InfoTech conference
2022 IEEE International Conference on Information Technologies

# Applications of Simulation Modelling Method in Prevention of Jamming Attacks

**Author:** Dr Yoana Ivanova,
Chief Assistant at the Department of Telecommunications
at New Bulgarian University, Sofia, Bulgaria
E-mail: yivanova@nbu.bg

# ABSTRACT

- Background and method
- Aim
- Results and conclusion

# Background and Method

- In cybersecurity the method of simulation modelling has advantages for effective prevention.

# AIM

The aim of this paper is to contribute to development of techniques for cyber defense by a joint application of simulation modelling of a jamming type of DoS (Denial-of-Service) attacks using software Riverbed Modeler Academic Edition 17.5 and jamming antennas using CST Studio Suite 2021.

# Results and Conclusion

The results show that the proposed approach is suitable for determining the severity of cyberattacks due to the complementarity of selected products.

# I. Introduction

Simulation software

Jamming and anti-jamming antennas

A classification of horn antennas

# JAMMING AND ANTI-JAMMING ANTENNAS

- Horn antennas for jamming are:
  - *characterized by a capability to direct radio waves very accurate [1].*
  - *designed to cover a broad frequency spectrum as their applications work mainly at microwave frequencies, UHF (300 MHz to 3 GHz), although their range is wider (150 MHz to 15 GHz) [2].*
- „Anti-jamming uses massive planar antenna arrays“ [3]:
  - *are characterized by a low-cost and ultra-wide band.*

# Simulation Software

- Riverbed Modeler Academic Edition 17.5 - for studying the impact of a jamming attack on a communication network.
- CST Studio Suite 2021 - for simulation of jamming antennas.

# A Classification of Horn Antennas

- For ground platforms;
- For mobile platforms;
- For airborne platforms;
- For fixed platforms;
- Gain standards for calibration.

# CONTENT

| | |
|---|---|
| SECTION II | Presents the background and provides a literature review. |
| SECTION III | Emphasizes on the advantages of a jamming attack simulation using Riverbed Modeler Academic Edition 17.5. |
| SECTION IV | Represents the main concept of the study supported by a comparative analysis of the experimental results obtained from various simulations of cyberattacks on the model of a typical control centre of a management system. |
| SECTION V | It is devoted to the second part of the research related to analysis and simulation modelling of horn antennas which are applicable in jamming and includes a summary evaluation and analysis. |

# II. Related Work

A. A classification of main techniques for detection and prevention of jamming

B. Advanced jamming and anti-jamming techniques in wireless networks

# *A. A CLASSIFICATION OF MAIN TECHNIQUES FOR DETECTION AND PREVENTION OF JAMMING*

- Channel surfing [4]:
  - *can be realized by a specific spectral evasion by "legitimate wireless devices changing the channel that they are operation on".*
- Spatial retreat:
  - *a method based on a spatial evasion characterized by moving legitimate mobile devices away from the location of the DoS emitter [5].*

# *A. A CLASSIFICATION OF MAIN TECHNIQUES FOR DETECTION AND PREVENTION OF JAMMING*

- Randomized channel hoping over multiple channels:

  - *the scheme Quorum Rendezvous Channel Hopping (QRCH) allows nodes to hope over random channels without pre-key establishment, transmitting packets to many receivers at the same time and exchanging pending messages when meet in the limited time interval [6].*

# *A. A CLASSIFICATION OF MAIN TECHNIQUES FOR DETECTION AND PREVENTION OF JAMMING*

- Reactive jamming detection:
  - *„targeting packets that are already on the air "protect the attacker from disclosure [7].*
  - Hermes nodes:
  - *represent hybrid DSSS (Direct-sequence Spread Spectrum) and FHSS (Frequency-hopping Spread Spectrum schemes for prevention of attacks in sensor networks [9].*

# *A. A CLASSIFICATION OF MAIN TECHNIQUES FOR DETECTION AND PREVENTION OF JAMMING*

❑ Trigger control detection:

- *„detection of trigger nodes whose transmissions invoke the jammer nodes“.*
- It aims all target packets to be destroyed while the jamming is performed in the shortest possible time interval [8].

