Groups of Surface Marine Craft with Intelligent Control: Bayesian Estimation against Adversarial Attacks

Amolkumar Bhoyar* M.Tech.

Rajneesh Sharma* M.Tech.

Sukratu Barve[+] ** Ph.D. M.Tech. M.Sc.

Commodore (Dr) R K Rana[£] Ph.D. M.Sc. B.Sc.

**** Department of Technology, Savitribai Phule Pune University, Pune 411 007, INDIA***
***** School of Mathematical and Computational Sciences, Savitribai Phule Pune University, Pune 411 007, INDIA***
£ Foundation for Innovation and Technology Transfer, Indian Institute of Technology, Hauz Khas, New Delhi 110 016, INDIA
+ Corresponding Author. Email: sukratu@gmail.com

Synopsis

With increasing in-roads made by intelligent control into design of marine craft in recent years many challenges are posed as regards safety and security in the course of operation. In particular, when intelligent controlled marine craft are subject to adversarial attack, their vulnerability appears to be of an extreme nature. It also appears that mounting an adversarial attack has its own challenges, the most important being physical. It is currently technically difficult to reach attack surfaces of the marine craft systems which have limited physical accessibility to devices expected to be used while mounting the attack. However, it is plausible that this situation would be of paramount importance to designers in the future. The authors in a previous conference (ICMET 2019) discussed a situation when two surface marine craft are designed to ply in a leader-follower fashion under intelligent control and are subject to adversarial attack assuming a compromised attack surface. It was suggested therein that the nature of intelligent control being Bayesian estimation is preferable from the point of view of security. We take the exploration further and study how a number of such intelligently controlled marine craft behave under adversarial attack. If mounted in such a situation with many craft, the implications of an adversarial attack would be severe if counter measures are not available. Our study shows that vessels beyond a certain number could be well handled within a given area of operation by adjusting parameters of the Bayesian filter employed as a safeguard against adversarial attack.

Keywords: Intelligent Control, Adversarial Attacks, Sequential Monte Carlo

---

Authors' Biography

Amolkumar Bhoyar completed his Master of Technology degree in Modeling and Simulation from Savitribai Phule Pune University and has worked as DRDO consultant on joint projects with the university carried out with the DRDO establishment ARDE. He has also guided several students as regards placement and functioned as a university department coordinator.

Rajneesh Sharma completed his Master of Technology degree in Modeling and Simulation from Savitribai Phule Pune University and has worked as DRDO consultant on joint projects with the university carried out with the DRDO establishment ARDE. He has guided several M.Tech. students and consults industry regarding machine learning projects.

Sukratu Barve is Assistant Professor with the Savitribai Phule University in India in the School of Mathematical and Computational Sciences.. He holds a Ph.D. in Physics and an M.Tech. in Materials Science. He has worked jointly with the Indian DRDO on weapon systems projects and carries out modeling and simulation in naval engineering related to fluid dynamics and to autonomous systems.

Commodore Rakesh Kumar Rana was commissioned in the Indian Navy on 01 Aug 1979. An Alumnus of Delhi College oF Engineering, 1980, Mechanical Engineering batch, he completed his post graduation from Royal Naval Engineering College, UK and thereafter pursued his PhD degree that was awarded by IIT, Madras in Jul 96. Commodore has served in a variety of organizations in the Navy encompassing training, research, dockyard, staff, design of warships, indigenous products development and onboard ships, during long and illustrious career spanning more than 33+ years.

1. Introduction

Rapid advancements in technology are enabling autonomous operations of naval platforms, with the primary aim of minimizing the number of naval personnel being put in harm's way, but still achieve operational objectives. One of the operational objectives could be ensuring that harbours are free from any mines installed by the adversary or by lurking enemy autonomous vessels and submarines, so as to assure safe passage of the fleet. Other objectives could be launching smaller vessels (such as missile boats - example Indian Navy attack on enemy harbour in December 1971)) near the enemy coast to deliver the ordnance at the right place; surveillance of the coast line; amphibious landings; transiting through oceans; etc

Autonomous naval platforms or marine vessels carrying out successful operational trips on designated routes have raised several questions within the naval engineering community as regards concerns like reliability , safety and resilience. These marine craft have several component systems possessing computational as well as physical aspects in their function within the context of which these concerns are being understood. Owing to the high levels of complexity as well as of the ubiquity of such devices, some authors have proposed that an entire marine craft (except the human beings on it) could be considered as a complex cyber physical system (Dracopoulos,1997). Such systems pose formidable challenges as regards design and analysis (Sanfelice, 2015). The National Institute of Standards in Technology has advanced a unifying Conceptual Framework for Cyber-Physical Systems [Fra] so that the challenges could be framed in a holistic manner. Such a framework offers options to address such complexity like Aspect Oriented Design (Advice, join points, join cuts etc.) See also (Khaitan, 2015; Graja, 2018) for formal frameworks. As such these advancements addressed cyber physical systems without any autonomy or intelligent control.
As a further design dimension of autonomy needs to be incorporated, the challenges like safety are bound to simply increase. On one hand, the design philosophy appears to be headed in a more holistic direction towards concepts like situational awareness (Wang, 2021) Assessments related to safety indicate that the software component of the ship should be most emphasized (Krzysztof, 2018) as regards vulnerability. Adversarial attacks are likely to affect the software component the most, putting at most risk the control system of the entire craft or fleet of craft. This challenge is aggravated in the case of heavy craft due to actuation related matters, as only three actuator variables, rudder angle, propeller pitch and propeller speed are available (Perera, 2020).The inertia in heavy vessels makes ship controllability an extremely difficult challenge especially under rough weather conditions. The rudder and propeller control systems, i.e. only available control units for vessel actuation, may be inadequate to control such craft under rough sea going conditions. When the marine craft ply at moderate or high speeds (i.e. over 3-4 knots), the thrusters offer negligible effect. Therefore, control solutions developed for autonomous surface vehicles (ASVs) and autonomous underwater vehicles (AUVs) would not be acceptable for large vessels as they would turn out to be rather under-actuated for autonomous real time operation. The controllability of under actuated autonomous vessels under various navigation conditions would thus remain an area of critical concern in the future. Not only the challenges in the design of marine vessels as autonomous cyber physical systems but also their safety under adversarial attack exposes them to significant risk.

A general framework for autonomous ship navigation has been discussed in (Perera, 2020). The aspect of autonomy and intelligent control enters the cyber physical system in the navigation and guidance blocks (Dezfoulian, 2013; Bhoyar, 2019). Four main categories of intelligent control (Antsakis, 1993) applied to marine craft for protection against adversarial attack have been listed in literature as statistical learning, Bayesian state estimation, fuzzy logic and expert systems. Some combinations have also been explored like in (Brossard, 2019)

The manner in which statistical learning (Vapnik, 1998; Shen, 2019) can be implemented is described in earlier works (Ceo, 2006; Bhoyar, 2019) using the hybrid automaton model for the purpose of intelligent control. See also control parameter identification and reinforcement learning control (Back, 1993; Dracopoulos. 1997). A security intrusion or adversarial attack was considered (Bhoyar, 2019) to occur in the communication channels. It was then described how learning based control has been recently shown to be highly vulnerable to adversarial intrusions.the design of the loss function would critically affect the choice of probabilities of state transition (Erbes, 2005). See also (Szegedy, 2013; Sun, 2018; Roberts 2019;Wieland, 2019) Learning based methods tend to work based on weak and local statistical irregularities which is very different from the causal relationships between parts of the information set that humans are sensitive to (Berad, 2001) Unfortunately that poses a serious drawback. As opposed to this, state estimation according to our results (Bhoyar, 2019) suggest robustness of the intelligent control system based upon it. It was shown therein that the difference between the two methods of intelligent control is well captured by the abstract concept of the hybrid automaton (Alur, 1995;

Alur, 2000; Alur, 2011;Alur, 2015; Branicky, 1995;Hespanha, 2004;Johansson, 1999; Lygeros, 1999) which has been important for understanding the advantages of state estimation methods. However, state estimation based control also has limitations in terms of computational effort and memory required. In particular the sequential Monte Carlo method (particle filter) used in (Bhoyar, 2019) is expected to present computational challenges when considered by designers as regards real time implementation (Snyder, 2008) .

In this work, coordinated motion under adversarial cyber attack is considered with seven such under actuated marine surface craft in mind designed primarily for following a leader, keeping in view the limitations of actuation. The intelligent control is implemented in this system via a particle filtering state estimator. We study the system of these craft in coordinated motion under adversarial attack occurring by way of measurement noise (jamming) It is found that more craft exposed to the attack allows the filter to perform better in terms of effectiveness, in a counterintuitive way. This can be attributed to the choice of the importance distribution and the leader follower model selected. We suggest that this could be considered further in terms of reducing particle number to counteract the computational effort required when more craft are included in the formation.

2. The leader follower craft model

Depending on the demand of actual naval combat operations, the fleet commanders could make use of different naval formations for the marine craft described above. Simple formations include

- Line ahead, in which each craft or vessel follows in the wake of the craft ahead
- Line of bearing, in which the craft or ships are deployed along a line running at a definite angle to the course of the lead craft
- Echelon formation, in which each craft follows to the right or left of the wake of the craft ahead
- Line abreast, in which the craft are deployed in a line perpendicular to the course

Though with the flexibility available to the fleet commanders of making use of different naval craft formations during combat operations, good old traditional and simple "line ahead" is still very effective in minimizing own damage and it is for this reason that the present study has concentrated this naval formation.

