International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Autonomous Signal Deception and Offensive System for Battlefield Application

P. Dr. K. Rama Linga Reddy, Penumarty Srilakshmi Bhanupriya, Nikitha Mora, B. Suchitra, Sruthi Gujjula
Electronics and Telematics Engineering
G. Narayanamma Institute of Technology and Science Hyderabad, India

Abstract- — The paper describes the design of an Autonomous Signal Deception and Offensive System to be used at the Battlefield - a Simulink-based RF electronic warfare (EW) simulation system based on an earlier created hardware prototype, the Ultrasonic Deception System. In the previous system, four deception methods, including range deception, angle deception, stealth, and noise injection are shown with Arduino Mega and ultrasonic sensors, and the choice of the technique is done manually by an operator. The proposed system completely removes any manual involvement and adds five important extensions: autonomous selection of deception techniques with a randomized decision engine, an offensive electromagnetic pulse (EMP) generation subsystem, a cryptographic Identification Friend or Foe (IFF) protocol based on challenge-response authentication via XOR operations and pre-shared secret keys, an accurate RF channel model including path loss, propagation delay, and additive white Gaussian noise (AWGN). This system is implemerandi-based technique selection, and a Countermeasure Generation block that generates high-amplitude EMP pulses. The results of simulations show that autonomous threat classification is successful, the deployment of unpredictable deception techniques, and the possibility to quantify the degradation of the enemy system. Performance is analyzed based on six metrics such as IFF classification accuracy, deception effectiveness, SNR degradation, Shannon channel capacity, deception unpredictability entropy and system health degradation rate.

Keywords— Electronic Warfare, Signal Deception, Identification Friend or Foe (IFF), Electromagnetic Pulse (EMP), Superheterodyne Receiver, Simulink RF Simulation, Autonomous Decision Making, AWGN Channel, Challenge-Response Authentication, Electronic Countermeasures (ECM).

I. INTRODUCTION

The main battlefield of electronic warfare now is the electromagnetic spectrum. Countries and military services put a lot of resources into the systems that are able to identify, jam, deceive and neutralize the enemy RF activity since tactical and strategic edge on the battlefield is the direct result of the control over the spectrum. Electronic warfare has three general areas: Electronic Attack (EA), offensive actions against enemy systems; Electronic Protection (EP), defending own systems against EA by adversaries; and Electronic Support (ES), monitoring and analysis of the electromagnetic environment. In these areas signal deception, the art of bending reflected or retransmitted signals to fool enemy senses, plays a peculiarly significant role. Deception techniques may disable even technologically advanced platforms of the enemy without any kinetic engagement, by disorienting the enemy's perception of distance, direction, signal strength or channel integrity.

Although EW has been identified as being of strategic importance, there is a dire lack of open research platforms available to facilitate the development and testing of autonomous EW algorithms. Real EW systems are classified, cost millions of dollars to develop, and are inaccessible to academic researchers. Current simulation platforms are either commercial or too specific to enable combined research on deception, identification, and offensive subsystems in a single platform. This is the reason why this gap is inspiring open, accessible simulation testbed in which autonomous EW strategies can be prototyped, tested, and benchmarked under realistic signal conditions. The current study fills this gap by creating an RF EW simulation environment based on Simulink that incorporates autonomous deception, cryptographic IFF, offensive EMP generation, and realistic RF channel modelling into a single, workable system. This project is a continuation of a previous hardware prototype, the Ultrasonic Deception System, that was built on a breadboard with an Arduino Mega microcontroller and two ultrasonic sensors. The prototype showed four deception methods: range deception through time-offset addition, angle deception through servo-controlled phase manipulation, stealth through signal attenuation modeled using a piezo plate, and noise-injection by a 555 astable multivibrator circuit. As a demonstration of concept, the prototype had three inherent weaknesses: All choices of deception techniques needed to be made by hand using push-button controls, the system only worked in the ultrasonic frequency range which is fully non-representative of actual battlefield RF

communications, and the system lacked any offensive capability (or any means of identifying friendly transmissions and enemy emissions). The above limitations are resolved systematically in the proposed simulation framework.

