

Embedded AI Application in Defense UAV

Uma Perumal¹, Vasantharajan Renganathan^{2*}

¹Assistant Professor, Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, India.

²Assistant Manager at TAQA Neyveli Power Plant, Neyveli, India.

****Corresponding Author***

E-mail Id:- rajavasanth2079@rediffmail.com

ABSTRACT

Embedded systems in combination with AI in defense systems is a boon for nations security. Various embedded hardware along with algorithms of AI, is a blend of computing techniques is a leading-edge tool for an army. Army drones, single or a swarm, can either inform the allies with necessary facts or can even misinform enemies with fake data is a game changer in a battle or military operation. The capabilities of embedded systems in addition edge and fog computing techniques to bring down latency, bandwidth and reduction in load to cloud servers. AI algorithms that can teach Intuition with advanced AI logics to UAV, can help drones think and act accordingly like a living being than simple machines.

Keywords:-Fog computing, Adversarial AI, Drone AI, Deep fake, Embedded AI.

INTRODUCTION

Battle fields are getting increasingly rich of data. The data from the field is collected by various types of sensors and they are of different types, like voice call, image, video etc., Vast quantities of such data from these sensors and sometimes data from the military personnel in the field are collected in all domains are collected by the command center for further analysis. The command center receives data from other sources such as satellite images from space and cyberspace. Each part of the data is important as any error in the collected data changes the decision in a dynamic environment such as a war or military exercise that may result in either a successful or failed mission.

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, 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.

Significant computational capabilities are imbibed in the onboard computer for keeping the track of the variables and update with the physical real world. Skills based on behaviors of the intended living being or human for e.g., is acquired based on the repetitive actions and these rely on perception-cognition-action loop is a response to stimulus. Automated agents programmed through equations based on feedback loops depend on the quality of inputs acquired through the input devices.

In an uncertain environment expertise sounds too good than skills as expertise is gained by experience with the help of lessons learnt from various dynamic environments over a period. To gain such expertise rules and knowledge are required in addition to skills as reasoning behavior is one of the elements of expertise. Skills come with assumptions as the situation is not forward-looking and every next action is always programmed with the limited set of variables.

TECHNOLOGY

Artificial Intelligence

Artificial Intelligence (AI) is a field of science that enables computers or machines to imitate natural intelligence of living beings such as insects, animals, humans etc., Here the real environment, goal or task is fed as datasets and various algorithms are used to recognize, read, understand the real environment, use logics, algorithms to deduct, reason with the available resources to imitate any living being that is required for the moment or operation. Here the behavior of that being is based on the environmental circumstances and the behavior is dynamic as that is required by the locale.

Data sets can be used for simulating various events, simply with data and numerals without the real need for any change in the working environment. AI uses the combination of statistical, scientific, advanced mathematical works in a simple streamlined form to achieve the expected result with less hard work and at the ease of the user. Techniques that investigate a particular data group with fact-finding and probing methodologies is set out by the numerous validated analytical methods.

AI has the flexibility to incorporate various living beings' behavior, that is unique to a particular intelligence level of the organism. The patterns of a group or a swarm can be fed to the instruments and can also be made to behave as they are real living organisms with the conscious level of the imitated entity.

Embedded Systems

Embedded systems are an electronic or computer system that has got a processor to process the data, a memory to store the data, input devices to gather or get the input and an output device to display or sent out the processed data. Embedded

systems are integrated systems that is built for a specific task or function and are dedicated to the specific work. These systems can either be a standalone or individual system or a part of another system in series or parallel. These systems are real time systems as they process the data and produce results as and when they get one input. They operate on a set of rules that is programmed inherent with the memory. System operation involves in inspecting the received data, process the same with the available or programmed algorithms to take knowledgeable, up to date decisions in real time when environment working is a dynamic one.

Embedded AI (EAI)

EAI is a technology that uses AI functions in an embedded or dedicated system where the complex function of processing is done in the embedded system than in a computer with higher capability, here the embedded system is upgraded to the level of a computer that can run large complex algorithms than relatively simple set of instructions. Single or multiple devices that are implanted with sensors in an embedded system, along with software and communication technologies for the intention of sharing information among and data with the working methodology of exchanging data with the internet or a wider connected network of computers and communication devices.

