2024 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN) | 979-8-3503-1764-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/DySPAN60163.2024.10632738

I2S Attack: Exploring MITM Attack on Satellite Communications by Spectrum Shared IoTs

Tamerlan Aghayev, Chad M. Fortenbaugh and Zicheng Chi
Department of Computer Science
Cleveland State University, Cleveland, OH USA
Email: t.aghayev@vikes.csuohio.edu, c.fortenbaugh@vikes.csuohio.edu, z.chi@csuohio.edu

***Abstract*—In satellite communication systems, the high sensitivity and vast coverage area make them prime targets for potential attackers. Given the integral role satellites play in modern communication, navigation, and observation systems, any vulnerability can have cascading effects on various sectors, from military to civil applications. On the other hand, recent exponentially growing IoT devices expose a potential security issue to the satellite communication running on the shared spectrum. In this paper, we for the first time propose to launch a Man-in-the-middle attack from ubiquitous IoT devices to spectrum-shared Satellite communication (I2S Attack) at a low cost but vast impact. The key idea is to use a compromised IoT device's OFDM signal to emulate satellite's MSK signals. Specifically, we discussed the feasibility of signal emulation, introduced the theory of I2S Attack, captured real-world satellite signals, and conducted simulations. The simulation result shows that we can achieve up to 65% emulation similarity between OFDM and MSK signals.**

***Index Terms*—Internet of Things, Satellite Communication, Spectrum Sharing, Man-in-the-middle Attack**

I. Introduction

The Internet of Things (IoT) paints a vision of a seamlessly interconnected world where physical objects, from household appliances to industrial machinery, are equipped with digital intelligence and are able to communicate and exchange data. At its core, IoT is about enhancing the utility and functionality of everyday objects through connectivity. With embedded sensors, software, and other technologies, these objects, termed "things," are linked to the Internet, allowing them to collect and share data. This enables a two-way flow of information between the digital and physical worlds, fostering real-time communication, analysis, and action. Though, while IoT offers unprecedented connectivity, its devices often lack stringent security measures, making them potential gateways for cyber-attacks [1].

On the other hand, as the backbone of various applications, from global communication networks to weather predictions, satellites have revolutionized the way we live. However, with increased reliance on these celestial devices comes the challenge of securing them. A study by IOActive in 2014 uncovered critical vulnerabilities in satellite communication (SATCOM) systems, potentially allowing attackers to intercept, manipulate, or block satellite data communication [2]. Such vulnerabilities, rooted in weak encryption, outdated protocols, and inadequate authentication processes, could have ramifications from service disruptions to severe security breaches. One of the most concerning threats in satellite communication is the man-in-the-middle (MITM) attack which can have catastrophic outcomes, emphasizing the need for rigorous security measures.

In this paper, we for the first time show the possibility that an MITM attack can be launched to satellite communication by spectrum-shared malicious (or compromised) IoT devices at a very low cost but vast impact. i.e., the MITM attack can be launched by ubiquitous IoT devices such as WiFi devices. In the rest of this paper, we refer to this attack as IoT to Satellite MITM Attack or I2S Attack.

The feasibility of the I2S Attack is based on our **observation** that *satellite communication uses a lower-order modulation scheme while IoT communication uses a higher-order modulation scheme*. By exploring the relationships between two different modulation schemes, we found that it is possible to use IoT modulated signals to "emulate" satellite signals and launch the I2S Attack by using signal emulation at a low cost.

For example, as shown in Figure 1, a satellite uses minimum-shift keying or MSK (i.e., a very typical satellite modulation scheme) signals to communicate with a ground station. Meanwhile, an attacker uses a WiFi device, which uses Orthogonal frequency division multiplexing-quadrature amplitude modulation or OFDM-QAM (i.e., a scheme used by all WiFi and LTE IoTs), to emulate MSK signal and launch the attack. This approach does not involve intercepting or decoding satellite signals directly, differentiating it from a traditional MITM attack. Instead, it showcases a unique method of signal disruption by spectrum emulation.

