World Academy of Science, Engineering and Technology
International Journal of Industrial and Manufacturing Engineering
Vol:10, No:5, 2016

Adopting Flocks of Birds Approach to Predator for Anomalies Detection on Industrial Control Systems

M. Okeke, A. Blyth

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf

***Abstract*—**Industrial Control Systems (ICS) such as Supervisory Control And Data Acquisition (SCADA) can be seen in many different critical infrastructures, from nuclear management to utility, medical equipment, power, waste and engine management on ships and planes. The role SCADA plays in critical infrastructure has resulted in a call to secure them. Many lives depend on it for daily activities and the attack vectors are becoming more sophisticated. Hence, the security of ICS is vital as malfunction of it might result in huge risk. This paper describes how the application of Prey Predator (PP) approach in flocks of birds could enhance the detection of malicious activities on ICS. The PP approach explains how these animals in groups or flocks detect predators by following some simple rules. They are not necessarily very intelligent animals but their approach in solving complex issues such as detection through corporation, coordination and communication worth emulating. This paper will emulate flocking behavior seen in birds in detecting predators. The PP approach will adopt six nearest bird approach in detecting any predator. Their local and global bests are based on the individual detection as well as group detection. The PP algorithm was designed following MapReduce methodology that follows a Split Detection Convergence (SDC) approach.

***Keywords*—**Industrial control systems, prey predator, SCADA, SDC.

I. Introduction

SCADA systems have evolved from single, monolithic entities to the Internet of Things (IoT) [1]. SCADA is used in many different critical infrastructures, from nuclear management to utility, power, waste and engine management on ships and planes. Security of ICS is paramount as deviation from normal operation may result in putting lives at risk. The interconnection of these devices in a distributed environment through the Internet and other means exposes them to various attacks.

The possibility of malicious intent in such an ecosystem of interconnected devices is high. Managing and securing such an ecosystem can be daunting for security engineers and operators due to the dispersed nature of it. Bruce Schneier [2] pointed out that sometimes it seems as if the attackers have the upper hand due to the fact that the technological advancement is faster than security. This is true, as security personnel needs to study the new technology before developing new methods and approaches of securing it.

M. Okeke is a researcher at the University of South Wales, Member of Information Security Research Group. Department of Computing Engineering and Science (e-mail: michael.okeke1@ southwales.ac.uk).

A. J. Blyth is the Head of Information Security Research Group. Department of Computing Engineering and Science (e-mail: andrew.blyth@ southwales.ac.uk).

ICS generates enormous amount of data that makes it difficult for traditional IDS to analyze. Thus, the volume of data as well as the attack vectors is overwhelming the current detection mechanisms such as witnessed in Stuxnet attack in 2010 [3]. Big Data generators, such as ICS, require new technologies for anomaly detection as well as data processing and storage [4]. Hence, this study presented the use of PP approach seen in flocks of birds in securing ICS.

The rest of this paper is organized as follows: Section II presents the related work with regards to application of PP approach in IDS. Section III justifies the reason for adopting the PP approach while Section IV is the application of the approach. Section V is the introduction of ICSs and Hadoop framework. Section VI is the algorithm design approach by following MapReduce methodology.

II. Related Works

The application of PP approach in IDS is very new. Hence this paper will explore into some areas where the approach has been applied. The PP approach has not been applied in IDS for the protection of ICS. However, research into prey-predator approach has been explored over the years in other areas. Researchers on this have been researching on issues such as fishery population control as well as population dynamics [5]-[7]. The population dynamics in this regard refers to increase or decrease in population of a particular species as a result of certain conditions such as more predators might cause less prey and less prey might bring about death of predators as a result of hunger.

III. Reasons for PP Approach

The idea of using PP approach or defensive mechanism seen in some bird species such as starlings has not been really exploited in IDS. Starlings as preys have their ways of detecting single or multiple predatory attacks through their movements and actions. Their movements and actions are coordinated in such a way that they watch each other's action and this confuses the predator, which is seen as anti-predatory approach named "Confusion Effect" [8]. These birds look alike that the predator finds it difficult to pick on one in their mist and through the movement, the predator is confused, thus making it hard for the predator to catch one. Some hypotheses such as "Many-eyes hypotheses, Chorus line hypotheses" were introduced as a result of birds' collective behaviours [8]. Birds such as Starlings in the group do not have a leader but their behaviours are collective. This collective behavior can be observed in the way they flee the scene when predators are detected. Application of this detection approach in computer

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf

system could increase the chances of anomalies detection in this age of big data.

In a flock of thousands of birds, each bird is capable of detecting a predator. Hence, if one detects the predator, the collaboration and coordination are so perfect that the predator is left dancing in the air. The same approach can be employed in the detection of anomalies in a big data environment where detection is done in groups of six birds. This eliminates the centralised coordination as seen in the case of ant colony and artificial bee colony that has a queen as a central figure.