These devices are equipped with the capability of self-reporting in real time without the need for any human intervention. They work with an active network connection and can transmit data, the network can either be the internet or a wireless/WAN/LAN for communication purpose.

Drones

Drones are Unmanned Aerial Aircraft

that can carry out flying operations autonomously or controlled by a drone pilot for the functions of collecting data by aerial survey, area measurement, transport of goods/logistics, emergency rescue, agriculture work, surveillance/monitor, reconnaissance or combat.

Here the tools of IoT sensors, communication devices, software relate to the drone and these individual systems act as a part of the whole embedded system to carry out a mission programmed with the drone.

Edge and Fog computing

Is a computing methodology where the calculations are made much near to the sensory devices than transmitted or communicated to a far away processor. Here the sensory devices are made available with high computing power in relation to cloud services that usually do the processing. Edge computing is used to bring down the latency as communication devices consume sizeable processing time. With a capable computer onboard with the sensors and limited storage memory, cloud devices store the transmitted data for further analysis and archives.

Fog computing is synonymous to Edge computing but an additional layer of edge computing. Fog acts as a bridge between edge and cloud servers. Fog in addition to communication also brings down the bandwidth required to transmit the data by differentiating the one that is required for cloud than all the data from the sensor/edge computers.

Hardware and Software requirements

- **Hyperspectral sensor fusion:** Hyperspectral sensors collect the light intensity of the continuous sets of frequency bands in its output image, which implies of each pixel containing a spectrum of values. This data is integrated with the LIDAR sensors to

create a high-quality image and precision.

- Multi-sensor EO/IR processing: This processor collects inputs from sensors across the visible and infrared band of the electromagnetic spectrum. This then create motion imagery of the target area all day and night for constant surveillance.

- 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.

- Counter-IED device: This device uses the inputs of hyper spectral scanners, ground penetrating radar to detect IED over the target area under surveillance.

- Wide-area persistent surveillance/motion imagery (WAMI): WAMI sensors sources images from a single or a group of HI-resolution mega pixel camera images that are updated at a rate of 1 Hz and an AI algorithm geo-register them after they are seamlessly stitched altogether. The target area is usually a kilometer in diameter and the focus area is a specific area inside the target area.

- AI tools: AI tools like TensorRT, PyTorch, Keras etc., - a high performance deep learning inference runtime for object detection, segmentation and image classification, that has got OS images, libraries, APIs, samples and documentation.

- Deep Neural Network: Deep neural network libraries with high performance primitives for deep learning framework, including support for convolutions, action function and tensor transformations. E.g., YOLO, MXNet, CUDA cuDNN.

METHODOLOGY

Military drones with the capabilities of edge and fog computing can be made to run based on the levels of autonomy. The autonomous levels are defined by the

level of human intervention starting from Autonomy, Semi-autonomy, Automation and Integration. Integration is offers the least or no human intervention to the drone AI, where the AI algorithms are free to work based on the preset condition of goals or mission. The type of AI can be chosen based on the mission.

Here Artificial Narrow Intelligence (ANI) tells the drone for a specific task which is skill oriented in addition to rules than expertise. Repetitive tasks such as logistics or transport of army goods to desired location to ensure supplies can use this mode as only mission is defined in a predetermined travel path.

The predetermined path is traced and followed with necessary corrections to ensure the success of the mission on time. Artificial Broad Intelligence (ABI) is a combination or blend of two or more ANI, that requires decision making. Decision making process involves knowledge in aid to learn the situation in addition to the skills and rules as the goal or the mission should not be compromised by the decision, and this could be an assisted one where the final decision is dictated by the human and the liberty to choose the way in achieving or the path to follow is given to the ABI restricted by the defined rules.

Artificial General Intelligence (AGI), popularly known as 'Strong AI' or 'Deep AI' gives the liberty to the machine to behave as a human. The level of intelligence is in par with a human who has got some expertise in the field of military operations in addition to the skills, rules and knowledge as the ANI has. Here the AI is supposed to have a thought of mind without emotions that strictly stick to the mission without regrets. Self-awareness or conscious are the terms used to mention the level of intelligence the AI is capable of.