II. RELATED WORK

Zheng et al. [1] suggested a Deception-As-Defense Framework of Cyber-physical Systems, which views defensive deception as a game-theoretic optimization problem. The framework, based on a hierarchical equilibrium, shows Nash equilibria can be developed to formulate deception strategies, which offer provable guarantees of the effectiveness of deceptive responses in the adversarial circumstances. Although this work provides a sound mathematical basis to deception-based defense, it does not focus on the issue of autonomous selection between variants of deception techniques in real-time RF settings, or on an offensive subsystem, nor does it include an identification protocol to identify friendly and enemy transmissions.

Kenney [2] discussed the Fight for Spectrum Superiority and Cognitive Electronic Warfare and showed how machine learning algorithms can be implemented into EW systems to perform a continuous analysis of spectrum conditions and dynamically adjust countermeasures. The article demonstrates the use of cognitive EW systems to enable spectrum dominance via adaptive sensing and response that is superior to the performance of fixed rule-based systems in contested electromagnetic space. This work, however, is about spectrum management and frequency agility, and not about signal-level deception schemes or cryptographic identification schemes. This direction is complemented by the current work which introduces a simulation testbed where the choice of cognitive strategies can be tested on the signal processing level.

In Real-Time Detection of Deception Attacks in Cyber-Physical Systems, Mozaffari et al. [3] came up with algorithms that use both statistical threshold-based anomaly detection and machine learning pattern recognition to detect deception attacks in real time. The work shows a high detection accuracy in an array of adversarial signal injection strategies. It is worth noting that this paper is focused on the issue of how to detect deception and not create it, and does not take into account the creation of offensive countermeasures. The current work adopts a complementary approach - the creation of the deception generation and attack aspect of the EW equation - the two works are therefore natural complements in a full EW research programme.

Together, these publications put the game theoretic, cognitive, and detection side basis of contemporary EW studies but introduce the challenge of bridging the gap between autonomous multi-technique deception generation, cryptographic IFF and offensive EMP capability into a single framework which is available to open academic research. This gap is filled by the current work.

Scope of Work

The proposed Autonomous Signal Deception and Offensive System to be used in battlefield applications offers new inputs. The environment offers the initial open, publicly available Simulink-based platform to prototype and evaluate autonomous EW strategies, bridging the current gap posed by secretive and costly real systems. A randi-based randomized decision engine is used to adaptively choose between four deception techniques - range deception, angle deception, stealth, and noise injection - that is, removing human intervention and maximizing Shannon entropy ($H = \log 2(4) = 2$ bits) in technique selection, and hence making the system as unpredictable to adversaries as possible. A challenge-response IFF protocol, implemented in Simulink, uses XOR operations on an 8-bit shared secret key to verify friendly transmissions.

The chances of a random 8-bit response coinciding with the expected response are $(1/2)8 = 0.39\%$, which can be used to prove the cryptographic strength of the classification mechanism. High-amplitude electromagnetic pulse generation module is a model of the attack capability at the hardware-layer of real EW systems with pulse amplitude of 1000 times normal signal amplitude and random factor of damage to assure unpredictable attack intensity. The RF channel includes free-space path loss (a gain of 0.1), propagation delay (modelled using transport delay block), and AWGN noise, which give a physically-grounded signal propagation environment to simulate. The system simulates an adversary (enemy RF EW unit) and our autonomous EW system (blue team) related to one another by the shared RF channel, and allows an adversarial test of the strength of deception strategies. A post-simulation data logging MATLAB tool measures 14 signal parameters at every timestep and generates timestamped CSV datasets that can be used to train machine learning models to act as autonomous EW systems in the future. A table showing how earlier works and the proposed model differ from one another on the above list of parameters is given below in TABLE I.