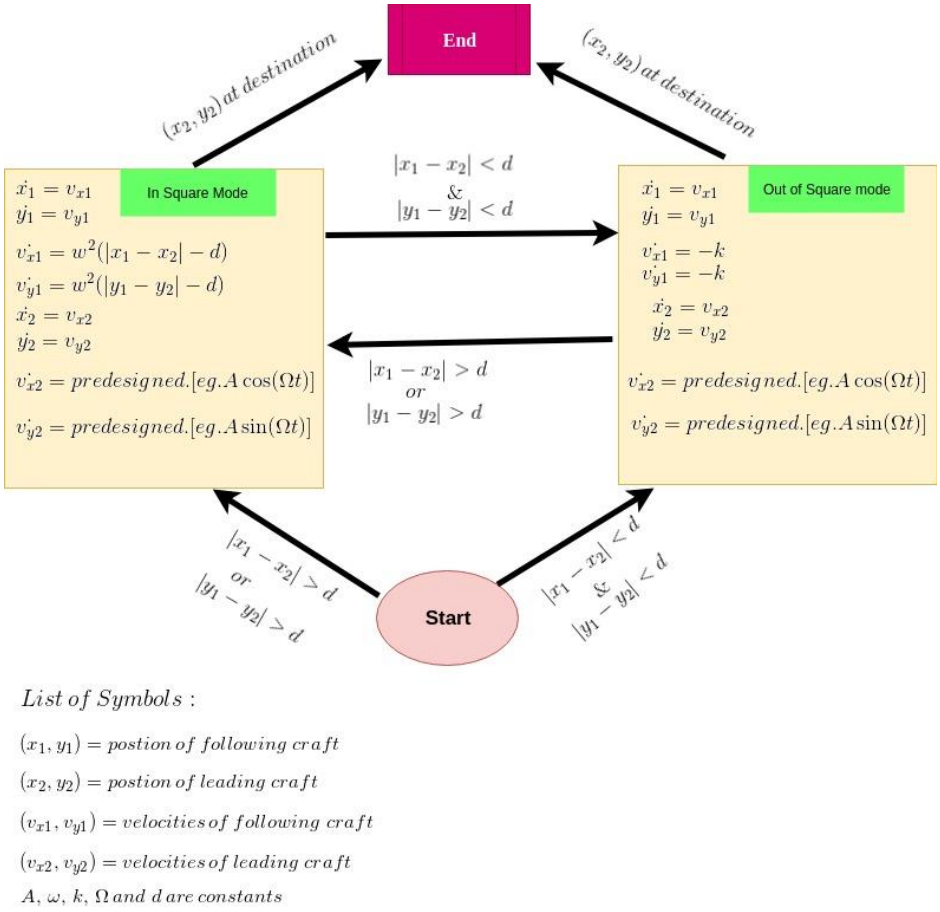
There are usually three broad approaches for multi-agent coordination reported in the literature - leader following, behavioural, and virtual structures (Bujorianu, 2012) The line ahead craft formation would fall in the leader follower category. The general advantage of the leader follower approach is reduction in tracking errors and that standard control techniques can be applied (Chunyu, 2009). Another benefit is that the motion of only the leader determines trajectories; therefore, the result is a simple controller better suited for underactuated marine craft.

The marine craft are assumed to manoeuvre according to the model described below in the line ahead class. We connect the model and the cyber attack with the actual physical design in the next subsection. Then we discuss stochasticity that is brought into the model and the filter that is put in as a safeguard. Following this, we note the outcome of the cyber attack

2.1 Deterministic dynamics

The leading craft follows a path which is independently decided. It can be predetermined or decided on the fly. The following craft however attempts to maintain a distance beyond a square region centered on the leading craft. If the following craft enters into this region a strong braking thrust is applied by the craft impeding its further movement. If the following craft is beyond the region, a thrust is applied accelerating the following craft towards the leading craft. This thrust magnitude is kept proportional to the separation between the craft in this mode of operation. This rule of dynamical motion of the craft is referred to as the leader-follower craft motion model. The first follower then plays the role of the leader for the second and so on. We consider upto seven such crafts. We recall below the representation of such a system in the case of two marine craft for simplicity, in terms of a hybrid automaton (Hespanha, 2004)

Figure 1 shows the hybrid automaton with two modes of operation (“in square mode” and “out of square mode”) These form the set Q of discrete variables of the automaton. The continuous variables of the hybrid automaton are x_1 , y_1 , v_{x1} , v_{y1} representing the position coordinates and velocity components of the following craft, and x_2 , y_2 , v_{x2} , v_{y2} representing the position coordinates and velocity components of the leading craft. The system of a pair of craft which we refer to as the fleet thus has a dynamical state which is specified by eight variables. These change in time as dependent variables of an ordinary differential equation in each of the modes of operation of the hybrid automaton as shown above. The differential equation itself contains the information about the dynamical motion rule used and thus is obtained from the motion model detailed above.



List of Symbols :

$(x_1, y_1) = postion\ of\ following\ craft$

$(x_2, y_2) = postion\ of\ leading\ craft$

$(v_{x1}, v_{y1}) = velocities\ of\ following\ craft$

$(v_{x2}, v_{y2}) = velocities\ of\ leading\ craft$

$A, \omega, k, \Omega\ and\ d\ are\ constants$

Figure 1: Hybrid Automaton representing the leader-follower interaction model for two marine (Bhoyar, 2019)

The case of a single marine craft has been addressed by (Rigatos, 2013) and two by (Bhoyar, 2019) We have examined such a case of seven marine craft, each following successive craft in a leader follower fashion. The first one is cruising on a predesignated path or a motion law involving exclusively its state variables. Each craft senses the position of the successive craft and this measurement is included in the dynamical model for its motion. The dynamics involves some amount of stochasticity owing to secondary behaviour of engineered systems like actuators and drives for example. But there is an element of stochasticity in the attacks which might be carried out on the sensor measurements. We model an attack as noise occurring in the measurements. The group of marine craft are considered to have a state estimator to mitigate such an attack. As expected, such a protection mechanism works adequately upto a certain intensity of noise introduced as an attack. We detail this in the next subsection.

2.2 Physical Design of Network and Adversarial Cyber Attack

The marine craft are actually viewed as a large communications network with five layers viz. physical, data link, network,transport and application layers (Vadlamani et. al., 2016) Some authors have recently suggested that the physical components of a vehicle system instead be understood from the point of view of communications and control, in terms of three levels viz. sensing, communication and control levels (El-Rewini et. al., 2020) This has been done in the context of land vehicles. We refer to this view, but taken over to context of marine craft

“At the bottom of the hierarchy is the sensing layer, which is vulnerable to spoofing and eavesdropping attacks on vehicle sensors, such as the inertial or radar sensors. Above the sensing layer is the communication layer, which encompasses both inter-vehicular and intra-vehicular communications and is vulnerable to eavesdropping attacks and the manipulation of messages between vehicles and roadside infrastructure. The communication layer is also susceptible to threats that propagate upward from the sensing layer, which is made of vehicular sensors. Threats to both the sensing and communication layers can affect the top most tier, the control layer, which describes automated vehicular control techniques, such as vehicle speed and steering control.” (El-Rewini

et. al., 2020, p2)

The mathematical model we discuss in this work would be implemented in the processing block of the control system, typically onboard or on shore computing machines. The adversarial attack is assumed to take place on the sensors in the primarily presented layer or lowest layer of the three. The sensing layer is made up of vehicle dynamics and environmental sensors, which are vulnerable to eavesdropping, jamming, and spoofing attacks. Hardware involved in this layer is lidar/cameras, radar/ultrasonic sensors, GPS/TPMS, gyroscopic sensors etc. which would be the immediate subject of the attack. We limit ourselves to the widely used class of attacks called the jamming attack. In such an attack, the signal to noise (or noise and interference) ratio is reduced after gaining access to the signal carrier for the particular measuring device transmitting its signal to the processing unit. In literature, jamming attacks and their countermeasures have been extensively studied and categorized. (Osanaiye, Alfa and Hancke, 2018) Non invasive countermeasures (i.e. those involving little change in hardware and more in the information processing unit) have been recommended (Caprolu et. al., 2020)
"Despite the availability of several anti-jamming schemes, vessels require the adoption of non-invasive protocols, that should be thoroughly assessed and contextualized in order not to require expensive and time-consuming hardware change operations, while providing seamless integration with current technologies and ease of use."

2.3 Safeguard against the Cyber Attack: Stochasticity and Particle Filtering

The differential equations in the two modes are appended by noise terms to bring in stochasticity due to actuators and due to measurement. The attack is expected to take place in the measuring system. The mitigation is achieved as follows. Replicas of the systems, called particles are imagined, each with states similar to the actual system. The dynamics of the system involves differential equations which involve the actual system state as dependent variables. These actual variables are replaced by the estimated variable obtained from particles. Particles are themselves evolved also according to this dynamics. In addition, though, at each time step, the particles are weighted and selected according to a distribution for obtaining the estimated state. This is essentially the part equivalent to the particle filter.

2.4 Outcome of the Cyber Attack

Even though autonomous marine craft are pre-programmed, they would still be communicating with the command and control station, who will be watching the trajectory or the path of these vessels as well as the general health of the machinery, onboard sensors and other payloads. Therefore, this presents a window of opportunity for the attacker to displace the vessels from their target paths, thereby fulfilling the attacker's objective. The Fleet Commander owning these autonomous assets will have no choice but to abort or modify the mission profile. The outcome would practically end up depending upon the action plans of the attacker and the fleet commander, though the fleet commander would be greatly aided by the computational safeguard we suggest.

3. Numerical Method, Algorithm and Simulation

We present some details about various control structures we used in our algorithm, then note three parameters which we vary in our simulations and present the algorithm.