Missions like spying/reconnaissance inside the enemy zone, neutralizing incoming enemy threat are examples of AGI. For e.g., a thermal radiation detected by a Passive Infrared (PIR) sensor over the target area radiated by humans, or any heat sources can be used as an input to AI and the AI processes the rate of change of the heat value and if this exceeds a pre-set then an alarm is activated to watch closely. Uncertainties in the battlefield demands expert AGI system as the input to the systems are incomplete. Incomplete information jeopardizes the quality of data collected in the field. Without complete information, efficient data processing is not possible, and the blanks of data are to be filled with bias or assumptions.

Correct assumptions can be made only by experts in the fields of those depending on extra senses and intuition. The capabilities of intuition, guesses, assumption are inherent to humans, and they are not so easy to program in an algorithm. Probabilistic techniques and mathematical tools like statistics, distribution can be substituted to a certain level to improve the level of expertise of the AI algorithm, but a little success can be achieved. Here logical explanation of the occurrence of an event can throw more light and logical based reasoning is employed.

Adversarial AI is an evolution of AGI that uses expertise capability of the algorithms that can discriminate between a real or valid data from a fake data that can be used to rig the machine that process the data. Adversarial AI is technique used to identify a misinformation given as a data (that can be an image or numerical value) that could easily mislead the decision process intentionally spread by the hostiles and revert back the same to the foes by allies with or without modifications in the

methods of achieving a goal to take a lead in a battle situation as adversarial AI depends on training imperfection.

CASE-1

For e.g., Spoofing is a technique used by the hostiles to take in control of any allies UAV or even manned aerial vehicles. Here the GPS signal of the allies is rigged by taking over the control by the spoofer, by gaining control over the GPS signal and after the takeover, the adversarial AI is supposed to monitor the vehicle by using the Satellite number, Signal-to-Noise Ratio, Pseudo range, Doppler shift, Carrier Phase Offset etc., and even if all the above mentioned are compromised by the spoofer by using nominal Signal Strength Intensity (SSI), multi antennae with uniform power levels to confuse the satellite, a drift made by the UAV to adjust to the new rigged GPS location set by the hostiles from the location dictated by the existing real GPS satellite, the power levels of the processor to adjust to the new location can be an indicator of the UAV is under the control of spoofer, as the increase in load of CPU is not spent on calculations but aligning to new co-ordinates and a constant change in the flight route.

This method of drifting the UAV from its initial position to the spoofer desired position consumes additional power in addition to the normal power consumption. This uneven flight route is initiated by the spoofer to bring down the battery levels and make it to land, for capture. Here the rate of discharge in battery level and the additional computing power(utilization) can be taken as feedback by the AGI, that the machine is compromised and necessary actions to recover the UAV is taken either by AI or go for any per any standard operating procedure like calculating the last time from which the CPU load started to increase and taking

the input as reference than the real time (rigged) input. Then UAV starts moving to the home position where it was launched.

But the changes that happened inside the AI is not displayed or communicated outside (even to the allies controlling/monitoring UAV-as any data transmitted has a chance of being monitored by spoofer) as the intention of the spoofer is still unknown. It could be to capture the vehicle, use it as a weapon against allies in flight mode. Not taking any chances the UAV can start fly in the direction of the home and here the CPU utilization, battery discharge rate is monitored continuously as it is a direct measurement that tells the control of vehicle (could be still under the spoofer control or run-back protocol-safety protocol to come back home in case of emergency).

Sensor spoofing goes on an attack for the sensor algorithm directly, whenever a spoofing is detected, or the UAV has some disturbances a Safe mode operation can be initiated in addition to the run-back or home-run mode. After a landing the UAV is inspected in the lab for the aftereffects of the attack experienced by UAV by the spoofer. In safe mode the UAV activates its NFC sensors without any indication and scans for the work bench with the access code to open the UAV for inspection or data download. A sequence of operation pre-determined or programmed with the UAV is initiated. Tamper proof mechanism ensures this and if any such violation occurs initiates a self-destruct mechanism by UAV in suspicion of tampering. Here the tools to open the cabinet of the UAV are also equipped with NFC. There can be three NFC sensors, one from the work bench, NFC with UAV, NFC from the tool. When all of these aligns, then the UAV can go for

maintenance mode, where the personnel inspecting can have access to the data can move on. Any deviation from the procedure of maintenance mode can revoke the self-destructive phase. An addition layer of the fourth NFC can also be included with the instrument used to download or upload the data from the UAV. When 4 NFCs are in series then, AI in UAV is convinced of the location and can grant access to the accessor and abort the self-destruction mode.

