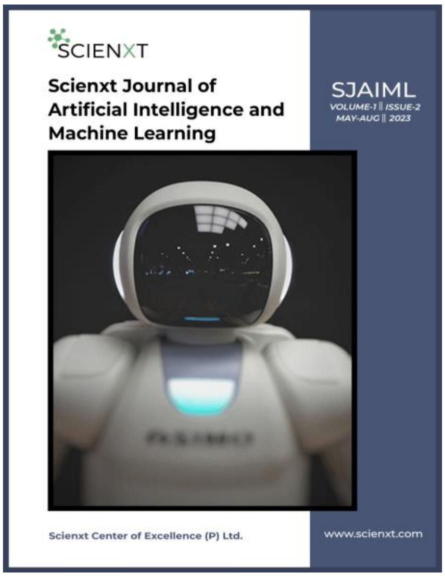

Scienxt Journal of Artificial Intelligence and Machine Learning
Year-2023|| Volume-1|| Issue-2||May- Aug|| pp. 29-42

Improved embedded AI application in Defense UAV

Uma Perumal[*1]
Assistant professor, Department of Artificial Intelligence and Machine Learning
Virudhachalam Taluk, Tamil Nadu, India

Vasantharajan Renganathan[2]
Assistant professor, Department of Artificial Intelligence and Machine Learning
Virudhachalam Taluk, Tamil Nadu, India

**Corresponding Author: Uma Perumal*
Email: rajavasanth2079@rediffmail.com

Abstract:

Improved embedded systems uses existing UAV/drone tech hardware with AI, Deep Learning Networks in addition to existing software to run an autonomous or user driven UAV. Here additional hardware is installed to monitor real-time data, compare with available, preloaded, and pre-recorded data for authenticity and reliability to perform tasks. Some additional safety protocols are also included to deal with dangerous and uncertain situations by spoofers, anti-drone systems and attacks by other objects that may occur at the time of flight.

Fog computing techniques with a redundant processor in addition to working and software abilities powered with decisive cross-referencing techniques such as a human or any living being can do to act according to real-life situations can provide independent capability to sustain itself and be free of depending on command center for every action in a hostile environment, that must be performed.

Keywords:

Fog computing, Adversarial AI, Theory of Mind, Drone AI, Out of Box Thinking AI, Self-Aware AI.

1. Introduction:

Every single piece of information from a hostile in the battlefield has the capacity to change the course of a battle from defeat to huge victory. Data which was then only in the laboratories for analyzing are now getting in real time with a dynamic perspective that changes with time and location. Command Center's (CC) communicating with drones are getting out of trend as adversarial AI now "thinks on its own" and act accordingly to bring down delay due to communication and chances of spoofing, hacking of communications in an electronic warfare environment.

Sensors mounted on UAV's can provide data of significance about the parameters required for the calculation by the processor to make necessary alteration or change during travel or action in the battlefield. But the data obtained must be of good quality ranging from data trueness dictating its reliability. These days sensors mounted on the UAV's can be easily rigged for misinformation, hacked to provide unreal or false data or be used against the original user by hostiles with various intelligent techniques like Radio Jamming, Detect, Hacking, Denial Of Service (DoS), Hijack (Bind before owner, overpower fixed frequency/fixed ID), Intercept, Backdoor, Reverse engineering, Leased AWS keys, Spoofing and attacking hardware using trained birds (like eagles) to shut, bring down or destroy the whole UAV.

Attack on users UAV to disrupt the operations by hostiles using new trending tech is a continuing story of no end, but the ways to tackle the same using AI, Deep Learning are trending. Fog computing and Edge computing are used to train UAVs in different situations by simulating the same have bought some success, but new areas need to be improved.

Raw data received is processed onboard with Edge computing devices and verified Fog devices and then is communicated to the cloud servers. The data obtained from every contributor has a significant role in the operation of the mission. With AI and ML, apposite and functional data is utilized and shared in real time for analysis, helping in decision making picking up pace much glorious than our corrivals. Modern warfare relies mainly on the data flow from the sensors and effectors in all the domains that is processed in real time to achieve a desired outcome.