The crux of this paper lies in the exploration of how OFDM sub-carriers can be used to emulate MSK signals.

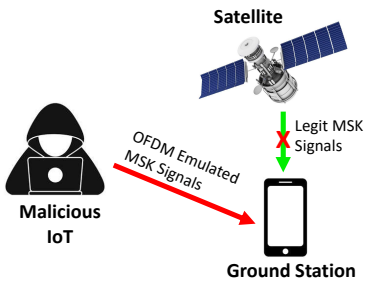

Fig. 1. IoT to Satellite MITM Attack

By establishing a relationship between the two modulation schemes, we aim to shed light on potential vulnerabilities and, consequently, devise ways to enhance the security of satellite communication systems. Specifically, we will briefly introduce the background of OFDM and MSK modulation schemes, respectively (Section III-A). Then, we will discuss the feasibility of using OFDM signal to emulate MSK signal and provide the mathematical proof. In Section IV, we provide our on-site satellite signals measurements and simulation results for our proposed method. We will conclude current status of our work in Section V.

II. Related Work

In addressing satellite communication vulnerabilities, this study builds upon foundational research in the field. The examination of IoT's vulnerability to DDoS threats [1] lays the groundwork for addressing security challenges in IoT devices. Research revealing critical vulnerabilities in SATCOM systems [2] underscores the necessity for fortified security measures. The foundational principles of OFDM for wireless communications [3] and the theoretical contributions to digital communications [4] inform our approach to signal emulation techniques. Additionally, the practical context provided by the DTUSat-2 CubeSat project [5] offers a real-world backdrop for our theoretical and experimental findings, collectively emphasizing the importance of advancing satellite communication security to mitigate risks associated with MITM attacks.

III. Methodology

To fully grasp the nuances of the vulnerabilities and potential threats between satellite systems and IoTs, we will review the background of OFDM and MSK. Then, we will analyze the emulation feasibility and provide our methodology.

A. Background

Orthogonal Frequency Division Multiplexing (OFDM): OFDM is a digital multi-carrier modulation method, especially suited for high-speed data communication, often used in broadband internet, wireless networks, and digital television broadcasting. In OFDM, a single data stream is divided across multiple separate narrowband channels at different frequencies to reduce interference and improve efficiency [3].

The fundamental principle behind OFDM's effectiveness lies in its utilization of orthogonality. This ensures that the individual carrier frequencies do not interfere with each other, enabling high-speed data transfers even in environments prone to multipath propagation and interference. With its robustness against channel imperfections, OFDM has become a preferred method for modern wireless communication systems.

The baseband OFDM signal can be represented as:

$$S_{\mathrm{OFDM}}(t) = \sum_{n=0}^{N-1} A_n e^{j\phi_n} e^{j2\pi f_n t} \tag{1}$$

Where, N is the number of sub-carriers, A_n and ϕ_n are the amplitude and phase of the n-th sub-carrier, respectively, and f_n is the frequency of the n-th sub-carrier. The complex exponential term $e^{j\phi_n}$ represents the phase of the n-th sub-carrier, while $e^{j2\pi f_n t}$ represents the sinusoidal oscillation at frequency f_n. The OFDM signal is essentially a sum of sinusoidal signals, each with a specific amplitude, phase, and frequency.

Minimum Shift Keying (MSK): Minimum Shift Keying (MSK) is a type of continuous-phase frequency shift keying. In simpler terms, it's a modulation scheme that transmits data by altering the frequency of a carrier wave. What makes MSK stand out is its minimal use of bandwidth. In MSK, the difference between the higher and lower frequency is equal to half the bit rate, ensuring optimal bandwidth usage [4].

The continuous phase property of MSK provides benefits such as minimizing phase discontinuities, making it particularly suitable for applications where preserving phase is crucial, like in many satellite communication systems. Its predictable nature and efficiency have made it a popular choice for satellite-based communication, including systems like the Global Positioning System (GPS).