Table 1: Comparison of Existing Electronic Warfare Systems With the Proposed System

Criteria	Deception-as-Defense Framework [1]	Cognitive Electronic Warfare [2]	ML-based EW & Detection Models [3]	Proposed Ultrasonic Deception System
Detection Capability	Based on system state estimation	Adaptive signal sensing using AI	Automated anomaly detection.	Real-time signal classification using secure IFF
Deception capability	Strategic information manipulation	Limited, mostly adaptive responses	Minimal deception support	Multi-strategy deception (noise, stealth, angle, range)
Decision Making	Theoretical / model-based	Adaptive but partially autonomous	ML-driven but data-dependent	Fully autonomous real-time decision-making
Security Authentication	Not explicitly addressed	Limited	Physical-layer or ML-based	Secure authentication using decoding protocol
Computational Complexity	High (game-theoretic models).	High (AI/ML integration)	High (training-intensive models)	Optimized for efficient simulation and real-time use.
Real-Time Capability	Limited.	Moderate	Moderate	High; supports real-time adaptive response
Offensive Capability	Not included	Not included.	Rarely considered	Integrated offensive subsystem.
Scalability	Limited practical deployment	High but resource-heavy	Moderate to high	Highly scalable modular design.
Data Handling	Not emphasized	Data-driven learning	Requires large datasets.	Integrated data logging and monitoring
Practical Applicability	Mostly theoretical	Research-oriented	Experimental setups.	Designed for realistic simulation and future deployment

Table 2: Feature Comparison of Existing Approaches and Proposed System

Parameter	Existing Systems	Proposed System
Approach	Jamming / Detection-focused	Deception + Authentication + Offensive
Techniques Used	Interference, basic ML	Multi-layer deception strategies
Environment	Simplified or controlled	Realistic RF simulation (Simulink)
Autonomy	Low to Moderate	Fully autonomous
Security	Limited	Strong (IFF-based authentication)
Parameter	Existing Systems	Proposed System
Adaptability	Limited	Dynamic and adaptive
Output	Signal disruption	Signal manipulation + targeted response

Current electronic warfare systems demonstrate development through their jamming capabilities and their machine learning functions and their simulation ability, but they do not possess autonomous operation or robust identity verification or complete integrated attack functions as shown in TABLE II.

III. SYSTEM ARCHITECTURE AND BLOCK DIAGRAMS

Th The proposed system, Sketch Rush, is a real- time multiplayer web application designed to replicate and enhance the experience of playing the classic Pictionary game. It is built on a client- server architecture using Node.js and WebSockets to ensure synchronized, low-latency interaction. The system is designed to be accessible, requiring no installation or specialized hardware beyond a standard web browser and an internet connection. System Architecture The architecture of Sketch Rush is divided into two main components: the Client-Side Application and the Server-Side Application. The client is responsible for rendering the user interface, capturing user input (drawing and text), and displaying the game state. The

server manages game logic, session state, and real-time communication between clients.

Fig. 1. Block Diagram

Fig. 1 The diagram shows an RF system where the blue team processes signals and the red team creates interference. A dummy unit helps identify friend vs enemy signals