3.1 Control structures

A function 'update' was prepared for updating the state of the system of craft (which we refer to as a fleet) This involves the differential equation for the dynamics, the Runge Kutta discretization time step size and the previous state. No stochastic dynamics is included in this function though the estimated state is actually used instead of previous actual state (which is what one would if the vehicle sensors were 100% modelable) We have however provided the previous actual as well as the estimated state in the function, just in case it would be needed to include both in the dynamics in the future. But as such the previous actual state is not presently being employed within the function code.

We use two other functions 'dash' and 'prepk' in the above update function. 'Prepk' prepares the Runge Kutta multivariable change in the state of the fleet by adding the four standard contributions (of fourth order Runge

Kutta method) together and ‘dash’ adds this change to the state of the fleet. A special function is needed to add states which we call ‘addfleet’.

The main control structure which contains the dynamics of the system is simply named as ‘f’. This function contains the (nonlinear) differential operator. We have allowed for the estimated state to be accessible to this. Normally, in the case of usual solvers of differential equations, we would have had just the actual state. In case of an attack, the actual state being used would mean that we have not provided any protection. When we wish to switch on the protection we use the estimated state wherever we otherwise require to use the actual state in this operator. We find this function useful. By providing such a function data structure for the differential operator, we can easily change the differential equation whenever needed.

3.2 Parameters of importance in simulations

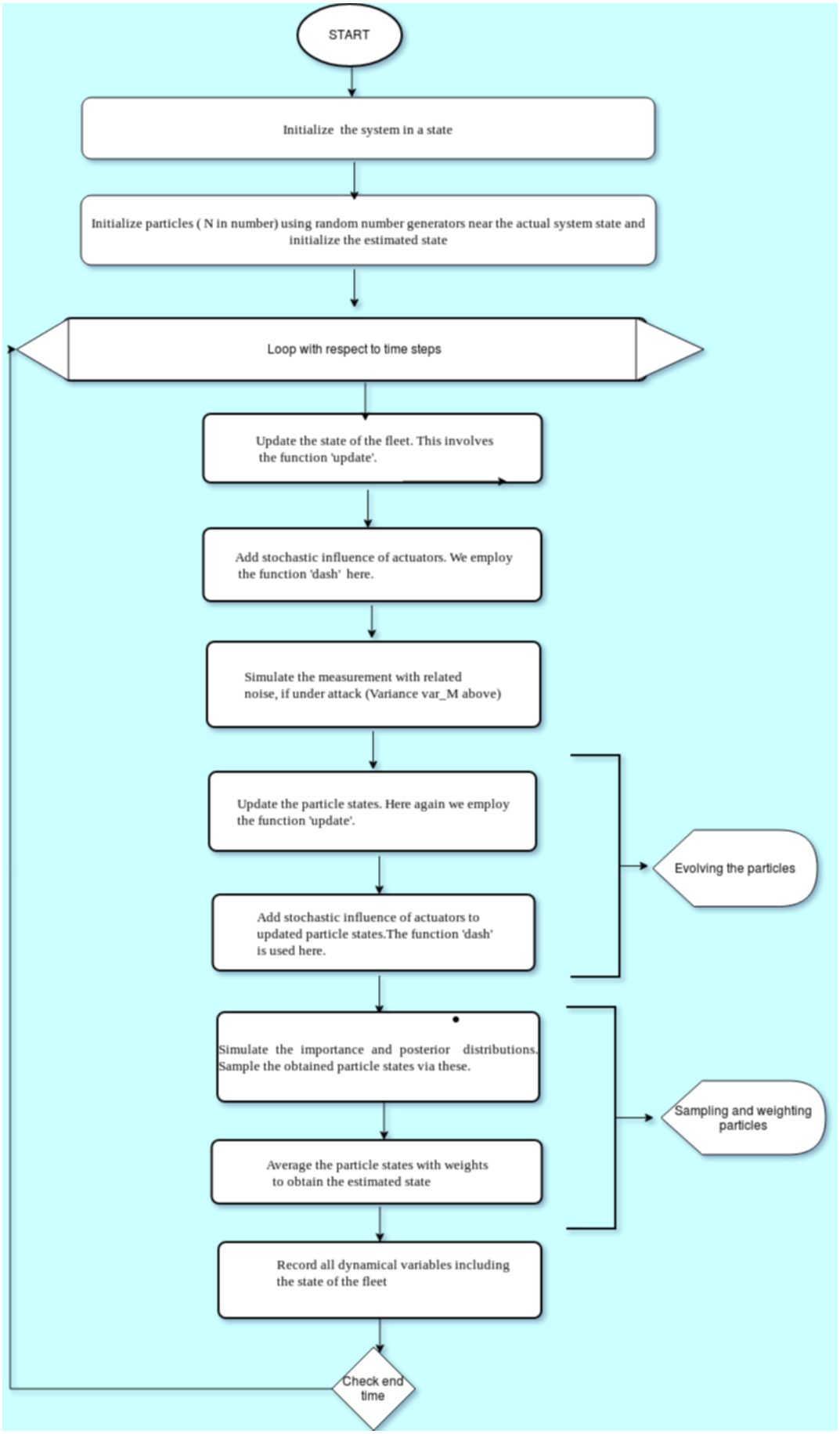
The number N of particles of the filter and the importance distribution are controlled in our code for the purpose of this work. The effect of the attack is mitigated via this importance distribution. We include the effect via state variables of two, three and four marine craft. This way we seek to study how the system responds under a particle filter to attack if the number of craft in the fleet increases.

We also allow for four separate variances -

1. the variance used in random generation of particles.
2. the variance used in the stochastic part of the system dynamics, which represents actuator stochasticity.
3. the variance used in the stochastic part of dynamics while being used for estimation purposes. This is separate from the one above as it represents judgement of stochasticity of the system dynamics or judgement of stochasticity of actuators as opposed to representing actual stochasticity.
4. the variance that represents the adversarial attack (var_M) and this is the main concern in this work.

3.3 Algorithm

The main algorithm is provided below.


START
Initialize the system in a state
Initialize particles (N in number) using random number generators near the actual system state and initialize the estimated state
Loop with respect to time steps
Update the state of the fleet. This involves the function 'update'.
Add stochastic influence of actuators. We employ the function 'dash' here.
Simulate the measurement with related noise, if under attack (Variance var_M above)
Update the particle states. Here again we employ the function 'update'.
Add stochastic influence of actuators to updated particle states.The function 'dash' is used here.
Evolving the particles
Simulate the importance and posterior distributions. Sample the obtained particle states via these.
Average the particle states with weights to obtain the estimated state
Sampling and weighting particles
Record all dynamical variables including the state of the fleet
Check end time

We essentially have employed bootstrap filtering with unbiased sampling.

4. Results

We have simulated main cases of the marine craft system wherein the attack is mounted on the first two, three and four craft. The remaining cases are similar to the one with the attack on four craft. In each main case we increase the number of particles from 10 to 20 and call them subcases. As the number of particles increases , the filter provides more robustness to uncertainty and one can interpret that the level of offered protection increases. Further, in each of these subcases we increase the measurement variance in position, which represents the attack intensity, from 5.0 length units squared to 15.0 length units squared.

It should be noted that there are only two scales of physical quantities in the system, length L and time T. We have obtained all physical quantities in terms of L and T. For the purpose of this work we assume L = 1.0 metre and T = 1.0 second. This sets the speed of the leading craft to 19.4 knots. The remaining craft start from rest. Initially, each of the remaining craft are separated from successive craft by 5 km. A total time of operation of 10 minutes has been simulated. However, the results can be scaled dimensionally to any specific size and time period depending upon the application.

We first show the trajectories when there is no attack on the system.

4.1 ***Without attack***

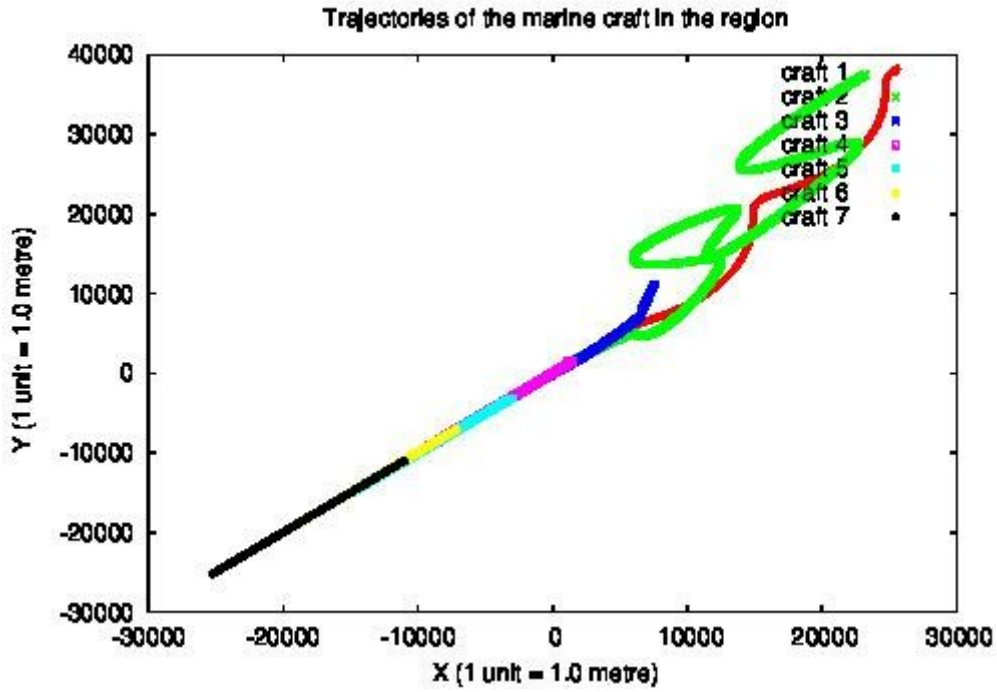


Figure 2: Motion trajectories without any attack.