The baseband MSK signal can be represented as:

$$S_{\mathrm{MSK}}(t) = \sum_{k=-\infty}^{\infty} a_k G(t - kT) \tag{2}$$

Where, a_k is the data symbol, T is the symbol duration, and $g(t)$ is the modulated Gaussian pulse with a bandwidth-time product $BT = 0.5$. The MSK signal is a sum of Gaussian pulses, each multiplied by a data symbol and shifted in time by integer multiples of the symbol duration.

B. Emulation Feasibility Analysis

The emulation of MSK signals using OFDM, at its core, is a testament to the intricate properties and adaptability of both modulation schemes. Recently, researchers have proposed the possibility of using OFDM signals to mimic IoT protocols such as ZigBee [6].

OFDM's defining feature is its capability to transmit multiple data streams simultaneously over numerous sub-carriers. Within this structure, each sub-carrier can be modulated using traditional schemes. A hallmark of OFDM is its inherent flexibility; the scheme permits the dynamic alteration of waveforms, enabling it to adapt to different communication needs and challenges. MSK, on the other hand, represents a specialized form of Frequency Shift Keying (FSK) wherein the frequency difference is deliberately minimized to optimize bandwidth consumption. This approach is pivotal for satellite communications, where bandwidth is a treasured resource. Given this technological landscape, OFDM's versatility emerges as a crucial enabler for the emulation of MSK signals. The depth of control within OFDM, allowing individual sub-carriers to be fine-tuned in amplitude and phase, facilitates the generation of signals that mirror MSK characteristics closely. Moreover, the shared spectrum of OFDM and MSK compounds this emulation potential.

C. Gaussian Pulse and Its Fourier Transform

The Gaussian pulse is fundamental to our exploration as it is integral to the representation of MSK signals. MSK signals can be depicted as a summation of modulated Gaussian pulses, each representing a data symbol. The Gaussian pulse, characterized by its bell-shaped curve, is expressed mathematically as:

$$g(t) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{t^2}{2\sigma^2}} \tag{3}$$

Here, σ is the standard deviation of the Gaussian function. The Fourier transform of the Gaussian pulse is as follows:

$$G(f) = \sigma e^{-\frac{(2\pi\sigma f)^2}{2}} \tag{4}$$

We can observe that the Fourier transform of the Gaussian pulse is another Gaussian function, but in the frequency domain.

D. Fourier Transform of MSK Signal

The Fourier transform of a function $s_{\mathrm{MSK}}(t)$ is defined as:

$$S_{\mathrm{MSK}}(f) = \int_{-\infty}^{\infty} s_{\mathrm{MSK}}(t) e^{-j2\pi ft} dt \tag{5}$$

Since the MSK signal can be expressed as a sum of shifted Gaussian pulses, we can apply the linearity property of the Fourier transform:

$$S_{\mathrm{MSK}}(f) = \int_{-\infty}^{\infty} \left(\sum_{k=-\infty}^{\infty} a_k g(t - kT) \right) e^{-j2\pi ft} dt \tag{6}$$

Now, we can use the Fourier transform of the Gaussian pulse, $G(f)$, and the time-shift property of the Fourier transform:

$$S_{\mathrm{MSK}}(f) = \sum_{k=-\infty}^{\infty} a_k G(f - kF_s) \tag{7}$$

Here, $F_s = \frac{1}{T}$ is the symbol rate, and $G(f)$ is the Fourier transform of the Gaussian pulse. The Fourier transform of the MSK signal is a sum of shifted Gaussian functions in the frequency domain, each multiplied by the data symbol.