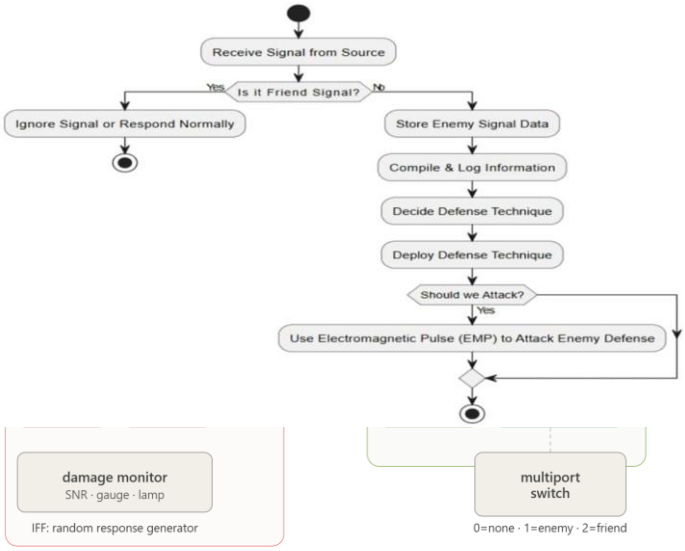

Fig. 2. Flow chart

Fig. 2 Flowchart of an autonomous system that classifies signals and applies deception or attack based on threat detection. The Baseline RF EW Unit is a series of four subsystems that include the RF Front End (RF FE), Signal Processing Unit (SP Unit), Decision Making Unit (DMU) and Countermeasure Generation block (CMG). The RF FE deploys a superheterodyne receiver structure to detect and precondition the arrival of RF emissions. The SP Unit implements the cryptographic IFF protocol to distinguish between a detected transmission that is friendly and hostile. The DMU puts in place the autonomous deception logic based on the IFF decision. The CMG produces EMP pulses when a threat is detected. The Enemy RF EW Unit is a manually operated RF emitter that has a damage monitoring subsystem that is used to visualize the effects of deception and EMP attack. The Friend Unit is a constantly transmitting unit which responds to IFF challenges with the appropriate cryptographically calculated response. The entire inter-uni

1. RF Front End (RF FE)

The RF Front End is the sensory interface of the baseline EW unit. It works by accepting incoming RF emissions, processing them via a superheterodyne processing chain, and providing a digitized signal of energy as a representation of the power of the emission detected. Its implementation is based on the classical superheterodyne receiver architecture, which has the following stages in that order. The input RF signal is then sent through an analog Butterworth bandpass filter, in a MATLAB Function block, centered on the band of frequencies of interest. This preselector filter eliminates out of band interference in advance of amplification. A Low Noise Amplifier (LNA) that is modelled as a Gain block amplifies the filtered signal. After amplification, a Local Oscillator (LO) sine wave of higher frequency is mixed with this signal and the frequency of this signal is adjusted to be lower than that of the incoming RF signal. The product-to-sum trigonometric identity generates sum and difference frequency componentωc = 5 rad/s, and message frequency ωm = 2 rad/s. The frequency of LO will be ωLO = 12 rad/s which will give the IF of ωIF = ωLO - ωc = 7 rad/s. The RF channel path loss decreases the amplitude of the signal by 0.1 and LNA reinstates the signal to a functional level.

2. Signal Processing Unit (SP Unit)

Signal Processing Unit is the cognitive part of classification of the system. Its only purpose is to select a cryptographic challenge-response IFF protocol to identify whether the detected transmission is by a friendly or hostile unit. The SP Unit takes two inputs; the conditioned RF signal of the RF Front End and the IFF response signal of the unknown transmitting unit coming through the RF channel. It generates three outputs: the binary IFF decision (logic 0 = friend, logic 1 = enemy), the challenge sequence to be sent to the unknown unit, and the original RF signal that will be sent to the downstream deception processing.

The IFF protocol works in the following way. The Random Integer Generator (binary output version) with 8 samples per frame produces a random 8-bit challenge sequence each simulation timestep. A Memory block is used to stabilize the challenge between samples to avoid timing mismatch due to RF channel propagation delay. The challenge is both passed on to the unknown unit via the RF channel and XOR-combined with a stored secret key of 8 bits to calculate the expected answer. A Transport Delay block delays the response that is expected to be received to match the response that is actually received by the RF channel after propagation delay. A Relational Operator compares the expected and received responses bitwise. MinMax block set to minimum operation on all 8 comparison bits compares all bits at once, ensuring that they are all equal. The product is fed to a NOT gate to encode all-matching (friend) to logic 0 and any-mismatch (enemy) to logic 1. A