The red craft in Figure 2 is the leader and the craft 2 (green) follows immediately. The proportionality constant of distance is kept high to demonstrate the sensitivity of the system to this parameter. We see that the second craft is pushed back if it enters the square region about the leading craft. The other trailing craft have a lesser value for this constant and hence follow a more orderly path.

4.1 Attack on two leading craft

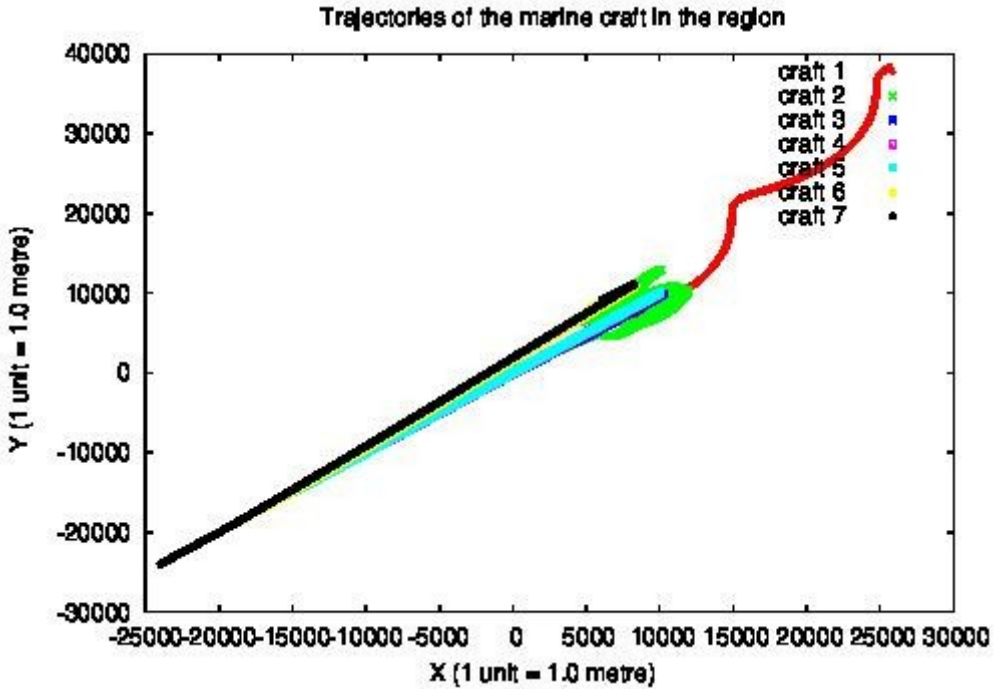


Figure 3 : Attack on two craft N=10 var_M=5.0

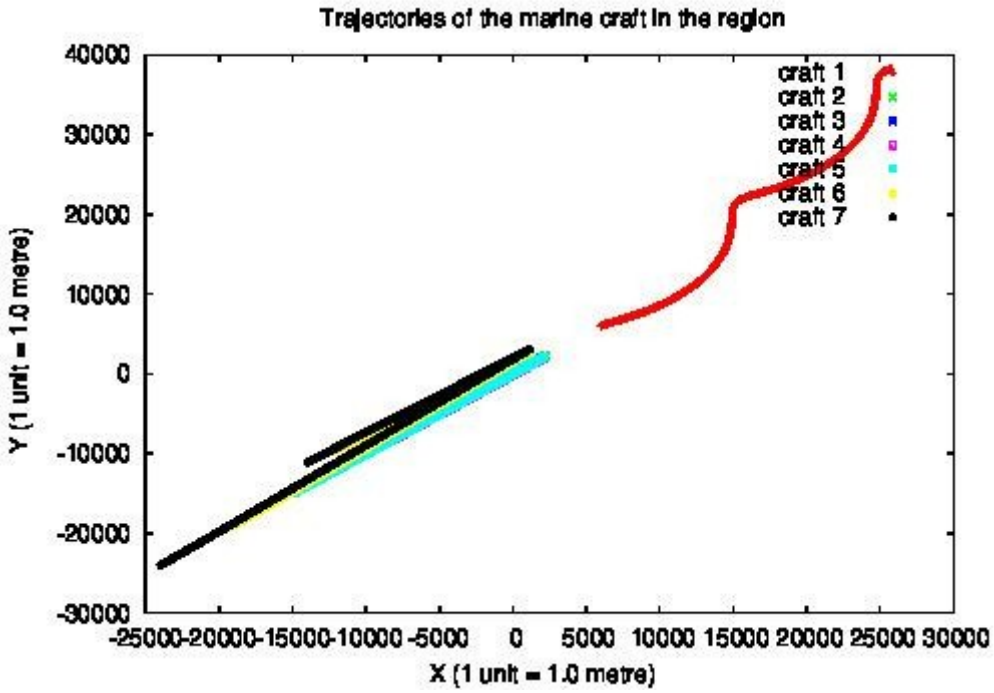


Figure 4: Attack on two craft N=10 var_M= 15.0

The attack is seen in figures 3 and 4 to increasingly disrupt the trajectories as its intensity increases. We then enhance the safeguard by increasing the number of particles to 15 below.

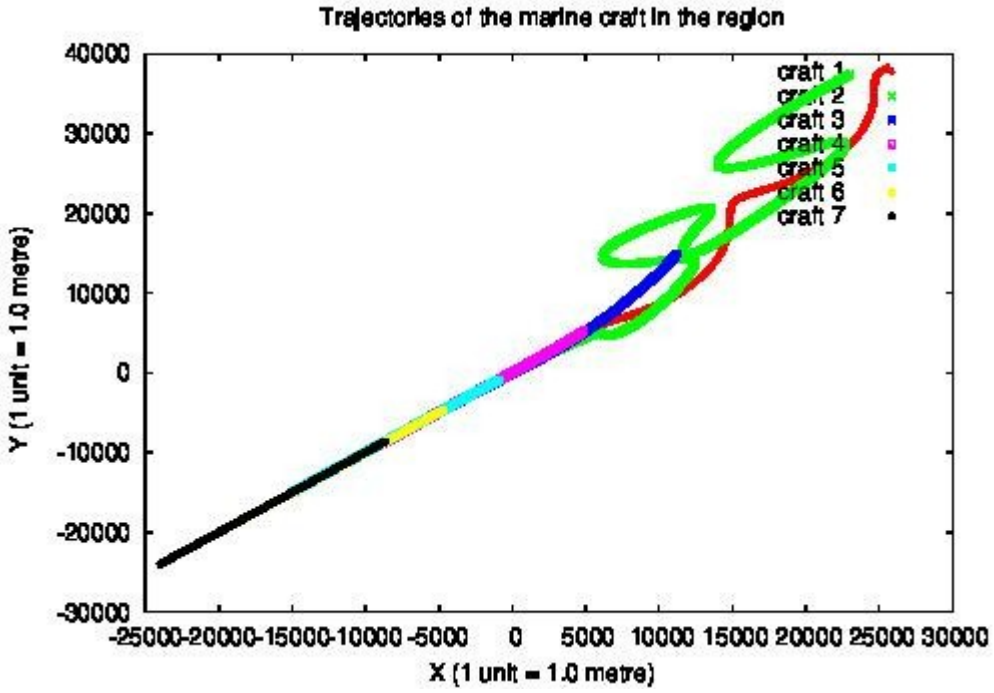


Figure 5: Attack on two craft N=15 var_M= 5.0

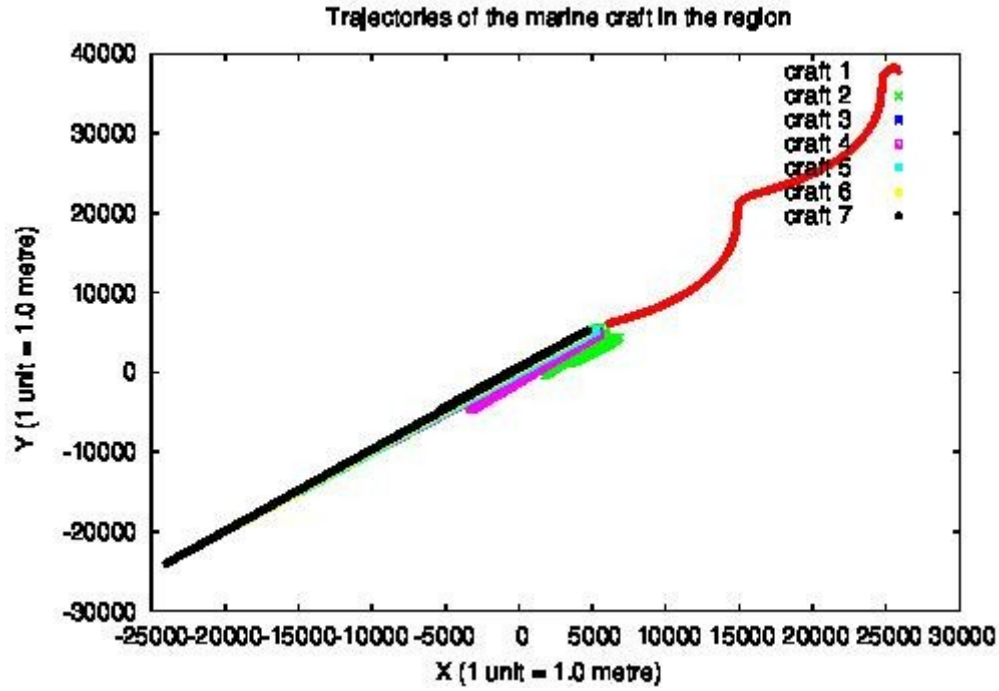


Figure 6: Attack on two craft N=15 var_M= 15.0

For 15 particles, we see in figures 5 and 6 that the level of protection has increased but there is still appreciable disruption when the maximum level of attack is reached in figure 6 above. We now increase the number of particles further to 20 below.