# B. Advanced jamming and anti-jamming techniques in wireless networks

- Prevention by “accurate detection of RF transmissions” and effective jamming, while a packet is still on the air [7].
- Using FHSS:
  - *it opposes fast-following jammers by 55 frequency channels and an average of 1 000 000 hops pers second.*
- Using DSSS:
  - *it is misleading the attacker to perceive the signals as white noise characterized by containing all frequencies and being broadband* [9].

# III. Advantages of Using Simulation Modelling of Cyberattacks for Network Security Analysis

Studying the impact of DoS attacks on control centres

A classification of jammers

# Studying the impact of DoS attacks on Control Centres

- Jamming attacks are a type of DoS attacks where the attacker aims to interrupt communication by transmitting a high-range signal.
- DoS jamming attack blocks the legitimate signals leading to a denial of service [12].

# A Classification of Jammers

- Pulsed jammer (a fixed, a mobile or a satellite node):
  - *this jamming is directed against airborne pulse-Doppler radar [13] that are used for "detection of moving targets" [14].*
- Single band jammer (a fixed, a mobile or a satellite node).
- Frequency-swept jammer (a fixed, a mobile or a satellite node):
  - *this type of jamming is expressed in a fast electronic sweeping of a narrow band of jamming signals in a wide frequency spectrum.*

# IV. A Comparative Analysis of the Results Obtained from Simulations of Cyberattacks

Cases and scenarios in the empirical study

Building simulation models in Riverbed Modeler

A. Summary evaluation and analysis

# Cases in the Empirical Study

| | |
|---|---|
| Case 1 | A reference model $M_{Ref}$ with a firewall. |
| Case 2 | $M_{Ref}$ with a firewall inserted under the impact of a DoS attack simulated by common cyber_effects (Fig. 1). |
| Case 3 | $M_{Ref}$ with a firewall inserted under the impact of a DoS jamming attack (Fig. 2) - the base frequency of the pulse jammer is set to 2401 MHz with 22 MHz bandwidth as in another study using the same simulation environment [16]. |
| Case 4 | $M_{Ref}$ without a firewall inserted under the impact of a DoS jamming attack. |

# Scenarios in the Empirical Study

| | |
|---|---|
| Number | Each of the cases is performed in 6 scenarios. |
| Input Parameters | Interarrival Time (T) of the packets in the range of 0.02 to 2 seconds starting from 2 seconds in Scenario 1 and ending with 0.02 seconds in Scenario 6 for $M_{Ref}$. |
| Output Parameters | End-to-End Time Delay ($T_D$) of the packets. |