friendly unit responds to the challenge by XOR-combining it with

3. Decision Making Unit (DMU)

The Tactical response engine of the baseline EW unit is its Decision-Making Unit. It accepts the original RF signal, the IFF decision, and uses one of four independent deception techniques on the signal in case a threat is detected. It is implemented with a Switch block as the main routing gate: with the IFF-decision logic 0 (friend), the RF-signal is sent directly to the output without processing; with logic 1 (enemy) it is sent through a MATLAB Function block containing the deception engine. The deception engine expresses the formula mod (floor (rand ()4), 4) + 1 to get a uniformly distributed random integer in the set of [1, 4] in each execution cycle, and is run to drive a switch-case representation of the four deception techniques. The range deception amplifies the signal by a random delay factor larger than one, and distorts the distance calculation of the enemy, which relies on time-of-flight. An offset in the apparent propagation time is added by the modified signal y = u × (1 +0.5 × rand ()) and is randomized. The angle deception implements a random phase shift y = u × cos (2π × rand ()), and disturbs the direction-finding calculations of the enemy. Stealth silences the signal to one-tenth to one-fifth of its original strength by y = u × (0.1 + 0.1 × rand ()), a model of electromagnetic camouflage. Noise injection boosts the signal by a random noise value y = u × (2 × rand () -1), and replaces the communication channel with an incoherent waveform. The extra rand () calls in each technique guarantee that it is double-layered randomness - unpredictable not only in type of technique but also in magnitude.

4. Countermeasure Generation (CMG)

The offensive subsystem of the default EW unit is the Countermeasure Generation block. It accepts one input, the binary IFF decision and produces an EMP pulse once a threat is detected. The pulse is given by the expression y = EMP amplitude x damage factor x exp (-rand), with the EMP amplitude = 1000 modeling a voltage spike that is significantly larger than PCB component ratings, damage factor = 1 + 0.5 rand modelling a randomized pulse shape and the exp(rand) term creates a sharp exponential shape pulse, which is comparable to the Dirac delta transient of actual EMP events. The pulse is sent over the RF channel to the Damage Monitor subsystem of the enemy unit.

5. RF Channel

There are three basic phenomena of electromagnetic wave propagation modeled in the RF channel. Path loss is modeled as a Gain block of 0.1, which (at a distance) corresponds to 90 percent signal power loss in the battlefield in line with the inverse square law of free-space propagation. A Transport Delay block is a model of propagation delay, the finite-time-of-flight of electromagnetic signals between units, at the speed of light. Additive White Gaussian Noise is represented by a Band-Limited White Noise source whose power is varied with regard to the performance analysis test matrix. The signal channels of the channel, enemy RF emission, IFF challenge, IFF response, decepted signal and EMP pulse, are each propagated through a separate pipeline of these three effects.

6. Enemy RF Channel

The Enemy RF EW Unit is a non-intelligent red team enemy to be used as a demonstration and performance evaluation system. Its emission subsystem is provided with a Manual Switch to switch a continuous AM-modulated RF signal, which enables the operator to switch between enemy transmission on and off when simulating. The blue team SP Unit presents the challenge to the IFF response subsystem, which disregards it, resulting in a random 8-bit sequence of Booleans, which ensures a failure in IFF protocols. The blue team CMG feeds to a Damage Monitor subsystem, which visualizes the pulse's effect by displaying four indicators simultaneously a Scope displaying the pulse waveform, a Display displaying the SNR value in decibels, a Dashboard Gauge showing degrading health of enemy systems (a number between 1.0 and 0.0) and a Lamp indicator which changes to red when the pulse amplitude surpasses.

7. Enemy RF Channel

The Dummy Friend Unit is a support transmitter which illustrates the proper working of IFF protocol in a friendly environment. It sends a constant RF signal at the same frequency as the enemy unit - a reflection of the real-world scenario of friendly and enemy units operating on the same frequency bands - and reacts to IFF challenges with the cryptographically correct XOR response with the same pre-shared secret key. When the blue team SP Unit gets the appropriate response, the transmission is classified as friendly, logic 0 is propagated to the DMU and CMG, no deception is used, no EMP is produced and the Damage Monitor indicators display the healthy system status. Such a situation of contrast gives the best possible illustration of the discriminatory nature of the IFF protocol.