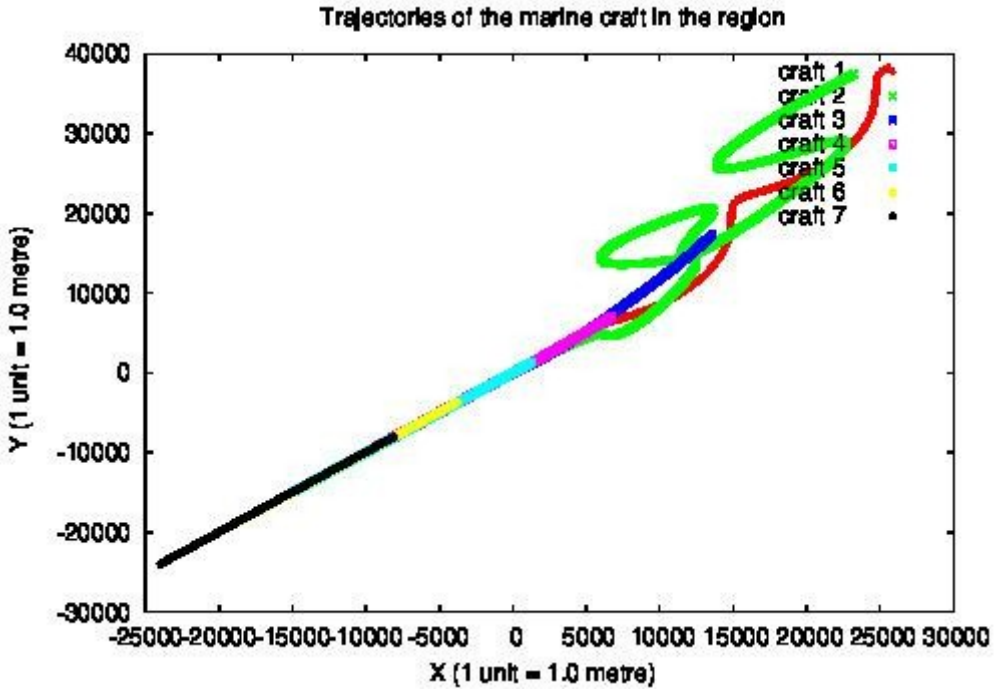


Figure 7: Attack on two craft N=20 var_M= 5.0

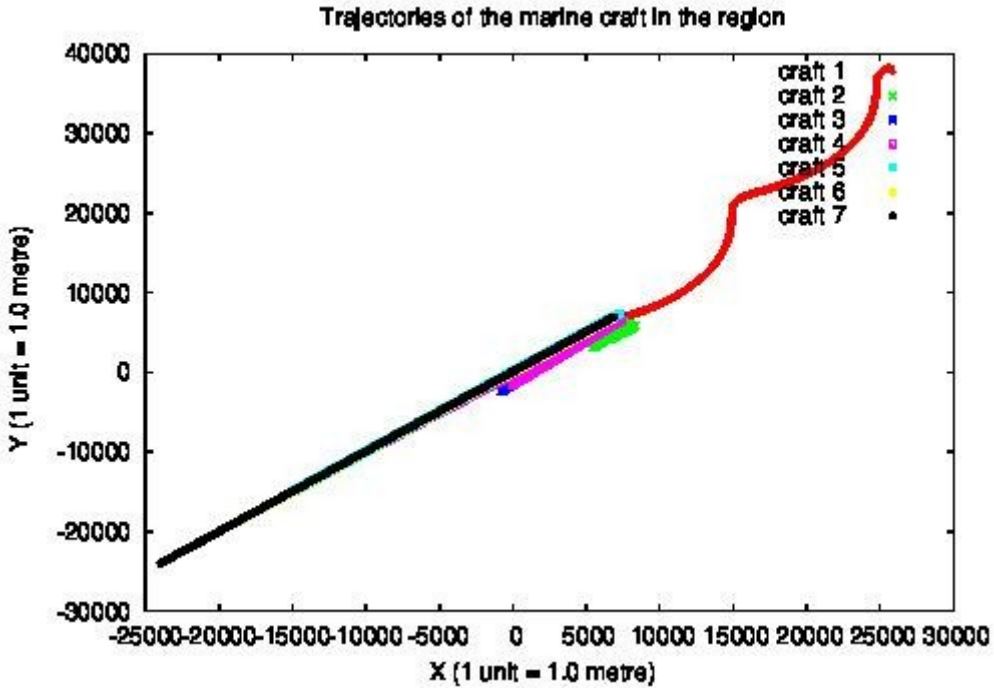


Figure 8: Attack on two craft N=20 var_M= 15.0

There is no significant change in the level of protection offered above in figures 7 and 8 as compared to 15 particles.

4.2 Attack on three leading craft

We now allow the attack to be mounted on three vessels and proceed again to study the trend with an increasing number of particles. We set the number of particles to 10 and examine the three levels of attack as before.

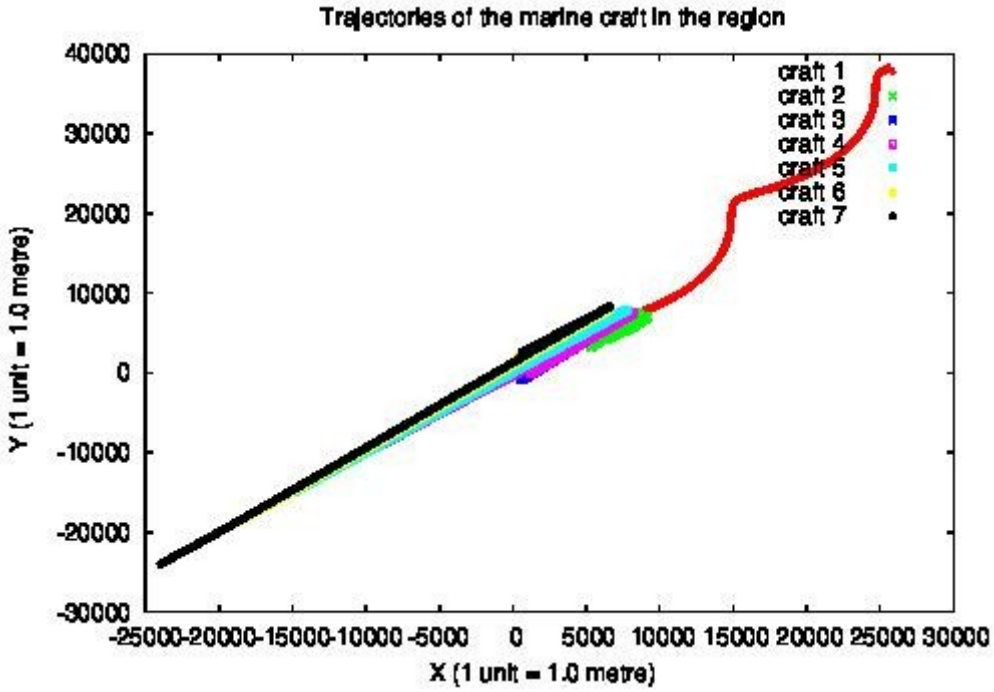


Figure 9: Attack on three craft N=10 var_M= 5.0

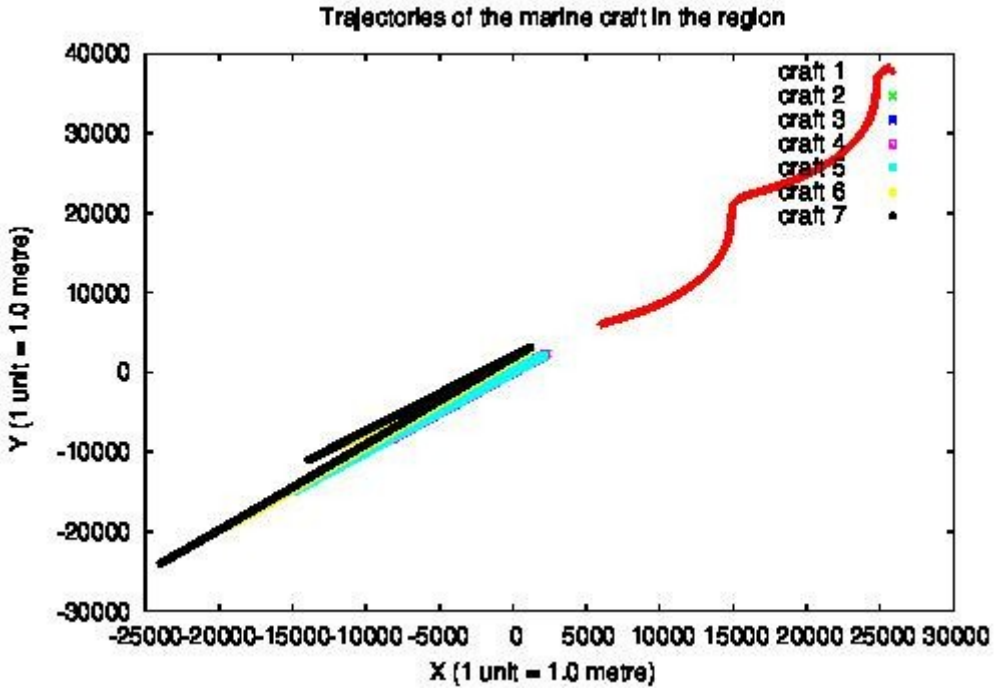


Figure 10: Attack on three craft N=10 var_M= 15.0

The protection offered by 10 particles offers only a slight improvement as compared to the case when two craft were under attack as seen in figures 9 and 10. The situation is better with 15 particles below.