A. Ant Colony

Ants are well known for their collective search for food in their environment. These social insects are partially blind but they can collectively locate the shortest part to the food source through their pheromones trail. During their search for food, they wander randomly and any one that locates the source of food normally deposits pheromones. Other ants will follow the pheromone trail to the food source [9]. This idea has been used in solving some complex problems such as Travel-Salesman-Problem (TSP). The TSP is for connections finding and the shortest path for delivery of goods and vehicle routing [10]. It is evident from this information that adopting this approach has resolved some issues. Hence, the suitability of it in IDS for securing ICS with regards to distributed detections can be questionable compared to PP approach.

B. Application of Ant Colony Approach in IDS

Ant Colony has been applied in many optimisation problems such as TSP as mentioned in Section *A*. Hence, its application in IDS have started evolving as security experts are finding out that it can be used in searching out anomalies with or without data classifiers such as Support Vector Machine (SVM) and among others. Ant Colony Optimisation (ACO) was applied by [11] for detection perpetual echo attack. The ants monitor the User Datagram Packets (UDP) for detecting perpetual echo attack on port 7. This kind of attack allows the source and destination port echo at each other causing disruption in the whole network. These ants are meant to monitor the state of the system in order to detect such attack. The ants know the normal state of the system and when there is promptness from ants to move from one state to another, it arouses some kind of suspicion in the system of anomalies. The approach detected port scanning and echo attack. However, the detection rate was better compared to signature base detection based on their result.

Reference [12] implemented Multi-Agent IDS in ICS using ant colony clustering approach and unsupervised feature extraction. This approach was for detection and protection of the SCADA system by using different categories of ants for searching and detection through communication and collaboration with one another in the system. The application of Ant Colony Clustering Model (ACCM) and unsupervised feature extractions namely; Principle Component Analysis (PCA), Infomax Independent Component Analysis (Infomax ICA), Extended Infomax ICA and FastICA, reduced the clustering issues in the algorithm. The PCA and ICA are applied to remove the features that are not consistent with the defined parameters in order to maintain the clusters. They were applied mainly for the separation of the clusters based on their features. Training and testing ACCM as well as K-Means and E-M algorithms with the KDD-Cup 99 benchmark dataset showed that the Average Detection Rate (ADR) of the ACCM was 88.39 and the False Positive Rate (FPR) was 1.35 by the application of PCA. The ADR of the ACCM in combination of the three ICAs were not less than 90.50 while the FPRs were less 2.80 which outperformed the K-Means and E-M algorithms, although the margin were not too big (between 0.5-2). The Denial of Service (DOS) attack detection was 97.3 with ACCM, User to Remote (U2R) 30.7. However, the margins were not so big compared to K-Means and E-M algorithms, which were between (0.2-3).

C. Artificial Bee Colony

Artificial Bee Colony (ABC) is an optimisation algorithm that is based on the behaviours seen in some species of Bees such as honeybees during foraging for food. The algorithm was proposed by [13], which categorised the honeybee colony into three components namely; the employed foragers, food sources and the unemployed foragers. The food source is where the bees get their food to their nest. The employed bee foragers are the ones that currently located and working on a particular food source. They communicate to others about the food source through some particular movement such as waggle dance on the dance area. The unemployed bee foragers are the ones that are either waiting to be employed by searching the areas or by waiting in the nest for information from the employed with regard to the food source. The later one is called the onlookers while the former is called the scout. These collective behaviours of searching and locating food sources as well as communication among each other have been applied in IDS for securing computer systems as explained in Section *D*.

D. Application of ABC in IDS

ABC algorithm has been successfully applied in IDS by emulating their search, communication and collaborative abilities as seen in [14]. Their approach was a hybrid algorithm where a modified ABC algorithm will be integrated with Particle Swarm Optimisation (PSO) algorithm. This approach was to remove the shortcomings in both algorithms such as weak local and global search abilities. The ABC algorithm is weak in local search but very strong in global search while the PSO is the opposite. The two algorithms; Modified Artificial Bee Colony and Enhanced Particle Swarm Optimisation together were named MABC-EPSO. The two algorithms are working side by side and the main thing there is the communication between both in determining the best solution. The feature selection methods that were used are the Single Feature Selection Method (SFSM) and Random Feature Selection Method (RFSM). The SFSM is one dimensional feature vector where only one attribute is considered in every iteration for accuracy calculation using SVM. However, the RFSM approached the same issue randomly by evaluating all

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf

the features and deleted one feature as well as updating the dataset used. The approach outperformed other approaches such as SVM, ABC, J4.8 and among others. The margin for the Denial of Service using RFSM was 16.77. The detection rate for the MABC-EPSO was 99.81 while NB was 83.04 and J4.8 was 90.05.