IV. PERFORMANCE ANALYSIS

The analysis of performance is done based on six metrics that all assess the IFF accuracy of the system, the effectiveness of the deception, the offensive capabilities, the channel robustness, the unpredictability and the progression of the damage. Analysis proceeds according to the sensitivity analysis

structure: the power of noise is varied based on five levels (0.0001, 0.001, 0.1, 0.100) with all other parameters kept constant, and indicates the extent to which the system performance is impacted by a progressively adversarial channel environment.

1. IFF Classification Accuracy.

IFF Classification Accuracy is used to determine the percentage of correctly classified transmissions in a series of simulation runs. It is defined as:

Accuracy (percent) = (Correct Classifications/Total Signals) × 100.

In friendly transmissions, the accuracy of the classification is theoretically 100 percent since the XOR-based response computation is deterministic - using the same challenge and the same secret key, the correct response is always obtained. In the case of enemy messages, the chance of false classification (enemy is wrongly identified as friend) is (1/2) 8 = 0.39 which provides a theoretical enemy classification accuracy of 99.61. The higher the noise power in the RF channel, the more the bit errors in the transmitted response will reduce the classification accuracy.

Noise Power	SNR (dB)	Friend Acc. (%)	Enemy Acc. (%)	Bit Error Rate	Channel Condition
0.0001	30.97	[TBD]	[TBD]	[TBD]	Clean
0.001	20.97	[TBD]	[TBD]	[TBD]	Slight noise
0.01	10.97	[TBD]	[TBD]	[TBD]	Moderate
0.1	0.97	[TBD]	[TBD]	[TBD]	Severe
1.0	-9.03	[TBD]	[TBD]	[TBD]	System failure

Fig 3 shows the predicted IFF accuracy with respect to noise levels.

Fig. 3. IFF Classification Accuracy vs. Noise Power B. Deception Effectiveness

Effectiveness of deception measures the level of success of each method in corrupting the signal perception of the enemy. To measure the effectiveness of a range deception, the degree of error between the real and perceived distance to the enemy is determined:

Range Error (%) = |d_actual − d_perceived| / d_actual × 100

In the case of angle deception, the angular error, in degrees, of the true bearing and the deceived bearing are measured. To express the signal attenuation factor as a percentage of original amplitude, the signal attenuation factor is given in percent. In the case of noise injection, Signal-to-Interference-plus-Noise Ratio (SINR) at the enemy receiver is calculated. As the choice of technique is random, the effectiveness of deception is averaged over several simulation runs at each noise level. [Results to be completed on completion of simulation].

3. SNR Degradation during EMP Attack

The SNR degradation is used to measure the effect of EMP attack on the integrity of enemy systems. Signal-to-Noise Ratio =:

SNR (dB) = 10 × $\log_{10}$ (Signal Power / Noise Power)

Noise Power	Signal Power	SNR Linear	SNR (dB)	Condition
0.0001	0.125	1250	30.97	Clean
0.001	0.125	125	20.97	Slight
0.01	0.125	12.5	10.97	Moderate
0.1	0.125	1.25	0.97	Severe
1.0	0.125	0.125	-9.03	Failure

Fig 4: SNR Analysis at RF Channel Output

The RF Front End output SNR of the enemy system is recorded prior to EMP activation, and at the conclusion of each EMP pulse. The EMP is a noise source which is injected and whose power is proportional to the amplitude of the pulse. The drop in SNR in decibels is a direct measure of how much there has been degradation of sensing capability. When SNR decreases to an operational limit of less than -10 dB, the system is declared damaged and the energy detector of the enemy is not able to confidently sense any transmission anymore. Fig 4 shows the SNR values at the RF channel output of the five levels of noise power used.