E. Using OFDM sub-carriers to emulate the MSK signal

By deriving the appropriate amplitude and phase for each OFDM sub-carrier based on the representation of the MSK signal, we can configure the OFDM signal such that is closely resembles an MSK signal. Let's represent the MSK signal using OFDM sub-carriers:

$$S_{\mathrm{MSK}}(t) = \sum_{n=0}^{N-1} A_n e^{j\phi_n} e^{j2\pi f_n t} \tag{8}$$

We need to find the relationship between A_n, ϕ_n, and a_k. We can use the Fourier series representation of the MSK signal and compare it with the OFDM signal representation. Consequently, we can find the relationship between the amplitudes and phases of the OFDM sub-carriers and the MSK data symbols. For each sub-carrier, we can find the corresponding frequency component in the MSK signal's spectrum:

$$S_{\mathrm{MSK}}(f_n) = \sum_{k=-\infty}^{\infty} a_k G(f_n - kF_s) \tag{9}$$

By setting the amplitude and phase of each OFDM sub-carrier to match the MSK signal's amplitude and phase at the corresponding frequency, we can shape the OFDM signal to resemble the MSK signal:

$$A_n e^{j\phi_n} = \sum_{k=-\infty}^{\infty} a_k G(f_n - kF_s) \tag{10}$$

Since the amplitude and phase are separate components, we can represent them as:

$$A_n = \left| \sum_{k=-\infty}^{\infty} a_k G(f_n - kF_s) \right| \tag{11}$$

and

$$\phi_n = \angle \left(\sum_{k=-\infty}^{\infty} a_k G(f_n - kF_s) \right) \tag{12}$$

F. I2S Attach Algorithm

We designed a set of algorithms (Algorithms 1 and 2) to modify $S_{\mathrm{OFDM}}(t)$ by finding optimal A_n and ϕ_n for each sub-carrier within the MSK bandwidth. The process results in the creation of a modified OFDM signal, where the optimization seeks a pair that aligns closely with a pre-defined QAM (Quadrature Amplitude Modulation) constellation diagram.

Algorithm 1 Modifying $S_{\mathrm{OFDM}}(t)$

Input: $S_{\mathrm{OFDM}}(t)$
Output: $A_n e^{j\phi_n}$
Generate $S_{\mathrm{MSK}}(t)$ and time samples
Define sub-carrier frequencies
Call algorithm 2 to find the optimal pair
Generate $S_{\mathrm{OFDM}}(t)$ signal using optimal A_n and ϕ_n
return $A_n e^{j\phi_n}$

Algorithm 2 Finding Optimal A_n and ϕ_n

Input: $S_{\mathrm{OFDM}}(t)$
Output: A_n, ϕ_n
Set *min_error* to ∞
Generate a 2048 QAM constellation diagram
LOOP Process
for each A_n and ϕ_n within the MSK bandwidth **do**
  Check if A_n and ϕ_n closely matches a pre-generated constellation point
  Generate a signal from the found pair
  Find MSE and BER between this signal and $S_{\mathrm{MSK}}(t)$
  if error $<$ min_error **then**
    Set *closest_point* to the pair A_n and ϕ_n
  end if
end for
return A_n, ϕ_n

The signal similarity was evaluated using Bit Error Rate (BER) and Mean Squared Error (MSE) as metrics. The

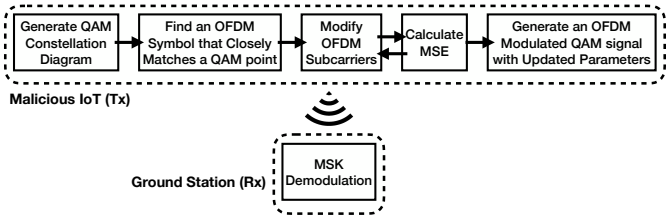

Fig. 2. Flowchart of the Optimization Algorithm

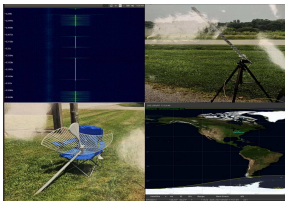

Fig. 3. Hardware Setup and DTUSat-2 Signal

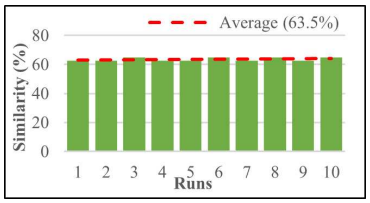

Fig. 4. Signal Similarity(%) over 10 runs

flowchart in Fig. 2 illustrates the sequence of operations executed by the optimization algorithm from the point of signal generation by a potentially malicious IoT device to the reception and demodulation of the signal at a ground station.