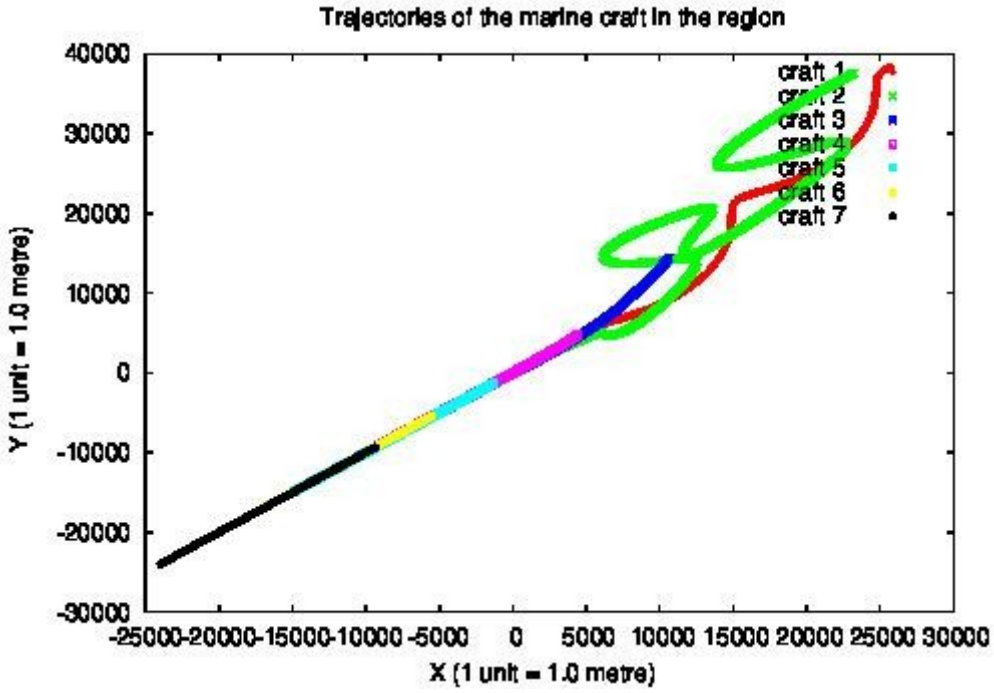


Figure 11: Attack on three craft N=15 var_M= 5.0

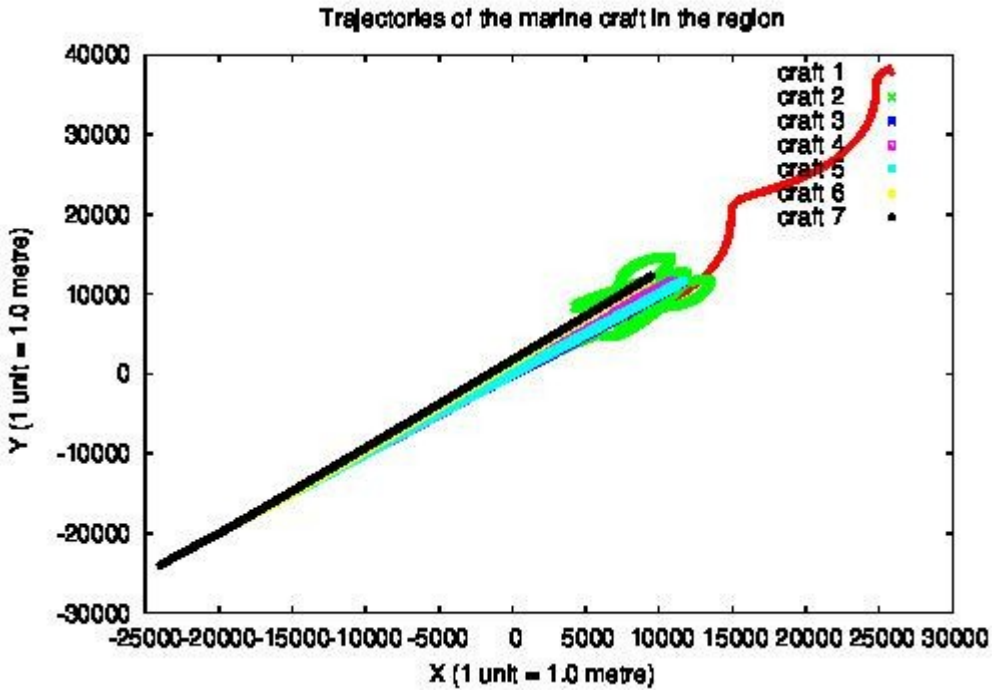


Figure 12: Attack on three craft N=15 var_M= 15.0

The disruption is visibly a little lesser in figure 12 when the particles are 15 in number as compared to the response when only two craft were under attack in figure 6. We now present the disruption when 20 particles are employed.

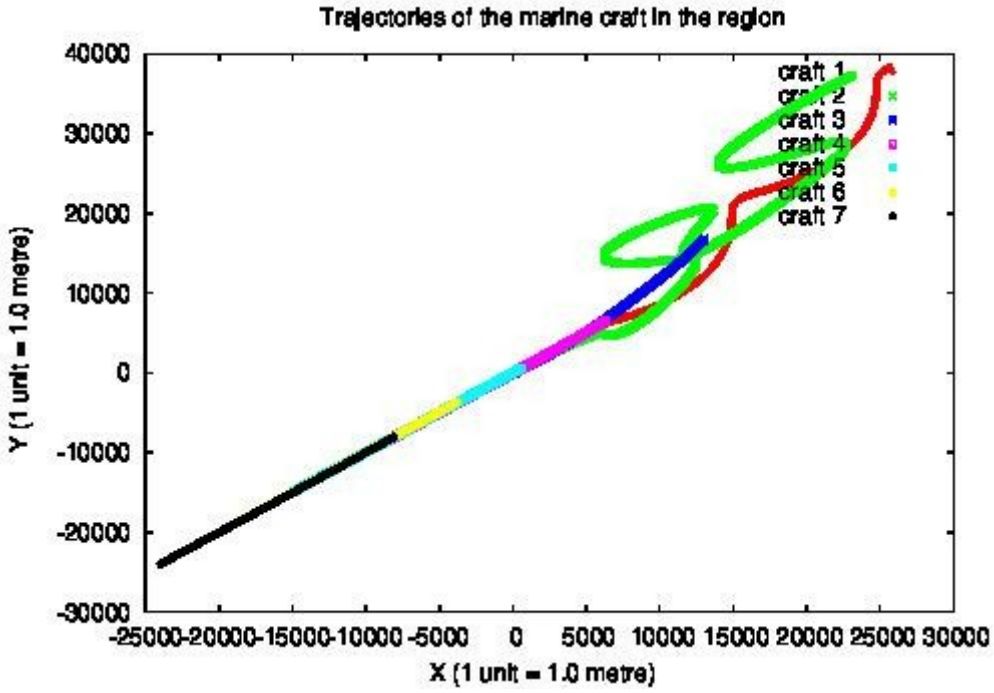


Figure 13:Attack on three craft N=20 var_M= 5.0

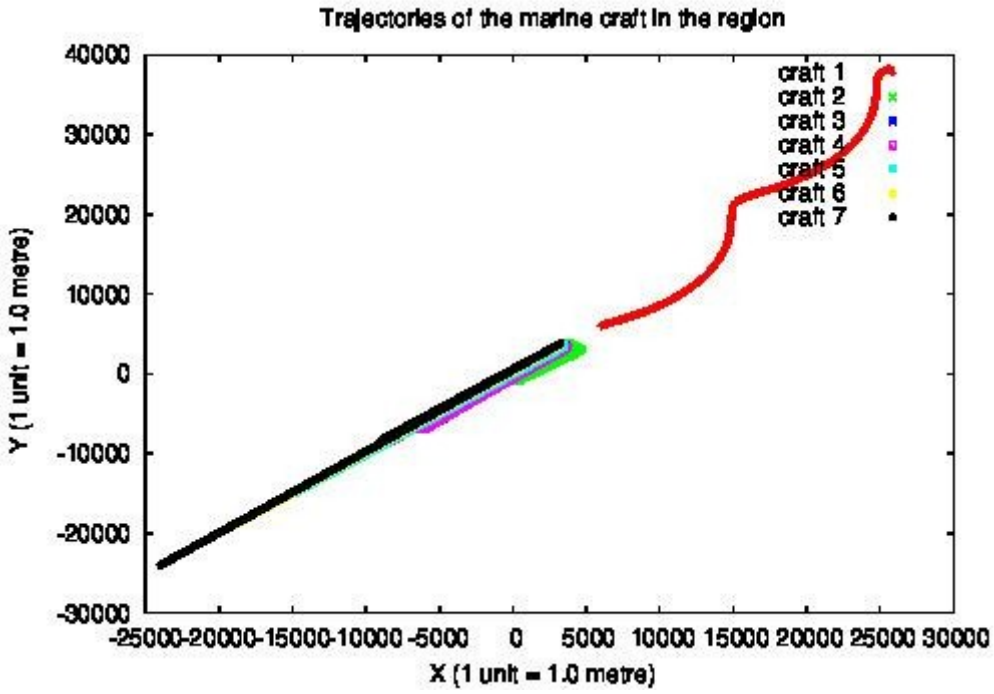


Figure 14: Attack on three craft N=20 var_M= 15.0

The protection offered when 20 particles (figures 13 and 14) are employed is significant but there is still a disruption at the third level of attack, the maximum out of the levels we consider.