4. Channel Capacity Analysis

The impact of noise injection deception of the capacity of enemy communication channels is discussed by the Shannon-Hartley theorem:

$$C = B \times \log_2(1 + SNR)$$

C is channel capacity, in bits per second, B is the normalised bandwidth (normalised to 1 Hz to normalise analysis), and SNR is the signal-to-noise ratio, on a linear scale. Noise injection deception decreases the SNR at the enemy receiver which decreases channel capacity directly. At very high noise injection levels, the channel capacity is close to zero, that is, it has the ability to completely deny communication. [Values to be filled when simulation is done].

5. Deception Unpredictability Index

Shannon entropy quantifies the uncertainty of the autonomous choice of a technique used in deception:

$$H = -\Sigma\, p(i) \times \log_2(p(i)) \text{ for } I \in \{1, 2, 3, 4\}$$

As the randi([1,4]) function generates a uniform discrete distribution, the p(i) = 0.25 of all four methods. The Shannon

entropy is $H = \log_2(4) = 2$ bits - the maximum possible entropy of a four-outcome distribution. This maximum entropy value gives formal evidence that the autonomous mechanism of selecting technique is maximally unpredictable to an adversary, ruling out the possibility of adaptive preparation of countermeasures by recognising patterns of techniques. Distribution uniformity across all four techniques is anticipated to be empirically validated by running multiple simulations.

6. System Degradation rate of Health

Enemy system health This is a continuous variable that declines between 1.0 (operating fully) to 0.0 (wholly destroyed) in response to the cumulative exposure to EMP:

$$\text{Health}(t) = \max(0, 1 - \text{EMP\_power}(t) / 1000)$$

The health value is monitored throughout the simulation period and represented by Damage Monitor Gauge block. Gradual exposure to EMP speeds up the deterioration of health, and the system is pronounced non-functional when health becomes less than 0.1. This damage of factor = 1 + 0.5 × rand () element is such that every successive EMP pulse will have a different magnitude so that the enemy cannot predict the rate at which the health is being damaged and adjust his defensive stance to it. [Health-degradation curves to be added on completion of simulation].

V. CONCLUSIONS

The development of an Autonomous Signal Deception and Offensive System represents a significant evolution in modern warfare, where dominance in the electromagnetic spectrum is as critical as control over land, air, and sea. By integrating advanced sensing, adaptive algorithms, and real-time decision-making, such systems can effectively disrupt enemy communications, mislead surveillance networks, and create strategic advantages without direct physical confrontation.

However, the deployment of autonomous offensive technologies also raises important considerations. Issues surrounding reliability, escalation risks, ethical boundaries, and compliance with international laws must be carefully addressed. Human oversight, robust fail-safes, and clear operational doctrines are essential to ensure that these systems are used responsibly and do not lead to unintended consequences.

In conclusion, while autonomous signal deception systems offer powerful capabilities for future battlefields, their success will depend not only on technological sophistication but also on disciplined governance, ethical deployment, and strategic restraint.

REFERENCES

1. D. Zheng et al., "Deception-As-Défense Framework for Cyber-Physical Systems," IEEE Transactions on Dependable and Secure Computing, 2021.
2. J. B. Kenney, "Cognitive Electronic Warfare and the Fight for Spectrum Superiority," IEEE Signal Processing Magazine, 2020.
3. M. Mozaffari et al., "Real-Time Detection of Deception Attacks in Cyber-Physical Systems," IEEE Internet of Things Journal, 2022.
4. D. Adamy, EW 101: A First Course in Electronic Warfare, Artech House, 2001.
5. C. E. Shannon, "A Mathematical Theory of Communication," Bell System Technical Journal, vol. 27, pp. 379–423, 1948.
6. MathWorks, MATLAB/Simulink Documentation, https://www.mathworks.com, 2024.
7. NATO Standardization Office, "Identification Friend or Foe Mode 5 Standards," STANAG 4193, 2019.