Information advantage is crucial in achieving collated and processed data that can get us into our rival's decision cycle in split second time thereby always giving us the leading edge in understanding the battlespace with the aid of AI's capability in rapid decision making.

Autonomous aerial systems can be designed with the available inputs from sensors and outputs to the actuators or physical devices without any human intervention as the navigation or operation of the unmanned vehicles is proportionately unambiguous. They can operate easily with preset maps and real time location information from GPS, defined routes, and height of the obstacles with guidance from radars, altitudes from altimeters with an eclectic mission of reaching the destination on time. For this the autonomous system must construct a world model, a conceptual model of the real-world environment that is dynamic one, that is continuously updated, from the inputs from the sensors, and reconstructed in a way that is understandable by the computer as data that can be processed using the conscious of the computer- the AI, to make decisions on time with the set of algorithms designed to complete the goals successfully.

2. Technology:

2.1. Radio Jamming:

Radio Jamming (RJ) refers to an intentional act of disrupting the communication signal between the drone and command center or the user. Hostiles have the hardware of a jammer that includes a transmitter (that can vary in size or shape depending on requirement). This is used to aim on a fixed drone that disrupts the radio and GPS signals guiding the UAV.

Jammers simply interfere with the UAV flight and cannot identify the characteristics of UAV or its payload. Jammer shoots a frequency ranging from 2.4 GHz~5.8 GHz, the ones UAV communicate with CC. Most cases may end up in UAV returning to Home Base (HB) and tracking the same may reveal the location of CC.

2.2. Detect:

Detection (DT) of UAV shows the presence of UAV’s using various techniques like Radio Frequency (RF) analyzer, Radar, and Optical Sensors. Though these techniques boast their advantages, they do have a downside of cons like RF non-effective towards non-piloted, areas of mixed frequencies and terrains with physical obstacles.

Even Radar has the problem of differentiating a bird with UAV along with frequency checks to avoid interference. Optical Sensors are less effective in poor visibility areas like fog mixed with darkness. False signals are as common as these sensors cannot be used for developing a safety or evasive operation protocol.

2.3. Hacking:

UAV Hacking (HK) is like RJ by breaking the encrypted communication channel using fake signals and making the UAV get lost by the user. “Brute force” attacks are common and to do this the design characteristic of the UAV should be known by the hostile. Onboard controls are usually computers that can be easily infected by malicious software or Maldrone (malware for drones). Hostiles or attackers can easily inject false data or silently install malware.

Controls obtain data from onboard devices and these devices can be rigged to destabilize the controls of a UAV. For e.g., gyroscopes can mislead UAV by false data when subjected to an external source of audio energy.

2.4. Denial of Service:

DoS attacks on UAV can be done by the hostile when he floods the wireless connection with large amount of traffic, disrupting the communication between UAV and CC. Malicious hostiles send multiple unwanted message or commands to UAV, making it busy, ignore legitimate request or orders and lose contact with CC. Here the computational power of UAV is targeted by overloading the processor using ICMP (Internet Control Message Protocol) packets at a very rate to make the network overflow with messages.

2.5. Hijack:

Hijacking (HJ) of drones is done by devices that use DSMx protocol that facilitates communication between radio remote controls and devices. Encrypted keys are required to effectively HJ a UAV and once hostiles have these keys, UAVs don’t accept commands from user but from hostiles. Here radio frequency interference is used to disrupt CC’s control over UAV.

2.6. Intercept:

Intercept (IC) is the physical capture of UAV using another UAV or devices that can hinder the flight path using physical devices than other techniques. UAV here is captured physically and taken to the required place by the hostile.

2.7. Backdoor:

Backdoor (BD) attacks rely on weak points of the software that runs the drone. Infiltration of the system or a network by deceiving the security protocols and gaining administrative access is the primary goal of this attack.

2.8. Reverse Engineering:

Reverse Engineering (RE) is the method of abducting user’s drone’s design and technology, improving the same and releasing replicated user drones to attack the user.