G. IoT, Satellite Communication, and MITM

In this section, the proposed methodology illustrates a concrete possibility that we can use OFDM signals to emulate MSK modulations. This emulation scheme opens a door of executing MITM attacks from spectrum shared IoT devices to satellite communications. Furthermore, these findings bring us attention that malicious entities can intercept communications between satellites and ground stations easily by using ubiquitous IoT devices, posing risks of data breaches or misinformation.

IV. Evaluation

In our ongoing evaluation of the I2S Attack on satellite communications, we currently completed two parts.

A. Real-world Satellite Signals Acquisition

We focused on the DTU 2 satellite [5], a notable Low Earth Orbit (LEO) satellite developed by the Technical University of Denmark. For hardware (as shown in Fig. 3), we used an off-the-shelf 2.4 GHz Yagi WiFi antenna mounted on a camera tripod. The antenna was connected to two LNA amplifiers and then to a URSP B210. We used the long-range Bolton satellite to receive signals from the DTUSat-2 satellite. GNURadio was employed to import and analyze signals received from the antenna. This was supplemented by setting a low-pass filter to mitigate associated noise. Additionally, we utilized a variety of tools such as Inspectrum, GPredict, and Gqrx for real-time signal recording and controlling the USRP FPGA. Within GNURadio, and with the help of hardware controls, we also implemented filters like the low-pass filter to further reduce noise in our received signals.

B. I2S Attack Scheme Simulation

We incorporated MATLAB and Python to implement the algorithms introduced in Section III-F. The algorithms aim to find the optimal amplitude and phase shift of each OFDM sub-carrier, that falls within the MSK bandwidth. The simulation first generates a 2048 QAM constellation diagram, and tries matching each amplitude and phase shift closely to a point in the diagram, given the size of the constellation diagram. The loop process of finding a match continues until the most minimal MSE and BER are found, indicating the pair is the most optimal pair for that run. Fig. 4 illustrates an average of 63.5% signal similarity over 10 experimental runs of the optimization algorithm (Fig. 2).

V. Conclusion and Future Work

In this paper, we explore the feasibility and methodology of launching a MITM attack on satellite communications using IoT devices that share the spectrum with satellites (I2S Attack). In a nutshell, amplitude and phase adjustments of OFDM sub-carriers could be made, to mimic an MSK signal. Our approach included both theoretical and practical elements and yielded an average signal similarity of 63.5 % between OFDM and MSK signals. The potential of a low-cost, high-impact attack vector, such as the one we have presented, underscores the necessity for enhanced security strategies in the spectrum of IoT and satellite communications. In our future work, on one hand, we will utilize the collected satellite signals to test our emulation scheme. On the other hand, we will implement our emulation scheme by using USRP.

Acknowledgement

This work is supported in part by NSF grants CNS-2127881 and 2215388. We also thank anonymous reviewers for their valuable comments.

References

[1] C. Kolias et al. “DDoS in the IoT: Mirai and Other Botnets”. In: *Computer* 50.7 (2017), pp. 80–84.
[2] R. Santamarta. *A wake-up call for SATCOM security*. 2014.
[3] R. Prasad. *OFDM for wireless communications systems*. Blackwell Publishing Ltd., 2004.
[4] J. G. Proakis and M. Salehi. *Digital communications*. 5th ed. New York: McGraw-Hill, 2007.
[5] eoPortal. “DTUSat-2 CubeSat Launch”. In: *eoPortal* (2014).
[6] Zhijun Li and Tian He. “WEBee: Physical-Layer Cross-Technology Communication via Emulation”. In: MobiCom ’17.