4.4 Attack on four leading craft

With four craft exposed to attack, we see that the situation improves even further. First, we check with the lowest level of protection, i.e. 10 particles. We show only the picture at the maximum level of attack.

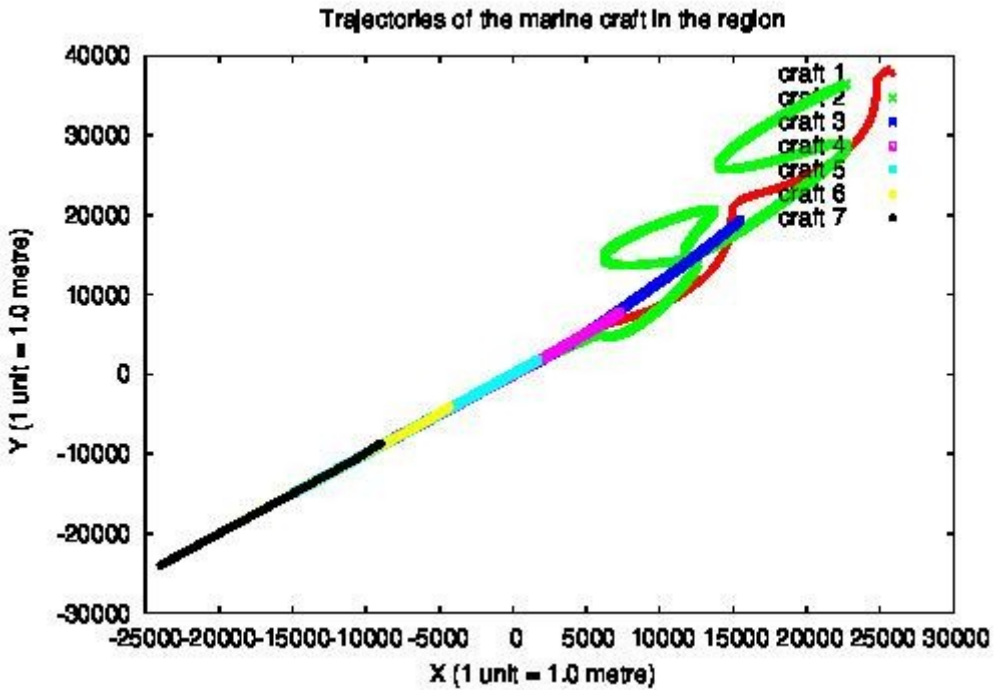


Figure 15: Attack on four craftN=10 var_M= 15.0

We see above in figures 15 that the disruption is hardly visible, especially in the third craft trajectory, unlike the previous two main cases when only two and three craft were under attack. We now increase the number of particles to 15 below. The picture remains unchanged. We show some instances below

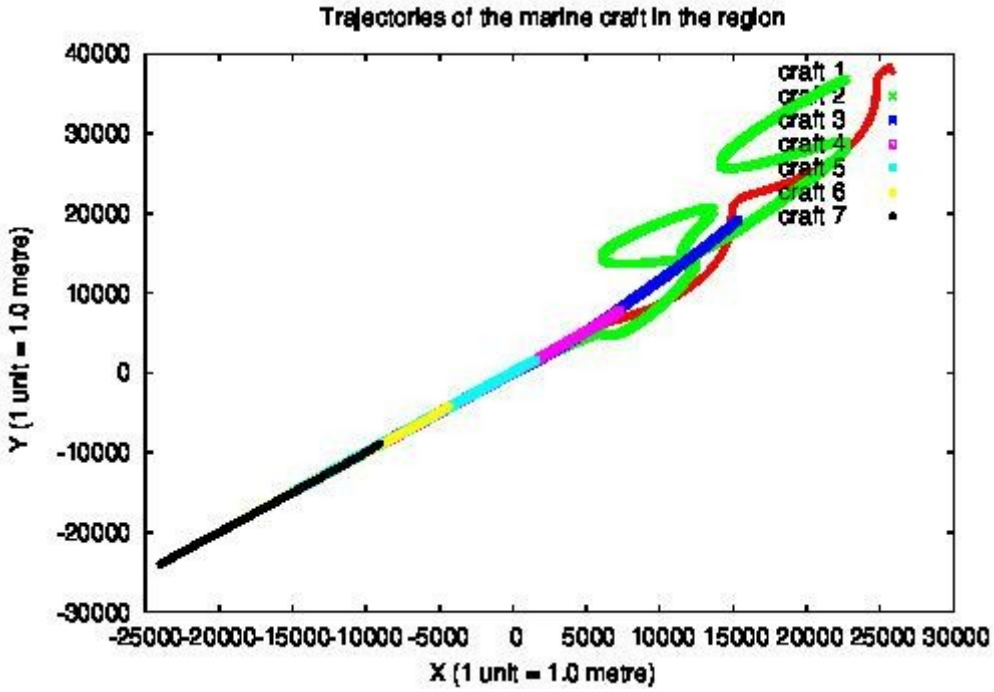


Figure 16: Attack on four craft N=15 var_M= 15.0

We see in figure 16 that at the level of 15 particles, the safeguard is performing well with hardly any disruption. The situation continues further. We again show only the maximum attack level below.

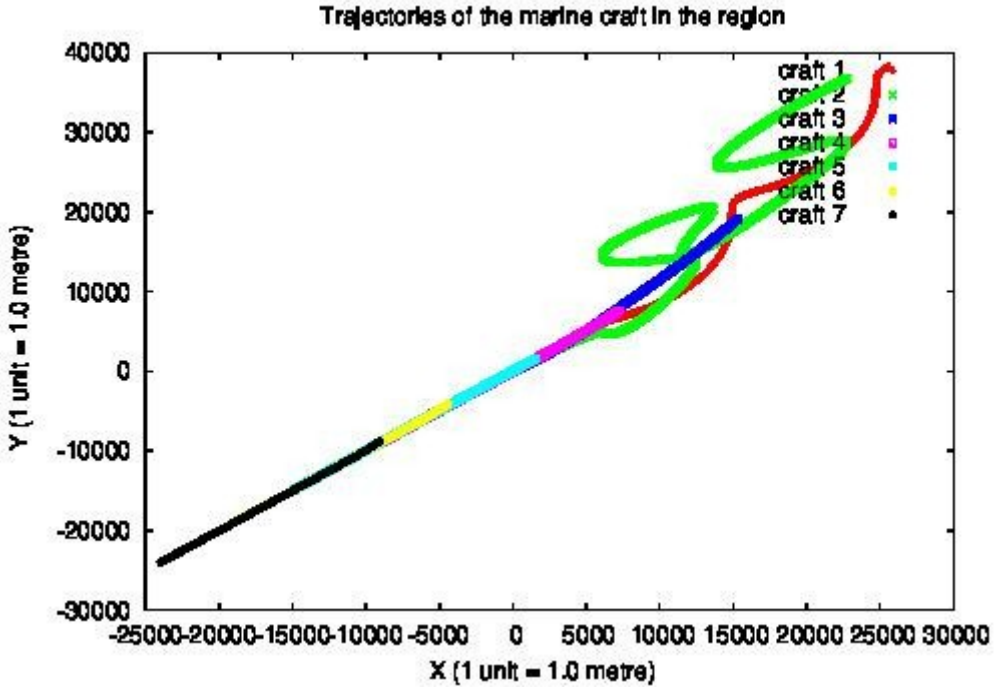


Figure 17: Attack on four craft N=20 var_M= 15.0

At the level of safeguard of 20 particles above in figures 17, we continue to see negligible disruption.

Overall, we see that the attack is better mitigated with an increasing number of particles as expected. As far as the number of attacked craft is considered, the results are also as expected for the case of two craft. The trajectories increasingly depart from the regular behaviour as the attack intensity increases. Increasing the number of particles improves the situation, but the attack is clearly evident. In the case of three attacked craft, the trend is the same. However, only the last level of attack is disruptive with the lower attack levels not very successful. The effectiveness of the particle filter is most notably observed when four leading craft are attacked. For all levels of attack and all three particle numbers. we see that the trajectories have not appreciably departed from the regular pattern.. This is the main observation in this work. Attacks on more craft were studied but no significant departure from the regular pattern has been observed. Though we have reduced the proportionality constant of separation distance in their case, the fact that the craft near the leader get less disturbed is noteworthy.

5. Discussion

As expected, we find that increasing the particle number offers better protection against attack in general by providing a quantification of uncertainty presented by the attack. More interestingly, the estimator works more efficiently if the attack has been mounted on more craft. We find that four or more craft being subjected to attack assures a considerable robust response. We attribute such behaviour to the choice of the parametric distribution employed and the craft interaction model. This rather improved performance of the particle filter which we observe offers designers an approach to better protection at low particle numbers. The particle filter, though well suited for nonlinear models with non Gaussian dynamical random variables, presents a curse of dimensionality problem. The number of particles required for robust uncertainty quantification can be impractical for high-dimensional systems. It has been proven that the number of particles grows exponentially with dimensions (or degrees of freedom) (Snyder, 2008) It is not known how high this dimensionality can be for it to be acceptable in case of a particular application like autonomous craft moving in a line ahead formation. We find that this issue could possibly be avoided. The results above indicate that for a particular leader follower model, the effect is mitigated as the accuracy of estimation improves with the number of craft. Further studies would be required to assess how the leading vehicle trajectory and different leader follower models would affect this result.