IV. Application of Flock of Birds Approach

There are some characteristics and attributes that differentiate swarm or birds from other social insects and animals as mentioned in Section III. One of the main characteristics is their ways of communication in the swarm by following three simple rules namely; Separation, Orientation and Attraction as described in [15]. These three attributes will produce flocks of birds, which are the main attributes in modelling their behaviours such as coordinated movements used in [16] as "The chorus-line hypotheses". This was based on the experiments and observation of the avian flocks. They have a form of unified movement such as seen in cheerleaders; whether turning right or left. This is a distributed kind of action that will be suitable for big data challenges where multiple detections happen on multiple places following some principles or rules such as seen in birds.

Predators are mostly bigger in body max compared to prey as observed in [17] by experimenting with Falcon as the predator and seven different species of preys of different sizes. Preys always develop escaping strategies against its predator based on their previous experiences. On a straight line, the falcon will catch the preys but their only escape based on the observation is smaller turning gambit. However, there are characteristics that will determine the escaping strategy a bird will take such as the size, wings build up as well as the muscles of the birds. However, sometimes these birds are faced with more than one predator trying to catch them.

When bird preys face with multiple predators, their reactions are not much different from when face with a single predator as observed by [17]. The reason might be related to many eyes watching at the same time. They are attracted to each other and move in the same direction as well as avoiding collision with one another. However, escaping from predator is only possible if the predator is detected on time and the environment for escape is free.

A. Starlings (Sturnus vulgaris) Predator Detection

Starling applies their own experience based on the previous information gathered about the predator in order to detect them [18]. The detection is done mostly by observing the environment as well as others in the group based on topological range; the six to seven nearest neighbour for any unusual movement [19]. However, the experiments from [20] showed that previous encounter with predator's increases the preys scanning rate, which enhances predator detection. Hence, the experiment was with a single bird while this study is for bird in a flock. Some experiments carried out with starlings from [21] suggested that birds have different visual focus for different things such as eyes for food and eyes for detecting other things.

Based on the available information so far in this section, three important factors were mentioned in detecting predators such as;

1. The scanning rate or frequency
2. The observation of the environments and mates in the group
3. Previous experiences of the predator in their environment that will trigger watchfulness among the starlings.

These three factors determine the effectiveness of detecting a predator by flocks of starling birds. This can be seen under a different light as scanning frequency or scanning rate. The observation of the environment is done through scanning the environment or scanning in order to observe the nearest neighbour. However, the previous experience of predator attack will make the prey to be more vigilant by increasing the scanning frequency. Hence scanning frequency is seen as the most powerful factor in detecting predator by starling birds in the flock as well as lone bird [22], which can be represented as;

$$\text{Detection } P_{GD} = 1 - e^{-VTN} \tag{1}$$

P = probability; G = group; N = the size of the group (6-7); T = time; V = scanning frequency.

The probability of the group detection of predator is also dependent on the number of active scanning birds. The more the number, the less the angle of view and scanning

$$\text{V} = \frac{-ln(1-P_{GD})}{T} \cdot \frac{1}{N} \tag{2}$$

$$V = -ln(1 - (1 - e^{-VTN}))$$

$$V = \frac{-ln(e^{-VTN})}{TN}$$

Equation (2) shows the probability of 1 in a group detecting the predator based on the number of active scanning birds. The more the number of active scanning birds N, the more likely predators will be detected on time, the more protected they will be and less scanning duty for each birds. The more the number of birds N, the less their individual active scanning and angle of view.

Michael Delm in his work [22] further referenced the work of Abramson 1979 as well as the work of Elgar and Catterall 1981 with regards to detection ability based on group size. Their works and experiments showed high constant rate of birds in small groups detecting predator. Hence the probability of detecting predator is independent of group size, which is constant and high [22], therefore the detection model of the previous equation is modified as;

$$V = a. \ \frac{1}{N} \tag{3}$$

$$a = \frac{-\ln(1 - P_{GD})}{T}$$

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf

'a' is constant with regards to group size. The above equations have shown clearly that the detection is based on the scanning frequency. The more the number of birds in the flock, the less scanning for individual birds in the group. The question now is how do they communicate in the group as social animals? Their approach in responding to situation is mainly distributed based on their reaction and responses.

B. Interaction and Communication between Starlings

This study is particularly focused on European Starling (*Sturnus vulgaris*), the way they interact in the flock and as well as their positions. However, determining their structure or position of individual bird during flight might be difficult as they are constantly changing position during flight and foraging [23]. There are some factors that are important in determining the position of a bird during flight as well as their interaction. This will show how starling in a flock interacts with each other. The following are the factors to be considered (a) topological as well metric distance, the most advantageous (b) vision during flight (c) anisotropic and or isotropic factor.