2.8. Leased AWS keys:

Leaked AWS keys that are used to authenticate and authorize API requests made to Amazon Web Service from repositories like GitHub that contains an access key ID and secret access key are used to gain unauthorizes access to cloud services that are used to control drones.

2.9. Spoofing:

Spoofing on UAV can be done by the hostile by rigging the GPS navigational signal using fake signals forcing the UAV's process to consider the situation of fly over a no-fly zone. The UAV's AI interprets the same and land the UAV based on the safety system protocols triggers because of erroneous calculations by depending on faulty GPS device.

2.10. Attacking Hardware:

Attacking Hardware (AH) is a physical attack with the intent of destroying the UAV using small rocket launchers or even trained birds like eagles. E.g., Indian army uses tactic eagle "Arjuna" to attack and destroy hostile UAVs in the Kashmir valley.

2.11. Hardware and Software requirements:

- Multi-sensor EO/IR processing: Generates motion imagery of the target area by continuous surveillance by gathering input from sensors that span the visible and infrared band of the electromagnetic spectrum.
- Hyperspectral sensor fusion: Hyperspectral sensor captures the intensity of available light across contiguous frequency bands and displays in their output image, meaning each of the pixels representing a spectrum of values. Data obtained from such is mixed with LIDAR sensors to create an image of high quality and superior precision.
- Counter-IED device: When deployed, the device compiles data from hyper spectral scanners in combination with GPR (ground penetrating radar) to identify and detect IED's that need to be monitored on the target area.
- Synthetic aperture radar (SAR): SAR used in drones are generally Low-weight full-polarimetric SARs can generate high-resolution 2-D or 3-D images over a large area.
- Wide-area persistent surveillance/motion imagery (WAMI): WAMI is a tech using HI-resolution megapixel cameras to capture images of the target area that is updated at the rate of 1 Hz as images with geo tagging and registering.
- AI tools: AI tools such as TensoFlow, Caffe, Scikit-learn for hi-performance deep

learning inferences runtimes for object detection, segmentation, and image classification.

- Deep Neural Network: Deep neural network with multiple layers of interconnected nodes for HI-performance. E.g., NVIDIA TensorRT, Chainer, PyTorch etc.

3. Methodology:

Functionality of UAV's directly depends on the capability of AI algorithms along with the hardware configurations available onboard the UAV. These days the communication with CC is minimized as there are chances of interference with the hostile or outside world is more pronounced. So, the AI available with the drone must have the capability of discriminating against a false input or signal from a legitimate one. Available configurations call for more computing power and complications arriving out of such measures. CC communication is a better option for analyzing the various inputs in real time with lesser latency is recommended, but external environment with intelligent spoofing, hacking techniques are bringing a real tough competition for an UAV to achieve its goals.

Single processor handling all the requests can be easily overloaded by DoS protocols and denied GPS environment can also be dealt with Visual Inertial Odometry (VIO) or Simultaneous Localization and Mapping (SLAM) and Vehicle Dynamic Model (VDM). Success of UAV operations can be achieved only up to a limit, but uncertain or unforeseen circumstances that may happen over the course of the journey of the UAV may jeopardize its move towards success. Usually, AI depends on training and more the problems or possibilities in training in Edge or Fog devices can make a better model until convergence happens. Convergence is the limit above which no Edge/Fog device can perform further like it did before with the models. Convergence is the end of training, and the model is ready for deployment.

Probabilistic tools and various mathematical solving techniques may improve the level of expertise but a logical explanation for an event to happen or not happen is totally different in Universe or World as there are infinite possibilities available with the Permutations and Combinations of a dynamic environment that changes every moment.

UAV's when sent out to carry goals by allies, face a lot of hardships and sometimes are unable to complete the task they are trusted for. Intelligent systems of those working on the principles of Theory of Mind (ToM) and Self-Aware AI (SI) can help these UAV's a lot to make decision on the spot and carry out the same without any latency delay, with the capability of CC, that runs with hi-power computers to make quick decisions.