6. Conclusion

Autonomous marine vessels, especially underactuated ones, are highly susceptible to adversarial attacks and intelligent control needs to be further developed to make such attacks very costly. The technique of Bayesian estimation based intelligent control was earlier shown to hold promising advantages over statistical learning based control. It was shown that even basic filter parameters like particle number could be effectively used to design effective safeguards in problems of marine vehicle following and collision avoidance. However, the limitations of the suggested estimation technique (sequential monte carlo or particularly, particle filtering) are believed to be compelling enough to investigate other options. The exponential increase of computational effort with the number of particles is the main bottleneck that has been indicated in literature and which has led to such a view. This problem would be especially severe in the case of underactuated marine vessels.

Suggesting a potentially contrary direction for future work, we have demonstrated via simulations that the particle filtering technique still has potential for implementation if employed with certain dynamical models for marine vessel interaction. We have considered marine vessels operating in a leader-follower fashion, the simplest and widely preferred line ahead formation, applicable to underactuated craft. Such a formation has been shown to demonstrate more robustness to jamming cyber attack if more degrees of freedom get exposed and are adequately addressed by the particle filter. Such a robustness could possibly be observed in other leader-follower models and for other choices of filter parameters or even filters. These studies would enable designers to consider employing a lesser number of particles when more marine vessels are exposed to adversarial attack. We suggest that this approach be considered to offset the exponential increase of computational effort expected when more marine vessels are incorporated into autonomous leader-follower formations.

References

Alur R. (2011) Formal verification of hybrid systems in EMSOFT (eds Chakraborty, S. Jerraya, A., Baruah, S. K. & Fischmeister, S.) *ACM*, 273–278.

Alur R. Principles of Cyber-Physical Systems (MIT Press, 2015).

Alur R., Henzinger, T., Lafferriere, G. & Pappas, G. J. (2000) Discrete Abstractions of Hybrid Systems. *Proc. IEEE* 88, 971–984.

Alur R., Courcoubetis C., Nicollin X., Halbwachs N., Henzinger T.A., Ho P.-H.-, Nicollin X., Olivero A., Sifakis J., Yovine S. (1995) The Algorithmic Analysis of Hybrid Systems. *Theor. Comput. Sci.* 138, 3–34.

Back Thomas, Schwefel Hans-Paul (1993). An overview of evolutionary algorithms for evolutionary computation. *Evolutionary Computation* 1(1):1-23

Branicky M.S. (1996) General hybrid dynamical systems: Modeling, analysis, and control. In: Alur R., Henzinger T.A., Sontag E.D. (eds) Hybrid Systems III. HS 1995. Lecture Notes in Computer Science, vol 1066. Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0020945

Bhoyar Amolkumar, Rajneesh Sharma, Sukratu Barve and Rakesh Kumar Rana (2019) Intelligent Control of Autonomous Vessels: Bayesian Estimation Instead of Statistical Learning? *Proceedings of the International Conference on Marine Engineering and Technology,* Muscat, Oman DOI:10.24868/icmet.oman.2019.008

Beard R. W., Lawton J. and Hadaegh F.Y. (2001) A coordination architecture for spacecraft formation control *IEEE Transactions on Control Systems Technology*, 9, no. 6. 777-790, doi: 10.1109/*87.960341*.

Brendel, W. & Bethge, M. (2019) Approximating CNNs with bag-of-local-features models works surprisingly well on ImageNet. *Proc. Int. Conf. Learning Representations (ICLR).*

Brossard Martin, Axel Barrau, Silvère Bonnabel (2020) AI-IMU Dead-Reckoning. *IEEE Transactions on Intelligent Vehicles*, Institute of Electrical and Electronics Engineers 10.1109/TIV.2020.2980758

Bujorianu Luminita Manuela (2012) Stochastic reachability analysis of hybrid systems. Springer

Caprolu Maurantonio, Di Pietro Roberto, Raponi Simone, Sciancalepore Savio, Tedeschi Pietro (2020) Vessels Cybersecurity: Issues, Challenges, and the Road Ahead (to appear *IEEE Communications Magazine*)

Ceo Ni (2006) Keynote address National science foundation workshop. *Business Wire.*

Chunyu, J.; Qu, Z.; Pollak, E.; Falash, M. A (2009) New Multi-objective Control Design for Autonomous Vehicles. In Optimization and Cooperative Control Strategies; Hirsch, M.J., Commander, C.W., Pardalos, P.M., Murphey, R., Eds.; Springer: Berlin/Heidelberg, Germany; pp. 81–102.

Dezfoulian S. Hamid, Dan Wu, Ahmad Imran Shafiq. (2012-2013) A generalized neural network approach to mobile robot navigation and obstacle avoidance proceedings. *Proceedings of the International Conference (IAS)* 12, 26-29.

Dracopoulos Dimitris C (1997) Evolutionary learning algorithms for neural adaptive control. Springer.

El-Rewini Zeinab, Sadatshara Karthikeyan, Selvaraj Daisy Flora, Plathottam Siby Jose, Ranganathan Prakash (2020) Cybersecurity challenges in vehicular communications *Vehicular Communications* 23, 100214

Erbes T., Shukla S. K., Kachroo P. (2005) Stochastic learning feedback hybrid automata for dynamic power management in embedded systems. *Institute of Electrical and Electronics Engineers (IEEE) Mid-Summer Workshop on Soft Computing in Industrial Application*s 208-213.

Framework for Cyber-Physical Systems (2017) Volume 1, National institute of standards and technology special publication. 1500-201.

Graja Imen, Kallel Slim, Kacem Ahmed Haj, Guermouche Nawal, Cheikhrouhou Saoussen (2018) A comprehensive survey on modeling of cyber-physical systems. *Concurrency and Computation Practice and Experienc*e 32(5):e4850

Henzinger T.A., Sontag E.D. (eds) Hybrid Systems III. HS 1995. Lecture Notes in Computer Science, vol 1066. Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0020945

Hespanha J. (2004) Stochastic hybrid systems: applications to communication networks. Hybrid Systems: Computation and Control: A coordination architecture for spacecraft formation control in computer Science. Springer, 387-401.

Johansson K.H., Egerstedt M., Lygeros J., Sastry S. (1999) On the regularization of zeno hybrid automata. *Systems & control letters*. 38,141-150.

Khaitan S.K. and McCalley J.D. (2015) Design Techniques and Applications of Cyberphysical Systems: A Survey *IEEE Systems Journal*, 9(2) 350-365.

Krzysztof Wróbel, Jakub Montewka, Pentti Kujala (2018) Towards the development of a systems theoretic model for safety assessment of autonomous merchant vessel. Antonioli GE. *Proceedings of the 3rd reliability engineering and system safety.* 178, 209-224.

Lygeros J., Johansson K.H., Sastry S. and Egerstedt M. (1999) On the existence of executions of hybrid automata *Proceedings of the 38th IEEE Conference on Decision and Control (Cat. No.99CH36304)*, 3, 2249-2254

Opeyemi Osanaiye, Attahiru S. Alfa and Gerhard P. Hancke (2018) A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks *Sensors* (18) 1691

Panos J. Antsakis, Kevin M, Passino (1993) *An Introduction to intelligent and autonomous control.* Kluwer

Perera Lokukaluge P. (2020) Autonomous ship navigation under deep learning and the challenges in colregs.*J. Offshore Mech. Arct. Eng*. 142(3) 031102 (10 pages)

Rigatos,Gerasimos G. (2013) Sensor fusion-based dynamic positioning of ships using extended Kalman and Particle Filtering. *Robotica.* 31 (3) 389 - 403.

Roberts, Fred S. (2019) From Football to Oil Rigs: Risk Assessment for Combined Cyber and Physical Attacks *Journal of Benefit-Cost Analysis* 10(2), 251-273.

Sanfelice Ricardo G. (2015) Analysis and design of cyber-physical systems: A hybrid control systems approach. In *Cyber Physical Systems: From Theory to Practice* p.3-31 CRC Press

Shen Haiqing, Hashimoto Hirotada, Matsuda Akihiko, Taniguchi Yuuki, Terada Daisuke, Guoe Chen (2019) Automatic collision avoidance of multiple ships based on deep Q-learning. *Applied Ocean Research*. 86:268-288.

Snyder, C. Bengtsson, T. Bickel, P. Anderson, J. (2008) Obstacles to high-dimensional particle filtering. *Mon. Weather Rev*. 136, 4629–4640.

Sun, L., Tan, M. & Zhou, Z. (2018) A survey of practical adversarial example attacks. *Cybersecur* 1, 9

Szegedy Christian, Zaremba Wojciech, Sutskever Ilya, Bruna Joan, Erhan Dumitru, Goodfellow I. J, Fergus Rob (2013) Intriguing properties of neural networks. CoRR abs/1312:6199.

Vadlamani Satish, Eksioglu Burak, Medal Hugh, Nandi Apurba (2016) Jamming attacks on wireless networks: A taxonomic survey *Int. J. Production Economics* 172, 76–94

Vapnik V. N. (1998) *Statistical learning theory.* New York. Wiley

Wang Yufei, Perera Lokukaluge P., Batalden Bjørn-morten (2021) Particle Filter Based Ship State and Parameter Estimation for Vessel Maneuvers Proceedings of *the 31st International Ocean and Polar Engineering Conference.* ISOPE-I-21-4176