C. Topological and Metric Rang

An experimental research in [24] showed the important of using topological range instead of the popular metric range. Their experiment shows that metric distance does not guarantee robust convergence after predator attack. Although the two approaches, both the topological and metric distance guarantee cohesion based on their observation, the question should be, under a strong predator attack like the one earlier mentioned, where three to five predators attacks the flock, how would you measure the resilient of the group cohesion? In order to answer this question, we take a look again at the demonstration of system robustness [24] using the mathematical approach bellow in 2D;

$$\vec{r}_{i(t+1)} = \vec{r}_{i(t)} + \vec{V}_{i(t+1)} \quad (4a)$$

$$\Theta_{i(t+1)} = \frac{[\Theta_i(t) + \Sigma_j \Theta_{j(t)}]}{N_i + 1} \quad (4b)$$

$\vec{r_i}$ = The position of ith bird in the group; $\vec{V_i}$ = The velocity of the ith bird in the group; Θ_i = The bearing or the direction of the ith bird in the group; N_i = Number of neighbours interacting with neighbour i.

In a topological range, a bird is only watchful of certain number of birds as they are moving, which is $N_i = n_c$. The number of birds in topological range is certain while in metrics is based on the distance or metric range r_c. Based on the analysis carried out in [24], as predator exert force or attacks the preys, the metrics range yielded scattered birds of 24% while topological was only 0.7% of scattered birds. The more scattered birds are as in the metrics range, the more they loose touch with others as a result of distance. However, topological range is based on watching and moving with a fixed number of neighbours. The result showed that there is a maximum probability of the birds in metric range breaking into 5 components after attack compared to 1 in topological range. Thus, in terms of resilience and stability of a system, topological range is preferred against metrics. As birds scatter, they expose themselves to predator, which makes it easy for a predator to target and catch a single bird than a group of birds. The predator approach always changes the direction of the movement, which goes away as the predator distance goes farther away from the preys. This shows that the heading or bearing Θ_i of the preys changes with every introduction or appearance of predator and stabilizes as the predator distance decays both in metrics ($1/r$) or topological range ($1/n$). The presence of predator as a force can be represented in (5):

$$F_0 \frac{[y_i \cos(\theta_i) - x_i \sin(\theta_i)]}{r_i^2} \quad (5)$$

D. Starling's (Sturnus vulgaris) Vision During Flight

The experiments in [21] showed that starlings *(Sturnus vulgaris)* have a blind rear axes as well as lateral visual axes. This explains why birds can only keep track of certain number of bird on both sides during foraging or flight. They can move their eyes together as well as independently without turning their heads [25]. They watch the movement of others within their vision field with both left and right eyes to see the direction of their movement and what they are doing [24]. However, their detection and interaction are not mainly vision focused; rather, it contributes to their survival. Focusing only on vision might be detrimental to the species since foraging and sleeping limits vision [26].

E. Anisotropic and Isotropic Factor

Based on the information in Section *D*, birds' eye structure is very important for their communication based on the experiments in [24]. The experiments showed that they could only interact with birds at some positions, mainly by their sides. The empirical studies carried out by [27] showed that anisotropic evidences in the angler distribution are as a result of interaction between birds in the flock. However, they pointed out that if the flocking conditions were non-interacting, the distribution would be isotropic. The idea was supported by [24]. This explained that the more birds are interacting together, they flock together and move together or their direction of turning as well as movement will be determined based on their interacting companions. However, in a situation where the birds are not interacting, movement can be in all direction (isotropic). Hence, Cavagna et al. have developed mathematical models that determine the anisotropy of birds in a larger group titled "Anisotropy Matrix" as seen below [27].

$$M_{\alpha,\beta}^{(n)} = \frac{1}{N} \sum_i^N v_i^\alpha v_i^\beta \quad (6)$$

M = The sum of many projector such as direction of the nearest *n*th neighbor I; v_i = The normalized distance vector of the *n*th nearest neighbor of bird *i*

In order to quantify the anisotropy in neighbors' distribution and see how it decays with the increase in density, some properties will be considered such as eigenvector and

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf

eigenvalue. The eigenvalues of M can be represented as $\lambda 1 < \lambda 2 < \lambda 3$ while the eigenvectors could be represented as W_1, W_2, W_3. In this instance, the eigenvector W_1 represents where the nearest neighbor is not likely to be found while W_3 represents where the nearest neighbor is likely to be found in the flock. However, the scalar value is less as well as anisotropy when the number of neighbors increases. Hence, the degree of anisotropy can be found based on the experiment in [27] by using the square scalar value such as $\gamma_1(n) = (W_1.V)^2$. This can only be calculated when the individuals are interacting in the flocks which is anisotropy but in the case of isotropy, the eigenvectors are statistically uncorrelated with the direction of motion V, since there is no previous known direction. This study will only consider the degree of anisotropy in determining the interaction between birds in groups n_c or their interaction range as it answers the question of resilience during predator attack on the flocks. Hence, isotropy will not be further evaluated at this time because it deals with uniformity in all direction (three dimensions $\gamma = 3\ \alpha$). Moreover, this study recognizes that in groups or flocks, there are birds at the boarder, which only have neighbors on one side, as well as birds in the front or back of the flock, which has neighbors only at the back, and in the front. The interaction can only be effective and complete when the neighbors are complete, in this case $n_c = 6$.