# Simulation Models in Riverbed Modeler

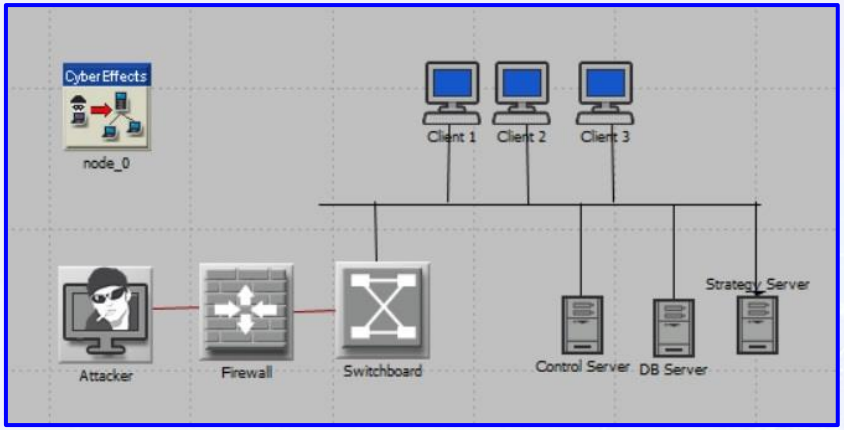



**Fig. 1. A reference model of the control centre $M_{Ref}$ under the impact of a standard DoS attack.**

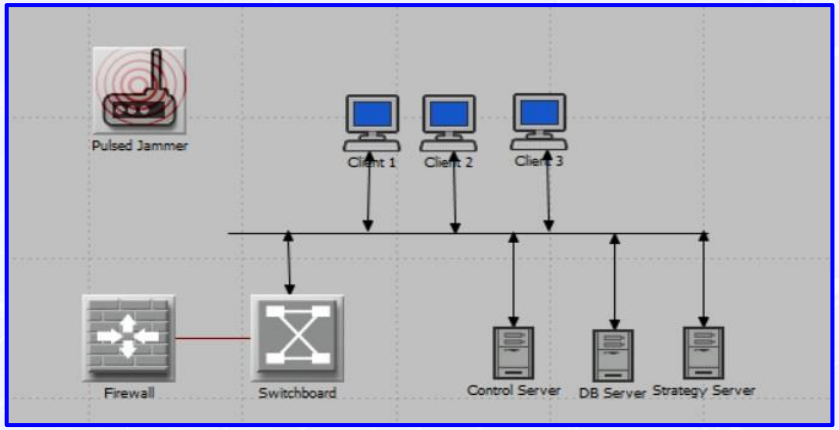



**Fig. 2. A reference model of the control centre $M_{Ref}$ under the impact of a DoS jamming attack.**

# Simulation Results

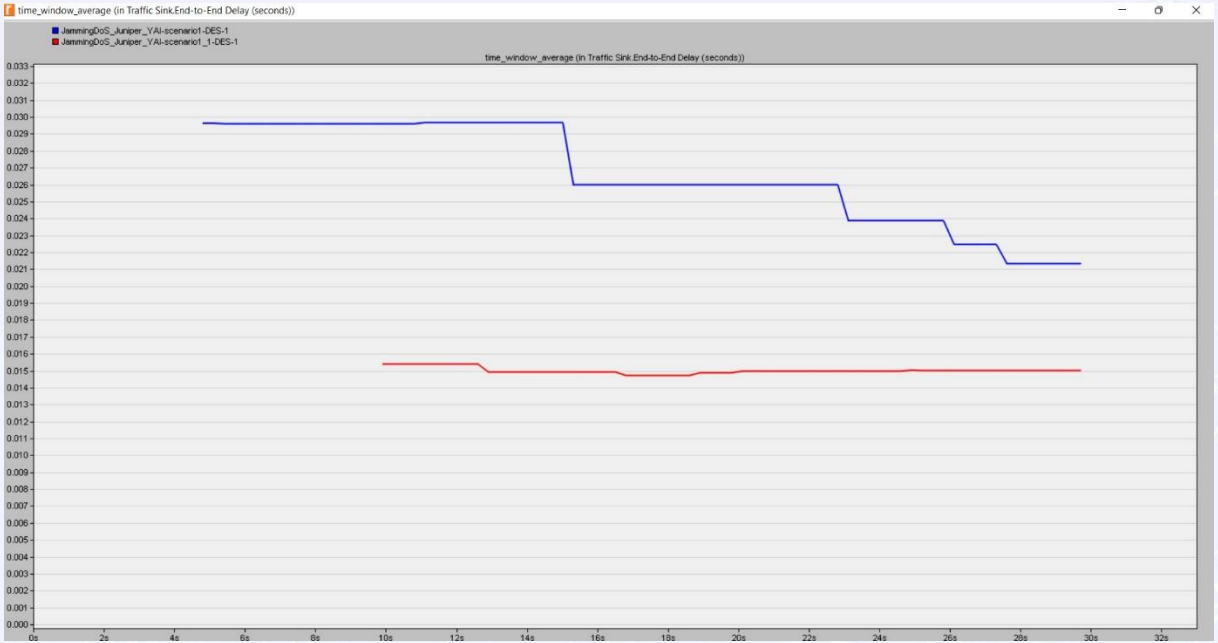