Out of Box Thinking (OBT) is a concept that does not value conventional ideas but answers to the problems. Answers produced by OBT are totally unexpected and they cannot be applied or trained to an existing AI, so that counter measures to one such idea really do not exist. OBT basically takes assumptions out of the problem formulation. It is a way that breaks the assumptions and gives solutions. Engineering problems are with assumptions that define the problem and these assumptions put restrictions to the level of answer or a perfect solution that can be applied for the problem.

Implementing OBT in an AI is a difficult task, but not an impossible task as algorithms that work for OBT must have the following algorithms that can train models in Spatial Navigation (SN), Memory Consolidation MC), Procedural Learning (PL), Cognitive Learning (CL), Conflict Monitoring (CM) and Error Detection (ED).

Algorithms that support SN are SLAM, Sensor Fusion are used for SN training. MC can be trained using Recurrent

Intuition is the capability of living beings possessed by nature for their survival. This capability can be taught to machines by using algorithms using models that blend intuition and analysis like Recognition-Primed Decision (RPD) model and Intuitionistic Logic based on ‘constructive provability’ using system of semantics constructed based on Heyting algebra or Kripke models. When the AI is trained using the above-mentioned models they start to “think” like living beings say an animal or a bird and act based on these inputs. These inputs are in the background processing, but not with real-time data and are used for making simulations or even actions based on real-time conditions. Intuition is more helpful in case of facing a threat or condition that is not pre-determined by the training models. Intuition here helps the AI to take steps and think ahead of hostiles for a strategic decision or move as there are proven examples and stories in the war environment or a spy assignment.

OM acts as observer of both the environment, the UAV’s flying and the internal process or activities happening inside the module in addition to the data received and processed by the FM. various data from the hardware is processed by the individual processors available along with embedded system. Both the raw and processed data is fed to the OM. Anomalies in the monitoring of healthiness of the various on-board equipment is also considered by OM. OM has various pre-loaded and trained modes of Hunter, the mode for offensive actions, the Prey for taking defensive action, Escape for fleeing out the area or situation, Kill to self-destroy in case of capture and Inject to activate the virus stored in the hardware to corrupt the existing UAV data and the one that breached (hostile) successfully. Leak mode can also be used where pre-loaded erroneous data can be leaked intentionally if some hostile tries to spy inside using Spyware in case of successful breach inside UAV.

OM provides a level of autonomy where the embedded modules work without any command from either CC or OM during any un suspected activity and activates itself in-case of a suspicion or a surprise check to find the integrity of the system on-flight that changes the course of direction or any regular operation and observe the response of the outer environment to know the level of interference by the hostiles when working in the outside environment.

4. Case-1:

For e.g., UAVs used for spying operations must disguise itself a normal living object like the birds flying on air, though there are radars to discriminate the flying of bird & UAV is available, techniques to confuse the radar from deciding can buy some time to finish the operation or escape the situation. Here to provide these actions some additional less-expensive hardware is provided. This hardware is a speaker that can produce sound like the birds flapping of wings in air. This sound does not imitate the birds' flap but introduces a lot of errors in detection using "False Positives/Negatives," thereby making the detection environment a complex one. The micro-Doppler (m-D) accuracy depends on background noise, so introducing a lot of background noise (like flapping sound of different birds and turbulent wind sound) using the hi-quality speaker can bring a great difficulty to the detection system. Modulation frequency of UAV's rotors is suppressed by introducing sounds that can superimpose with the original sound to produce something that is totally confusing or undetectable. UAV outer body is covered by sticker or thin films like TFT or diodes that can emit a spectrum of light ranging from infrared to ultraviolet as it is the most possible light that can be emitted. Here the IR, visible & UV LEDs are patterned or interleaved as they cover almost 33% of the total available LEDs from any side of the drone. These lights are made ON/OFF by the individual control system as dictated by onboard AI of UAV. Here a feedback system is used. An onboard mic, that captures the sound, uses Digital Signal Processing techniques aided with AI, produces indistinct sound forms, and sends to the speaker in real time. These frequencies produce noise to confuse the detection system and rule the early warning system.