F. Positions of Individual Bird in the Group

The anisotropic distribution in starlings *(Sturnus vulgaris)* as modeled by [27] based on their fieldwork demonstrated that interaction in starling birds are anisotropic. The interaction among the birds in the flock may be during flight as well as external stimuli introduced to the flock during feeding or flight. The external stimuli here might be predator attack. Modeling this kind of movement from a single bird to the birds in the flock can be very challenging. It requires meticulous processes and resources for the data collection and analysis. However, [28] came up with some model titled maximum entropy model for modeling the behaviors such as individual direction of movement.

Maximum entropy is a way of predicting an event occurring based on the information or facts at hand by eliminating assumptions [29]. Modeling of starling birds using maximum entropy approach was used in [28] for modeling a single bird's behavior according to birds in the group. Hence, the correlation C_{ij} of individual bird in a flock considering their direction of motion can be modeled as;

$$P(\{\vec{s_i}\}) = \frac{1}{Z(\{J_{ij}\})} \exp\left[\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} J_{ij}\,\vec{s_i}.\ \vec{s_j}\right], \qquad (7)$$

$Z(\{J_{ij}\})$ = Normalization factor; $\vec{s_i}.\ \vec{s_j}$ = Normalized velocity of the bird i and j; J = Interaction Strength; C_{ij} = Correlation of individual birds; C_{int} = Correlation strength (Scalar Correlation); $\langle \vec{s_i}.\vec{s_j} \rangle$ = Average velocity or direction.

Since interactions among birds are topological, based on this model, birds only interact with certain number of birds, which according to our model is six, and or within a certain distance in terms or metrics. This group interaction could be expressed mathematically as;

$$P(\{\vec{s_i}\}) = \frac{1}{Z(\{J,n_c\})} \exp\left[\frac{1}{2}\sum_{i=1}^{N}\sum_{j\epsilon n_c^i}^{N} \vec{s_i}.\ \vec{s_j}\right], \qquad (8)$$

Equation (8) shows that $j\epsilon n_c^i$ means the bird j is an element of the group n_c of the neighbor i bird. This can be illustrated diagrammatically as seen in Fig. 1.

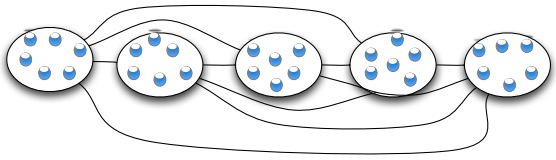


Fig. 1 Group of Interacting Birds

Fig. 1 shows group of six interacting birds, which illustrated what is in (8) as $j\epsilon n_c^i$. However, in a flock of birds, the groups can be hundreds and thousands based on the capacity. For starlings *(Sturnus vulgaris)*, they can be many in numbers, but free correlation movement and interactions between groups, as seen in Fig. 1, is maintained. This free correlation of movement is represented as;

$$C_{int} = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{n_c}\sum_{j\epsilon n_c^i}\langle \vec{s_i}.\vec{s_j}\rangle \approx \frac{1}{N}\sum_{i=1}^{N}\frac{1}{n_c}\sum_{j\epsilon n_c^i}\vec{s_i}\ .\vec{s_j} \qquad (9)$$

Birds are always in motion and modeling their position is very vital, they move from one group to another. Individual bird position is very important in locating the nearest neighbours or the group it belongs to. However, another vital important thing to consider here is the effect of birds at the boarder since their nearest neighbours are one sided either on the right or on the left based on their location. Since their neighbours might not be up to six, they are not considered.

G. Bringing It All Together

In the mathematical questions above, it was obvious that modelling birds' behaviours involves some properties. This paper might not require all the mathematical equations from (1) to (9), few will be useful for this study such as;

1. Detection equation in (1)-(3): One important thing to notice here is the scanning frequency of the birds. The bird's detection is based on scanning frequency or on the number of active scanning birds. A bird can either be scanning or eating (eating or scanning).
2. Flock of birds; the idea behind this paper is using the flocks of birds approach in detecting the predator. These birds move in thousands and even million in some aerodynamic forms and transfer information very fast within the flock. This is identified in the equation 9 as free correlation. Hence, (9) answers the question of information sharing within the flock.
3. Topological range and interactions; since interaction in birds is based on topological range and each bird only interacts with certain number of birds in the group; (7) and (8) answer the question.