**Fig. 3. The comparative diagram of the time delay in Cases 1 and 2 (T = 2 [s]).**

# SIMULATION RESULTS

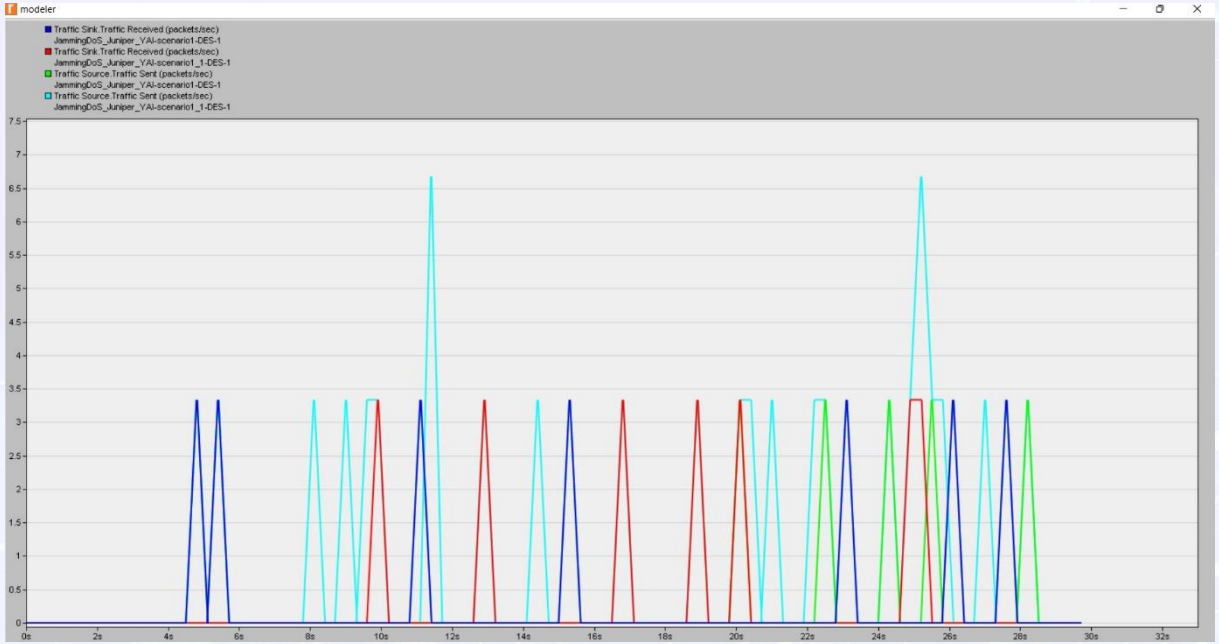



**Fig. 4. The comparative diagram of the packets sent and received per second in Cases 1 and 2 (T = 2 [s]).**

# SIMULATION RESULTS

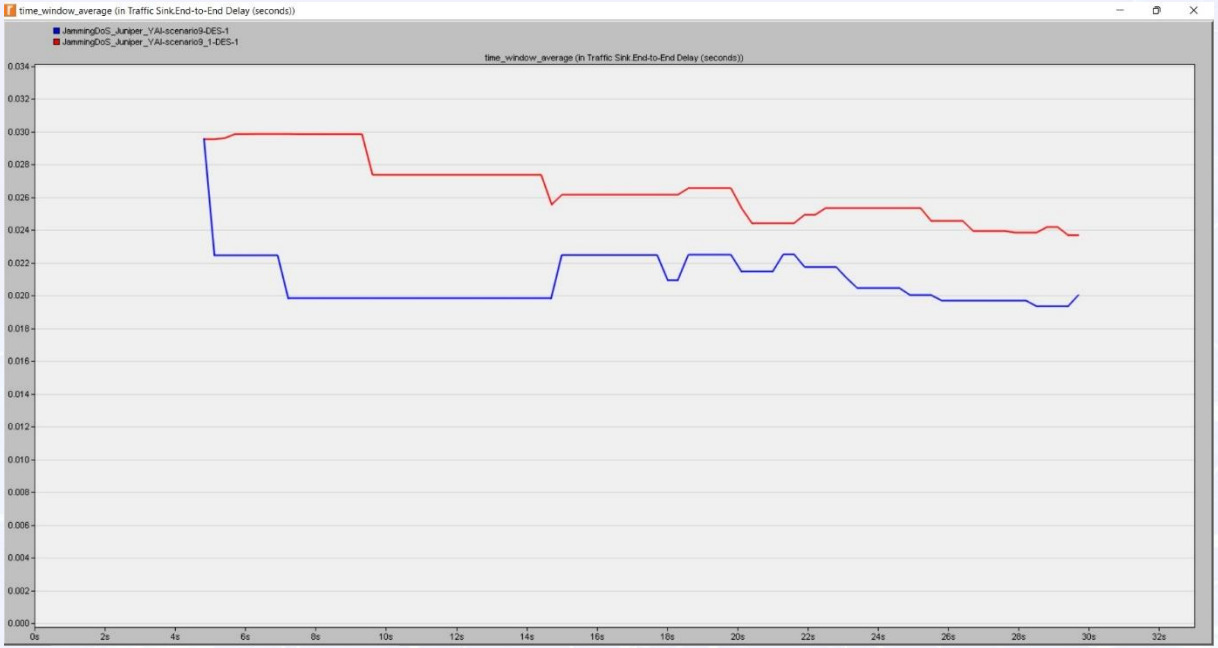



**Fig. 5. The comparative diagram of the time delay in Cases 3 and 4 (T = 1 [s]).**

# A. Summary Evaluation and Analysis

Cases 1 and 2

The conclusion from the comparative analysis of the results in the first two cases in two selected scenarios depending on $T_D$ is that the standard DoS simulated by *cyber_effects* has a stronger negative impact on the control centre, because the firewall does not completely prevent it (Fig. 3).

As the diagram in Fig. 4 shows twice as many packets were sent, as a result of the cyberattack which can be a signal for flooding and subsequent depletion of server computing power.