SAR is a part of hardware in these drones, but the capabilities of hunting birds like acute vision/sharp vision or image are made available with the software to convert the same as

PoISARPro ENVI SARscape etc. Wide Field of view is also provided with tools like Multiple SAR Image Stacking, Inferometric SAR (InSAR) etc. Telescopic vision is achieved with Fusion with Optical Data. The frequency of switching ON/OFF the LEDs at 145 Hz to keep away birds attacking or surrounding the drone is done by the TFT/LED of the drone. This frequency confuses the avians like pigeons not to come near drones as they directly impact eye-brain interactions of the bird using the Flicker Fusion Frequency (FFF). The same method can be used to drive off other drones attacking birds like eagles/crows or any kind by detecting the type of the bird and use the FFF of the bird. This can help UAV avoid bird attacks and stay safe on the air.

Micro-Doppler radar requires a lot of computational power to discriminate a flying object from UAV to bird. These computational requirements go up as the environment gets noisier and can stall the system. A group of such improved embedded AI assisted UAV can easily overload the m-Doppler processor by producing different kinds of sound that suppress the blade rotational frequency sound by increasing the pitch of the emitted speaker sound in four different directions using four speakers in either of the directions of the drone. Here all four speakers adjust their pitch using AI in such a way that analyzing and interpreting the same is a time-consuming process that buys enough time for the UAV to complete its spy operations or escape from the grid to a safe place or home.

5. Case-2:

UAVs attached with special devices to escape the situation can fare very well in operations like spying or attack. In case of escape from the current place surrounded by other drone capturing nets or drone attacking birds or UAV, the current escape routes of moving sidewards or below can easily be spotted by the hostile UAVs. Moving upwards can be a better option, but with the current capability to fly above can be hindered by the other hostiles, unless there is any supporting device to fly upwards fast available.

A 4-way solenoid-operated-valve (SOV) with an expansion device on the top of the drone that can inflate itself in seconds (say like a balloon with a low-density gas like hydrogen/helium, that easily goes up due to inherent physical property) can aid the upward direction in addition to the blades trying to move up above all the other hostile UAVs.