4. Position of each bird in the group; this is dependent on the direction and velocity. Since the group of six is based on the topological range, individual birds' position in the group or the entire flock can be determined based on the topological range and direction as seen in (6). This was the reason for selecting anisotropy with eigenvector and eigenvalue since it is dependent on the direction.

Looking at the detection in (1), birds can only perform two actions, either scan or fly. The problem here would be to chose which group will scan first at the data entrance into the system. In order to resolve this issue, "Dinning Philosopher Problem" will be applied for example $(Dp_1, Dp_2, Dp_3, Dp_4, Dp_5, \ldots Dp_n)$. The initial philosopher (groups or group) will be chosen randomly based on the number of groups available. The groups are either enabled or disabled (i.e. scanning or flying). Groups that are not scanning are disabled to allow for efficient computer resources such as processing power. The initial enabled group will be set at ¾ of p_n. As more data are coming in, more groups will be enabled as well as when the data are not coming in, more groups will be disabled. Each iteration will create a movement and as each group has six birds, they will move to next position. Individuals in a group are selected randomly as seen in Fig. 2 (a) and their angle of view as seen in Fig. 2 (b).

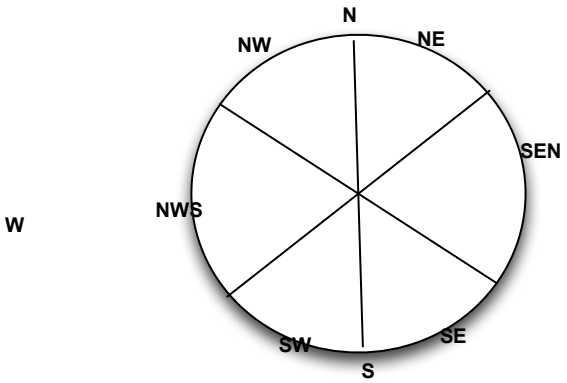


Fig. 2 (a) Position of Birds in the Group of Six

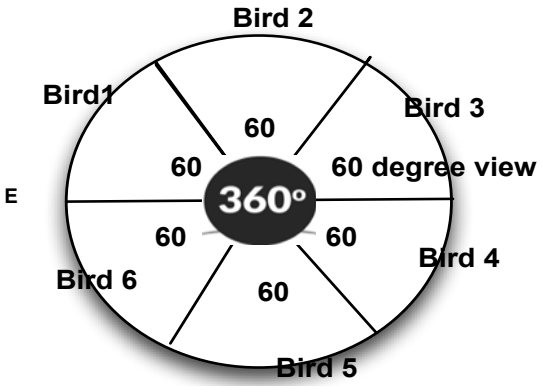


Fig. 2 (b) Birds Angle of View

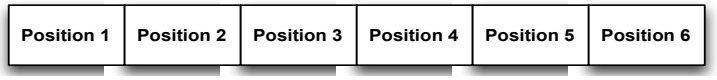


Fig. 2 (c) Positions as an Array

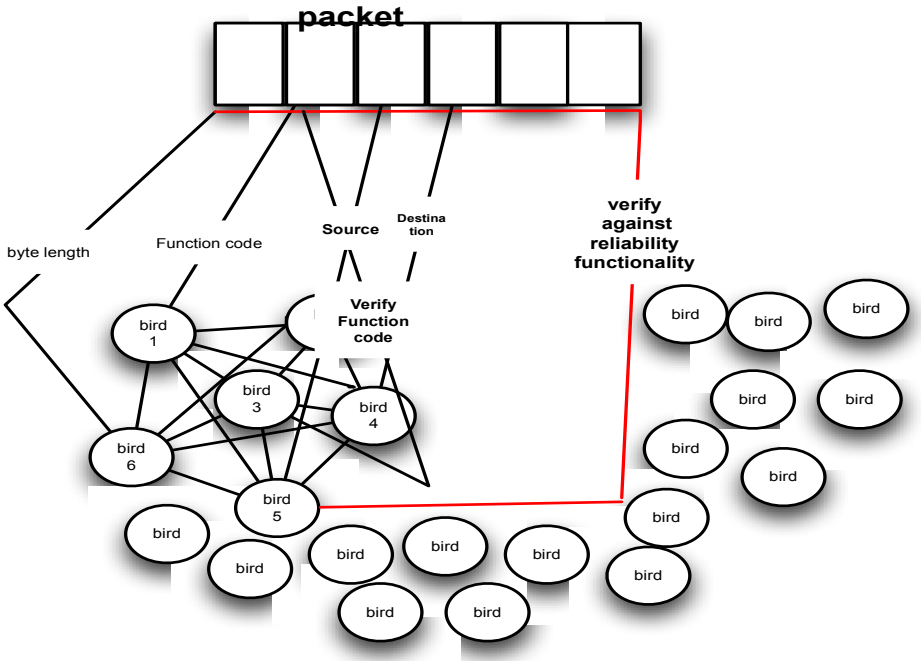


Fig. 2 (d) Analysis of Packets Based on Position

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf

Birds are chosen randomly in the group and the one that is chosen will be in position 1 while the numbering will be clockwise. Bird P (n) = {NE, SEN, SE, SW, NWS, NW} if n = SE, n+1 which is SW, n++. NE represents the North East, SEN represents the South East North, SE represents the South East, SW represents the South West, NWS represents the North West South and the NW represents the North West. This can also be determined by their angle of view as seen in Fig 2 (b). 90 degrees SE clockwise will point to the location S in the environment. As their position is determined, their functions can be represented as an array as seen in Fig. 2 (c) based on their numbers. Fig. 2 (d) represents the packet and the birds approach based on their position for the analysis.

V. Industrial Control Systems

ICS is a general term used to describe the control or monitoring systems used in controlling and monitoring production and resource in order to ensure reliability, functionality as well as security. Some of available ICS are SCADA and Distributed Control System (DCS). This study will focus on SCADA system as it is widely used nowadays in almost everywhere.

A. SCADA

The age of technological revolution has seen increase in the way things are being done and controlled; from nuclear system to aerospace management, from locomotives to utility and water managements, from engine management on ships to internet of a thing such as social media managements. The complexity in managing such an ecosystem in technological environment can be very demanding for engineers with regards to technological and operational standpoint. The idea of SCADA system for the control and monitoring such ecosystem ameliorated the difficulties in management of industrial system. Such industrial system can be seen nowadays, as mentioned above but not limited to; aviation, astronomical environment, agriculture, atmospheric monitoring, building management, consumer product and entertainment, military environment, nuclear environment monitoring and among others [30]. The idea and technology behind SCADA has been in existence for over 30 years, [31]. SCADA systems mostly comprise of software's and hardware's designed for monitoring and controlling systems for efficiency and reliability measures. The sensors are placed on the remote sites that report the conditions of the sites through remote system. SCADA system has its own way of communication and transportation of information. There are a few communication protocols used in SCADA system depending on the organization. Some organization has their custom made protocol, while some use open protocol such as Modbus, DPN3, IEC 60870-5 -101/-103/104 among others. The various subsystem of SCADA will be explained further in the SCADA Section V; ICS.