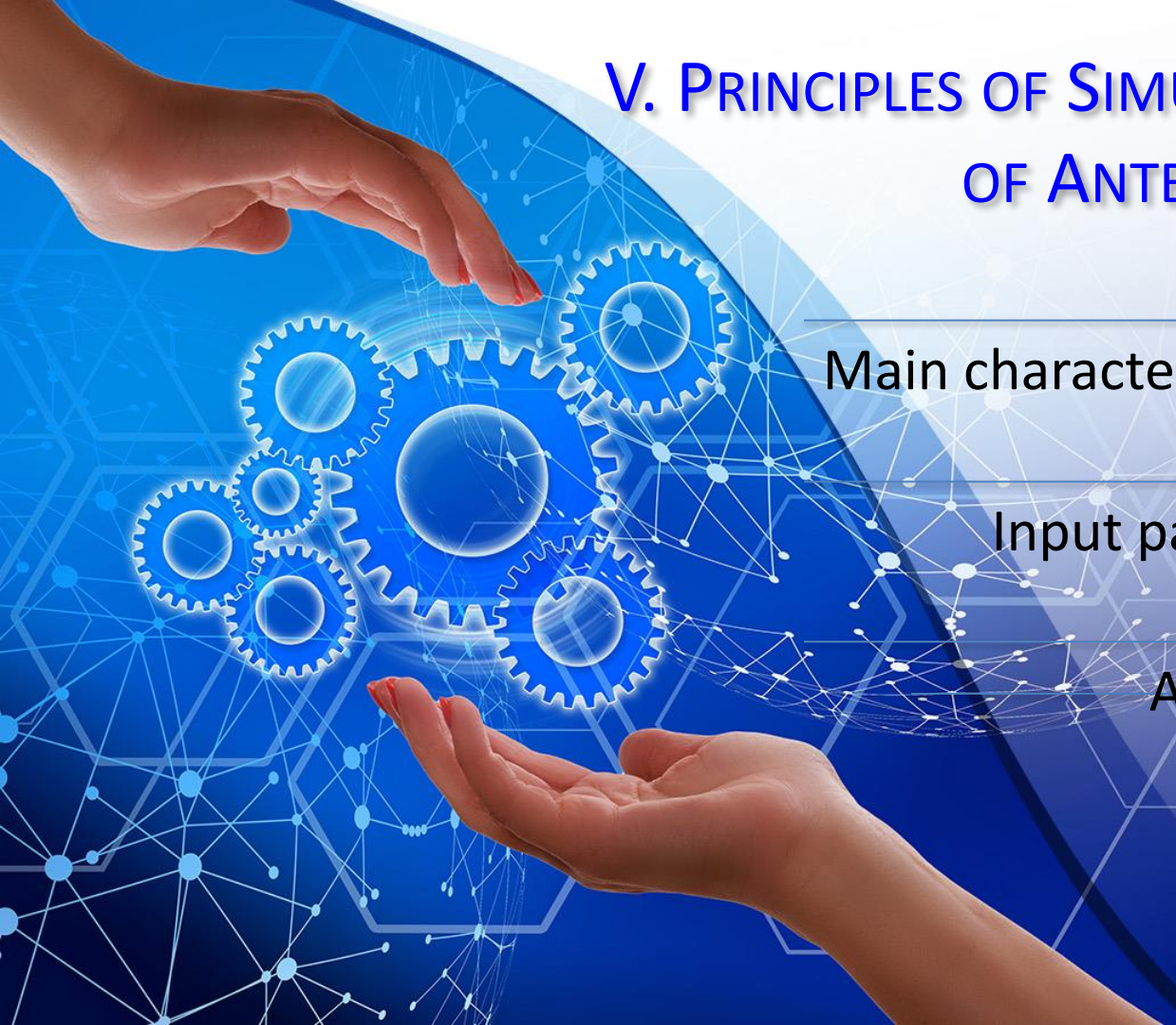
# A. Summary Evaluation and Analysis

**Cases 3 and 4**

The comparative diagram shows $T_D$ in two selected scenarios. In the first of them there is a firewall and no delay because of the jammer, but only due to the firewall (the blue line). In the second scenario no firewall is placed in the network and $T_D$ increases (the red line) – Fig. 5.

**Conclusion**

The simulation results obtained are a reason to assume that the standard DoS attack has a more negative impact compared to a DoS jamming attack in this software.



# V. Principles of Simulation Modelling of Antennas for Jamming and Anti-jamming

Main characteristics of a rectangular horn antenna

Input parameters for antenna modelling

A. Summary evaluation and analysis

# MAIN CHARACTERISTICS OF A RECTANGULAR HORN ANTENNA

- Aperture (A) - the physical area of the aperture.
  - *the emitting opening which have to be at least two times larger than the size of the waveguide.*

$$A_E = \sqrt{2\lambda L_E} \qquad A_H = \sqrt{3\lambda L_H}$$

- e – the efficiency with a value in the interval (0; 1).
- λ - the wavelength.
- $L_E$ and $L_H$ - the slant lengths of the side in the E- or H-field direction [17].

# MAIN CHARACTERISTICS OF A RECTANGULAR HORN ANTENNA

- Optimal gain (G) – if the source is isotropic then it is expressed as:

$$G = \frac{4\pi Ae}{\lambda^2}$$

- Direction (D) - the direction and gain of the antenna increase in direct proportion to the opening area [18].

$$D \approx 10log\frac{10A}{\lambda^2}$$

# INPUT PARAMETERS FOR ANTENNA MODELLING

| Input Parameters, [GHz] | Scenario 1 | Scenario 2 |
|---|---|---|
| **Frequency range** | 0-10 | 0-10 |
| **Farfield/RCS (Radar Cross Section)** | 2; 5; 9 | 4; 6; 8 |
| **Surface current (Transmission Line Matrix)** | 2; 5; 9 | 4; 6; 8 |
| **Electric/Magnetic Energy Density** | 2; 5; 9 | 4; 6; 8 |
| **E-field (Electric field)** | 5 | 9 |