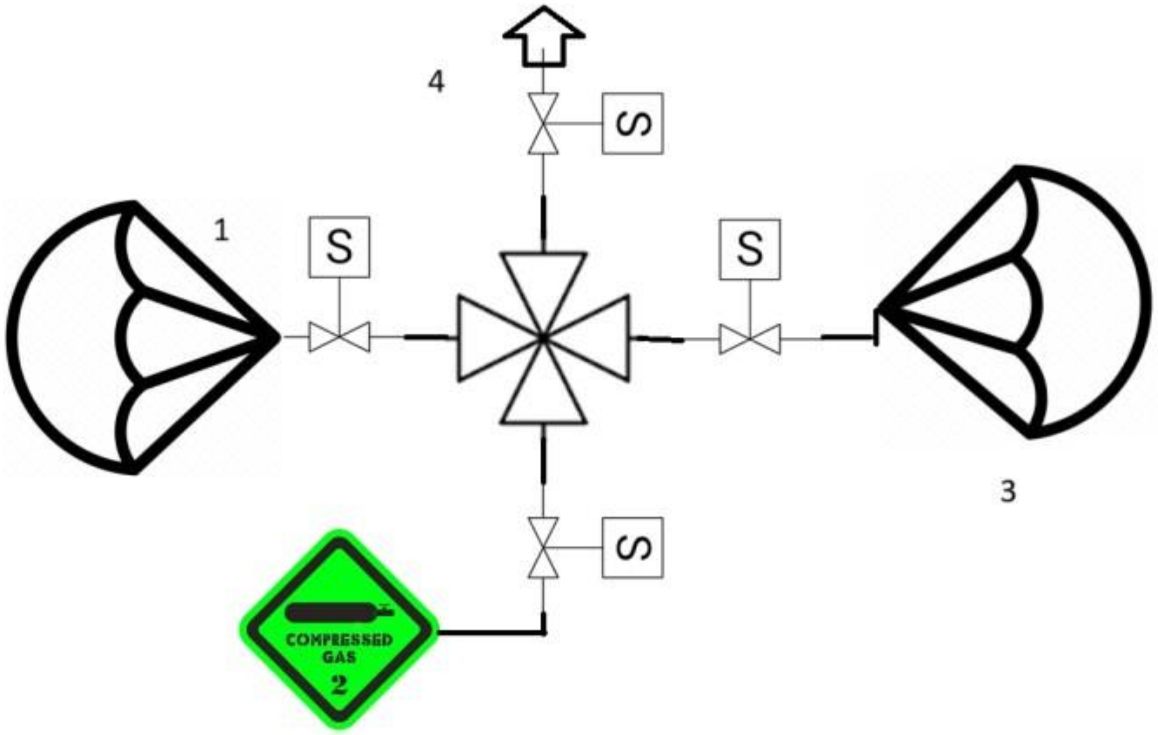

Figure. 1: A 4-way solenoid-operated-valve

The assembly consists of a compressed air tank with two inflatable devices side-by-side (one working and one stand-by, in case the former fails to open, the later can do the work). Here 1&3 are the inflatable balloon kept side by side for operation. Compressed gas from 2 is operated by opening SOV-2 & either of SOV's SOV-1 or SOV-3. Timing of opening of SOV's is already programmed in AI for faster ascending in the atmosphere. Descending or deflating of the balloons can easily be done by opening the SOV's SOV-4 (vent to atmosphere) & either of the inflated SOV-1/SOV-3. By the combination of logics, it is possible for faster ascend/descend in a recordable time. The balloons are also painted with colors that may have lesser contrast effect in the operating environment. The balloon is a shaped tubular that does have minimum hinderance with the UAV's rotor operation. Even in case of temporary failure of UAV rotor these balloons can hold the altitude of the UAV of decrease the speed of descend to avoid any sharp impact on the ground. This brings time for the AI to do alternate steps to adjust its inertial system to become normal.

Limitations of UAV flying above a certain altitude can also be dealt with this assembly as the upward draft is taken care of the inflated balloon with a lesser density gas and lesser power to control sidewise is used and controlling the gas to the balloons is achieved by both the combination of SOV-1 &4. By this way UAV can achieve great heights that is not possible previously by the rotor flying UAV due to design restrictions.

