate network entities in order to prevent intruders from interrupting them. However, this kind of approaches may secure network entities to be compromised but they do not prevent the chances of a malicious insider, who already has the control over the network.

7.2 | Limitations

Despite a number of advantages, our solution suffers from a few limitations as well. First of all, it provides a solution against a single kind of DDoS attack only, (*i.e.*, ping floods). It does not support the prevention of other kinds of DDoS attacks, such as ToS floods and TCP SYN floods. Another possible limitation of the proposed solution can be the false blockade of a legitimate node, whose IP address is spoofed by an adversary. An attacker can spoof the IP address of a legitimate node and use it to generate a large number of echo/requests across the network. However, preventing such attacks could be an interesting research direction for future work.

On the similar lines, another limitation is the false blockade of legitimate ping requests. There may be some scenarios when a legitimate user generates a large number of ping requests for network diagnosis or any other legitimate operation. This legitimate can be blocked by our system treating the legitimate user as malicious. One of the possible solutions to this problem can be to increase the threshold for the normal operation.

8 | CONCLUSIONS AND FUTURE WORK

In this article, we presented a solution to mitigate DDoS attacks in satellite networks. We highlighted various different possibilities of DoS and DDoS attacks in satellite settings targeting NOC and other remote sites at GSs. In particular, we simulated ping flood in satellite networks generated by a compromised network entity of a GS. We demonstrated that our proposed solution provides a proactive prevention apagainst DoS and DDoS attacks. The network is continuously monitored in normal operations and the average number of ICMP echo requests flowing through a GS network is observed. In case the echo requests start deviating from the observed number, a prevention action is taken to block all those requests at NOC and potentially blocking the source IP until the compromised network entity is rescued. Our simulation results demonstrate that DDoS attacks can be easily mitigated without placing much burden, in terms of communication and processing power, over NOC entities.

In future, we plan to implement machine learning techniques to capture the normal range of ICMP echo requests generated by each network entity across a satellite network and then utilize it to mitigate DoS/DDoS attacks. In addition, we plan to implement other types of DDoS attacks as well over the satellite links, such as ToS flood and SYN floods. We aim to provide different solutions to mitigate such attacks.

REFERENCES

[1] Evans BG. The role of satellites in 5G. In: 2014 7th Advanced Satellite Multimedia Systems Conference and the 13th Signal Processing for Space Communications Workshop (ASMS/SPSC) IEEE; 2014. p. 197–202.

[2] Xiao Y, Liu J, Shen Y, Jiang X, Shiratori N. Secure Communication in Non-Geostationary Orbit Satellite Systems: A Physical Layer Security Perspective. IEEE Access 2019;7:3371–3382.

[3] Li Y, An K, Liang T, Yan X. Secrecy Performance of Land Mobile Satellite Systems With Imperfect Channel Estimation and Multiple Eavesdroppers. IEEE Access 2019;7:31751–31761.

[4] Kalantari A, Zheng G, Gao Z, Han Z, Ottersten B. Secrecy Analysis on Network Coding in Bidirectional Multibeam Satellite Communications. IEEE Transactions on Information Forensics and Security 2015 Sep;10(9):1862–1874.

[5] Zheng G, Arapoglou P, Ottersten B. Physical Layer Security in Multibeam Satellite Systems. IEEE Transactions on Wireless Communications 2012 February;11(2):852–863.

[6] Bankey V, Upadhyay PK. Physical Layer Security of Multiuser Multirelay Hybrid Satellite-Terrestrial Relay Networks. IEEE Transactions on Vehicular Technology 2019 March;68(3):2488–2501.

[7] Lu W, Liang T, An K, Yang H. Secure Beamforming and Artificial Noise Algorithms in Cognitive Satellite-Terrestrial Networks With Multiple Eavesdroppers. IEEE Access 2018;6:65760–65771.

[8] Guo K, Lin M, Zhang B, Ouyang J, Zhu W. Secrecy Performance of Satellite Wiretap Channels With Multi-User Opportunistic Scheduling. IEEE Wireless Communications Letters 2018 Dec;7(6):1054–1057.

[9] Ai Y, Mathur A, Cheffena M, Bhatnagar MR, Lei H. Physical Layer Security of Hybrid Satellite-FSO Cooperative Systems. IEEE Photonics Journal 2019 Feb;11(1):1–14.

[10] Jackson S, Straub J, Kerlin S. Exploring a Novel Cryptographic Solution for Securing Small Satellite Communications. I J Network Security 2018;20(5):988–997.

[11] O'Neill M, O'Sullivan E, McWilliams G, Saarinen MJ, Moore C, Khalid A, et al. Secure architectures of future emerging cryptography SAFEcrypto. In: Proceedings of the ACM International Conference on Computing Frontiers ACM; 2016. p. 315–322.

[12] Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M. Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications. Computer Communications 2019;147:85 – 97. http://www.sciencedirect.com/science/article/pii/S0140366418310235.

[13] Rarity JG, Gorman PM, Knight P, Wallace K, Tapster PR. Quantum cryptography to satellites for global secure key distribution. In: Otrio G, editor. International Conference on Space Optics — ICSO 2000, vol. 10569 International Society for Optics and Photonics, SPIE; 2017. p. 300 – 307. https://doi.org/10.1117/12.2307891.

[14] Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, et al. Satellite-to-ground quantum key distribution. Nature 2017;549(7670):43.

[15] Liu J, Yang Z, Wu Z, Yin Z, Jiang X, Fu Y. Control Code Multiple Encryption Algorithm on Satellite-to-ground Communication. Mobile Networks and Applications 2019 Dec;24(6):1955–1974. https://doi.org/10.1007/s11036-019-01338-z.

[16] Onen M, Molva R. Denial of service prevention in satellite networks. In: 2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577), vol. 7 IEEE; 2004. p. 4387–4391.

[17] Radhakrishnan R, Edmonson WW, Afghah F, Rodriguez-Osorio RM, Pinto F, Burleigh SC. Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view. IEEE Communications Surveys & Tutorials 2016;18(4):2442–2473.

[18] CERT Coordination Center, 1996 CERT Advisories. SEI, Carnegie Mellon University; 2000. https://resources.sei.cmu.edu/asset_files/WhitePaper/1996_019_001_496172.pdf.

[19] Sharma SK, Chatzinotas S, Ottersten B. In-line interference mitigation techniques for spectral coexistence of GEO and NGEO satellites. International Journal of Satellite Communications and Networking 2016;34(1):11–39.

[20] Chisci L, Fantacci R, Pecorella T. Predictive bandwidth control for GEO satellite networks. In: 2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577), vol. 7 IEEE; 2004. p. 3958–3962.