# Simulation Models in CST Studio Suite 2021

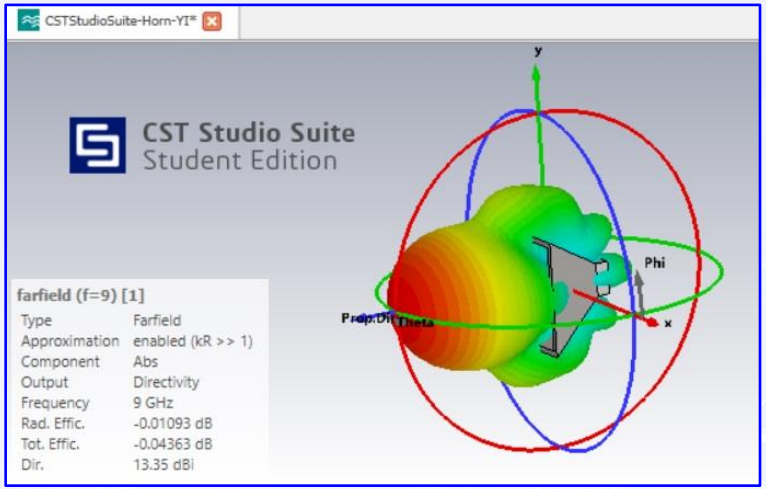



**Fig. 6. The simulation results at farfield (f=9).**

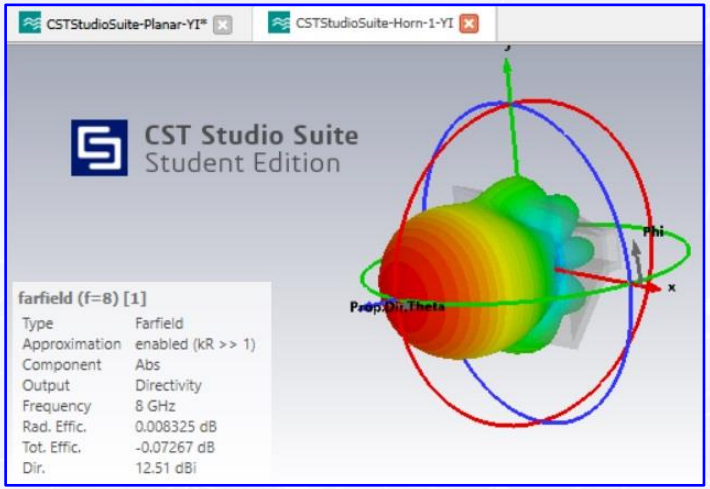



**Fig. 7. The simulation results at farfield (f=8).**

# A. Summary Evaluation and Analysis

| | |
|---|---|
| Output Parameters | They determine the level of effectiveness of a potential jamming. |
| | „Dir.“ is the amount of power that the horn antenna can send or receive in a particular direction. |
| | „Rad. Effic.“ (Radiation Efficency) is the ratio of the power emitted from the antenna to the input power supplied to the antenna excitation port. |
| | „Tot. Effic.” (Total Efficiency) is the ratio of the power emitted from the antenna to the power incident from the network. |
| Conclusion | The efficiency at farfield (f = 9 GHz) is 13.35 dBi. When the frequency is lower with 1 GHz the efficiency decreases to 12.51 dBi. |

# References


[1] C. A. Grosvenor, R. T. Johnk, D. R. Novotny, S. Canales, B. Davis and J. Veneman, National Institute of Standards and Technology Technical Note 1544TEM, Horn Antenna Design Principles, Electromagnetics Division National Institute of Standards and Technology, Boulder, CO 80305, January 2007, pp. 2-3.

[2] TMC Design, Horn Antennas, Available at: http://tmcdesign.com/what-we-do/custom-antenna-design/directional-antennas/horn-antennas/ (Visited on: 20.02.2022).