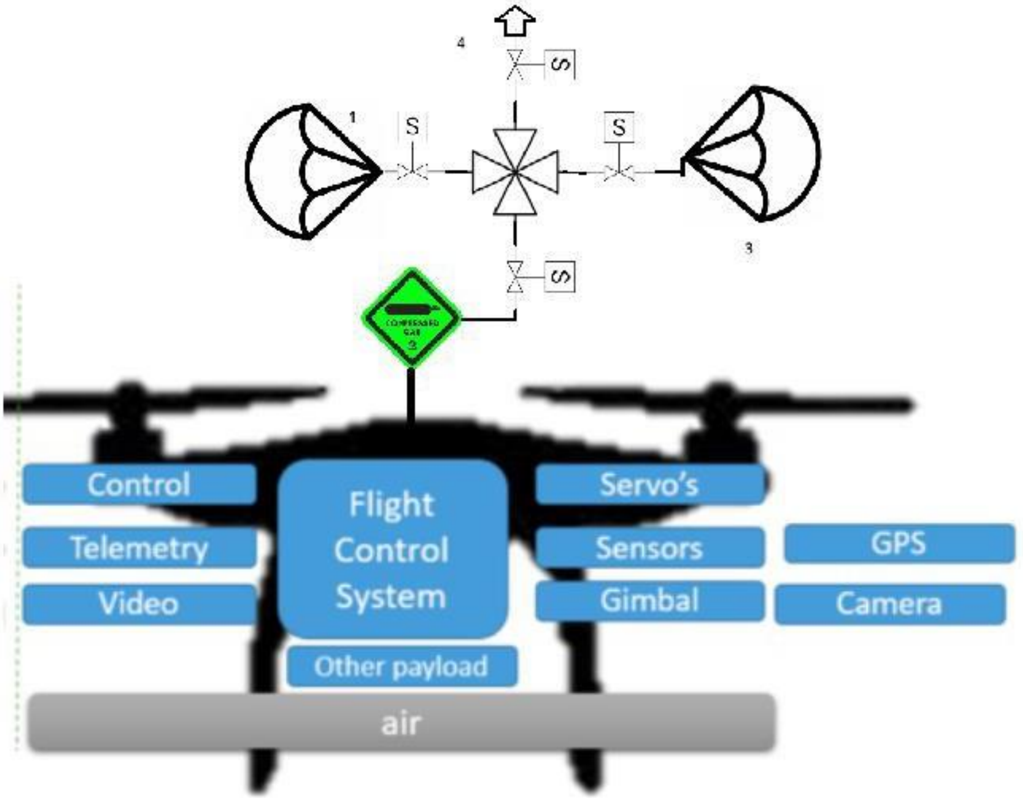

Figure. 2: Various parameters effecting the solenoid-operated-valve

Here the total weight of the UAV is calculated with the draft required to make it fly along with the size of the balloon is also considered in the overall design of the equipment.

6. Conclusion:

UAV with current designs can fare good, but with additional hardware that is added along to work can make UAV AI to take “Out of the Box decisions” as more the number of available hardware more will be the decisions and the combinations to work out will be mind-blowing.

UAV AI that can think like a living being, say a bird or a human requires additional hardware. Software aided with the latest tools and algorithms are reaching a point of maturity or convergence and any such change in intelligence may not reflect on the capability of the UAV with a bigger impact. Non-traditional thinking is the start of Out of Box thinking and this needs new additional hardware as mentioned in the article.

Improved UAV is aimed to bring a better strategic position of the allies UAV in a hostile environment to buy the allies an additional time to think, react and even change the situation in an environment. Additional gadgets can be fixed that is not mentioned in the article or additional logics can be made like making different sounds that resembles a flying living being in different directions along with emitting light in different frequencies can confuse an eagle trying to attack UAV, by bringing down the retina/brain co-ordination of the bird and will scare it away from the location.

7. References:

(1) Embedded AI application in Defense UAV, Uma Perumal, Vasantharajan Renganathan.

(2) Identification of GPS Spoofing as a Drone Cyber-vulnerability and Evaluation of Efficacy of Asynchronous GPS spoofing M. Surendra Kumar ∗ Gaurav S. Kasbekar , Arnab Maity.

(3) A review of UAV Visual Detection and Tracking Methods Raed Abu Zitara, Mohammad Al-Betarb, Mohamad Ryalatc, Sofian Kassaymeh.

(4) Infrared-Inertial Navigation for Commercial Aircraft Precision Landing in Low Visibility and GPS-Denied Environments Lei Zhang, Zhengjun Zhai, Lang He, Pengcheng Wen and Wensheng Niu.

(5) Inertial sensors technologies for navigation applications: state of the art and future trends Naser El-Sheimy and Ahmed Youssef Muskardin, T.; Balmer, G.; Wlach, S.; Kondak, K.; Laiacker, M.; Ollero.

(6) A. Landing of a Fixed-wing UAV on a Mobile Ground Vehicle. In Proceedings of the IEEE International Conference on Robotics and Automation (ICRA), Stockholm, Sweden, 16–21 May 2016; pp. 1237–1242. Kong, W.; Zhang, D.; Wang, X.; Xian, Z.; Zhang, J.

(7) Autonomous Landing of a UAV with a Ground-Based Actuated Infrared Stereo Vision System. In Proceedings of the IEEE International Conference on Intelligent Alvika, G.; Sujit, P.B.; Srikanth, S.

(8) A Survey of Autonomous Landing Techniques for UAVs. In Proceedings of the International Conference on Unmanned Aircraft Systems (ICUAS), Orlando, FL, USA, 27–30 May 2014 J. Ochodnick`y, Z. Matousek, M. Babjak, J. Kurty.

(9) Drone detection by ku-band battlefield radar, in 2017 International Conference on Military Technologies (ICMT), IEEE, 2017 K. R. Sapkota, S. Roelofsen, A. Rozantsev, V. Lepetit, D. Gillet, P. Fua, and A. Martinoli.

(10) Vision based unmanned aerial vehicle detection and tracking for sense and avoid systems, in 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Ieee, 2016, pp. 1556–1561.