The same methodology can be used for a swarm of drones used for surveillance over the hostile area. When a swarm of drones deployed from allies face the least possible chance of getting spoofed. In this all the UAVs are equipped with both edge and fog computing capabilities to bring down the bandwidth for communication. Here advanced AI algorithms can implement the characteristics of insects to the UAV's that can take the role of a queen, commanding others to do a teamwork. The queen enables its fog computing capability, processes the edge computed data from the other drones, communicate to the cloud servers as instructed by the command center.

This taking up of role of queen in a swarm can be rotated among others and a drone with maximum capability such as one with high battery power and one with low CPU utilization is chosen among the available drones. This queen drone gets the command from the command center and using the available ABI, breaks the work and gives individual task-based ANI to the other drones. When the AGI senses capacity-based limitation like high rate of battery discharge or CPU utilization, switching places with the other drones happen. Here the method of choosing is the same as before. Drones that are low of resources like power are relieved and sent back to home for

recharging. If any of the drone is prone for spoofing or the group senses spoofing by the method of measuring rate of battery discharge and CPU utilization above the normal, The swarm flies back to the home without any further transmission of data. GPS positioning of the swarm is fed to all the UAVs, and they know about their position regularly and any drift from the position of any of one such is an indication of being spoofed.

Intuition is the capability of a living being that can be defined as a feeling felt on some occasions. Experience shows intuition felt by the human or animal has helped the same in the times of danger or when the animal hunts for food. The main purpose of intuition is to warn people or animal and check with the surroundings, as this feeling is one that can be experienced only by living beings, AI with some algorithms and logics can fill the place of intuition in machines. This algorithm keeps the machine alert and look for any danger or opportunity. Humans sense intuition by various methods like pheromones in the surrounding air, mild difference in surrounding sound, change in the ambient air flow direction, look for change in the position of objects around them expecting detection of movements, change in behavior of people around him, vibration on the standing surface etc., Intuition to machines can be programmed by the AI, for e.g., if the air flow direction or wind speed changes around the machine, UAV/drone then it can look for any surrounding movement that is camouflaged to the sensors of the UAV. To make UAV learn, first the hostile area in the mission is fed not as a simple GPS map, but a 3D map with contours and terrain. The UAV travel destination is broken down to multiple waypoints, and when the UAV reaches each one, it checks the area with the

terrain map provided to it and verifies the area and is geo tagged in the memory of UAV. The verification of the area is done by using distance measuring sensors such as LIDAR, Ultrasonic distance measurement units, and the exact place from where the UAV is positioned in the scan area.

The Geo tagged data, verified with the 3D map provided by the allies should be the same. After reaching the area under surveillance, if there is an increase in the CPU utilization, then the UAV can scan the surrounding area and compare it with the geo tagged area and the map. If the UAV is under the control of spoofer, then the data will not match as the drifting can cause a change in location. With this UAV can confirm itself, being a target of a spoofer. If there is an Electromagnetic interference which jams all the sensors from working properly, then the UAV can go for a spin to look for any change in the values of its various sensors. In case there is no change, the UAV is now under spoofer control. Then UAV can go for run-back mode and look for retracing the way point it crossed during the travel or look for the exact opposite direction it was convinced by the spoofer to land or reposition.

CASE-2

Deepfake is a digital imaging technique that produces images or videos digitally that are not for real. Various digital imaging and audio encoding techniques aid deepfake product a fake substitution to real happenings that can be transmitted worldwide and be made to public. This technology, originally intended for making movies can be used as a weapon to misinform hostiles about the location. Here the method of implanting deepfakes is done as a procedure like making the allies UAV fly over the vulnerable/hostile comfort location, record a video of a particular area from

vulnerable location (where the hostiles are expected to send UAVs-hostile comfort area) of the in the allies-controlled area. A simple warehouse area packed with junk boxes and some non-critical military labelled empty boxes are recorded and using deepfake imaging techniques the area is shown as a highly critical military zone with lot of weapons, arsenal ready for attack. This deepfake video is made to display as fully equipped military bunker/shed or covered area well-conceived from a satellite view as any information not viewed from satellite is usually spied by other sources like UAVs or human spies. This area may be easily shown to spy satellites on the outside but well closed in the inside for a satellite to view.