[3] M. Chehimi, E. Yaacoub, A. Chehaba and M. Al-Husseini, „Physical Layer Anti-jamming Technique Using Massive Planar Antenna Arrays“, 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, June 2020, https://doi.org/10.1109/IWCMC48107.2020.9148405

[4] N. Nain and Santosh K.Vipparthi, „4th International conference on Internet of Things and Connected Technologies, Jaipur, India, Springer (ICIoTCT), May 2019.

[5] W. Xu, T. Wood, W, „Trappe and Y. Zhang, Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service“, WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security, October 2004, pp. 80-89, https://doi.org/10.1145/1023646.1023661

[6] E. Lee, S. Y. Oh and M. Gerla, „Randomized channel hopping scheme for anti-jamming communication“, 2010 IFIP Wireless Days, 22-22 October, Venice, Italy, 2010, https://doi.org/10.1109/WD.2010.5657713

[7] M. Wilhelm, I. Martinovic, J. B. Schmitt and V. Lenders, „Short Paper: Reactive Jamming in Wireless Networks—How Realistic is the Threat?“, 4th ACM Conference on Wireless Network Security, WiSec 2011, Hoboken, NJ, USA 2011, pp. 47-52, https://doi.org/10.1145/1998412.1998422

[8] Y. Xuan, Y. Shen, I. Shin and M. T. Thai, „On Trigger Detection Against Reactive Jamming Attacks: A Clique-Independent Set Based Approach“, 28th International Performance Computing and Communications Conference, IPCCC 2009, 14-16 December 2009, Phoenix, Arizona, USA, pp. 223-230, https://doi.org/10.1109/PCCC.2009.5403842

[9] K. Grover, A. Lim, and Q. Yang. "Jamming and Anti-jamming Techniques in Wireless Networks: A Survey", International Journal of Ad Hoc and Ubiquitous Computing, vol. 17, no. 4, pp 197-215, 2014, http://dx.doi.org/10.1504/IJAHUC.2014.066419

# References


[10] M. Odusami, et al. "An improved model for alleviating layer seven distributed denial of service intrusion on webserver." Journal of Physics: Conference Series. vol. 1235. no. 1. IOP Publishing, 2019, https://doi.org/10.1088/1742-6596/1235/1/012020

[11] M. Odusami, et al. "A survey and meta-analysis of application-layer distributed denial-of-service attack." International Journal of Communication Systems 33 (18), December 2020, https://doi.org/10.1002/dac.4603

[12] O. Osanaiye, A. S. Alfa, and G. P. Hancke, „A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks“, Sensors (Basel), 2018; vol. 18 (6), 1691, https://doi.org/10.3390/s18061691

[13] F. Y. Li, J. Xu and X. D. Zhang, „Pulse jamming suppression for airborne radar based on joint time-frequency analysis“, IET International Radar Conference 2013, 2013, ISBN:978-1-84919-603-1, https://doi.org/10.1049/cp.2013.0387

[14] X. Jiang, F. Zhou, S. Chen and H. He, „Jamming Resilient Tracking Using POMDP-Based Detection of Hidden Targets“, IEEE Transactions on Information Forensics and Security 16:983-998, January 2021, http://doi.org/10.1109/TIFS.2020.3027145

[15] Britannica, Doppler effect, https://www.britannica.com/science/Doppler-effect

[16] H. S. Obaid, „Wireless Network Behaviour during Jamming Attacks: Simulation using OPNET“, Journal of Physics Conference Series 1530(1):012009, May 2020, http://dx.doi.org/10.1088/1742-6596/1530/1/012009

[17] Electronics Notes, „Microwave Horn Antenna Theory“, Available at: https://www.electronics-notes.com/articles/antennas-propagation/horn-antenna/theory-equations.php (Visited on: 20.04.2022).

[18] Radartutorial, Ruporen oblachvatel, Available at: https://www.radartutorial.eu/03.linetheory/tl50.bg.html (Visited on: 20.04.2022).

Dr. Yoana A. Ivanova
Department of Telecommunications,
New Bulgarian University
21, Montevideo Blvd., 1618 Sofia, Bulgaria
yivanova@nbu.bg

# Thank You for Your Attention!