B. Hadoop Framework

The major components of Hadoop framework are the MapReduce and the Hadoop Distributed File System (HDFS). The MapReduce is for the processing of the data using key value pair while HDFS is for data storage. There are distinctive characteristics that distinguish Hadoop from a database and other frameworks that use distributed systems such SETI@home which are; robustness, scalability, simple and accessibility. The robustness of Hadoop can be seen in the way failures are been handled, due to the fact that it runs on commodity hardware and failures are being anticipated and managed. Hadoop is scalable based on its architecture, it scales linearly and can handle bigger amount of data faster by simply adding more nodes. The simplicity of Hadoop made it easy to write your own code and integrate it to the framework, which is evident in the amount of applications that can be integrated on it, such as but not limited to Hbase, Zookeeper, Apache Flume, and Pig. Hadoop framework can be accessible everywhere if it is integrated into the cloud environment [32].

VI. Designing the Algorithm Using MapReduce Methodology

The approach that will be used in designing the algorithm is called Split Detection and Convergence (SDC) approach as seen in Fig. 3. Data are split into six categories based on six nearest birds approach. Each bird among the six has something to check in the packet or to verify the results of the other birds in the same group. However, each bird acts autonomously and exhibits six characteristics such as checking the byte length, function code as well as verification and among others, but can only do one thing at a time.



Fig. 3 Algorithm Approach

The activities of the birds depend on their position at the time of packet entry as the approach is based on topological range rather than metrics; therefore, it is based on the number of interacting birds rather than distance. The split idea here is the separation approach used in modeling flocks of birds. Hence, the separation serves as a mechanism used by the flocks in distancing themselves from each other in order to avoid collision. Convergence on the other hand will bring the data together after the detection process has been carried out. Detection involves making the final decision that the packet is right or not based on the set parameters.

Fig. 4 depicts the architecture of the algorithm and explains the three process of SDC adopting MapReduce methodology. This methodology has been successfully applied by [33] for IDS. Therefore, the approach, as seen on Fig. 4, is the six nearest birds checking the packet for anomaly detection by initially splitting the packet. The six birds will be selected based on the topological range as seen on Fig. 1. The behaviors of this swarm of birds are concurrent in their environment as many of them are carrying out the same tasks of checking and analyzing packets at the same time. Thus, as packets are coming more birds are taking up activities and

reporting the outcome of the analysis. The Reducer in Fig. 4 represents the detection, where all the information from the split will be gathered for the final decision, which is the detection. It is obvious based on the information above that the increase in the number of birds reduces the number of scanning frequencies. The increase in the number of birds will enhance the detection and faster processing as more groups of six birds will be formed as seen in Fig. 1.