Signal Jamming technique is used, by sending in the noise into the sensor or receiver, resulting a condition whereby the sensors are unable to report any signal. Electromagnetic Interference (EMI) signals are used to confuse the signals as they don't work very well in an area with so much interference.

When a hostile UAV that transmits video, is observed by the spoofer from allies jam the signals in/out of the area, then send the deepfake video just like the one sent from hostile UAV, this information can misinform the hostiles and prevent them to take necessary action, as hostiles will first confirm the genuineness of the video, either to consider the received data and act accordingly.

If more such locations with units of conceived areas loaded with fake arms can easily confuse the hostiles and delay for a decision, that bring more time for the allies to react. If hostiles believe on this, they may spend more of their resources in chasing fakes and if they

don't believe, they cannot discriminate the one real from a group of fake, incase any such real video leaked and is available with the foes. This deepfake tool is a reliable one to misinform hostiles and lead them to a trap, where the recording devices is mostly depended on, as line of sight is very limited.

CONCLUSION

Drones are getting smaller, smarter with embedded AI algorithms and more powerful in working range, unless big enough to detect by a radar can easily come inside in swarms and get the information from the ally's zone. Autonomous UAVs are increasingly getting ubiquitous with the combination of both ML and DL algorithms. If convolution Neural Networks are integrated with the former, AI algorithms get their expertise like intuition, sense of consciousness which can aid the UAVs to think logically and detect for any attacks proactively and act accordingly. Very best of services is expected from these devices, as war zones are need of smarter moves to reduce the damage of the allies and damage more to the hostiles.

Introducing intuition using various algorithms and make machines behave as a living being is possible using sensors to measure environmental parameters like, look for markings in a way point as ancient men did to recognize locations, wind speed and direction measuring sensors with algorithms to behave like a fly or bird (this is used to calculate the optimum path to descend or travel to minimize the use of resources) etc., in addition to the SAR, multisensory EO/IR. With the additional sensor and algorithms, the desired UAV will be more capable as a machine with intuition and stay alert.

REFERENCES

1. <https://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf>.
2. <https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf>.
3. https://www.claws.in/static/IB-344_Artificial-Intelligence-in-Military-Operations.pdf.
4. <https://cps.iisc.ac.in/wp-content/uploads/2020/10/Collaborative-Tracking-and-Capture-of-Aerial-Object-using-UAVs.pdf>.
5. <https://stanleycenter.org/wp-content/uploads/2020/05/MilitaryApplicationsofArtificialIntelligence-US.pdf>.
6. <https://www.asisonline.org/globalassets/foundation/documents/digital-transformation-series/ai-guidance-document-final.pdf>
7. <https://www.imagimob.com/resources/case-study-how-to-build-an-embedded-ai-application>
8. <https://www.sciencedirect.com/science/article/pii/S2214914721000271/pdf>
9. <https://www.cigionline.org/documents/2120/no.263.pdf>
10. <https://www.ijert.org/research/interconnected-robots-a-real-life-military-and-commercial-application-based-on-embedded-system-technology-IJERTV5IS060698.pdf>
11. <https://www.fraunhofer.de/content/dam/zv/de/forschungsthemen/schutz-sicherheit/rise-of-intelligent-systems-in-military-weapon-systems-position-paper-fraunhofer-vvs.pdf>

AUTHORS' PROFILE

Uma Perumal is an Assistant Professor in the Department of Computer Science and Engineering at Sri Venkateswara College of Engineering, Sriperumbudur, Chennai. She's got a master's in computer science and Engineering. Field of interest includes Big Data, Data Analytics and Data Science.

Vasantharajan Renganathan is a certified sustainable business agent and a business English professional. He works as an Assistant Manager at TAQA Neyveli Power Plant, Neyveli. He has got a Bachelor's in Engineering and master's in business administration. He is also a freelance Expert and a consultant for online consultancy services.