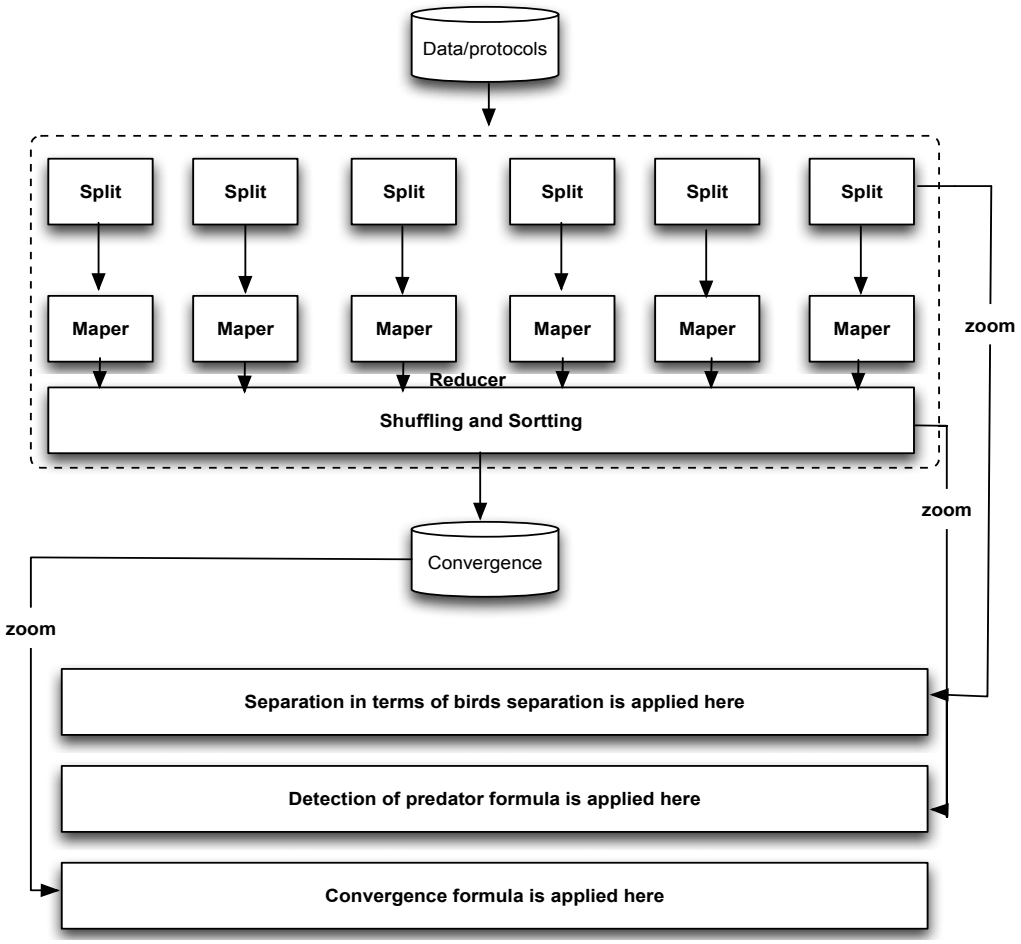


Fig. 4 MapReduce Methodology Architecture of PP Approach

Each bird is represented as a particle based on Particle Swarm Optimization (PSO) theory in modeling flocks of birds. The diagram in Fig. 1 represents five groups of local birds with each group containing six individual birds. As packets are flowing in to the system, each group will handle one packet based on the six interacting neighbors. Since each group contains six birds, the analysis of each packet is carried out in six parts as shown in Fig. 2 (d) such as verifying function code, checking protocol header. Packets are split for analysis and detection of anomalies and brought back together or reassembled together for storage. However, the fitness is determined by finding the local best as well as the global best. Fig. 1 shows that the particles (bird) are in groups and each particle in a group has a Time To Live (TTL). Among the particles in a group, one has an infinite TTL. Particles die based on their TTL if there is no packet for it to analyze within limit of its time to live. Thus, the local best here is based on the detection of malicious activities in a packet. The detection of anomaly by a particle will increase its TTL by 100%, which will be as a reward to the one that detected the anomaly in a packet and raised alarm for other groups. Others in the same group will update their time to live based on the new local best. The global best will be based on the detection within two groups. Comparison between the first two local best will form their global best. Both detection and increase in TTL is a form of raising an alarm in a system and others are attracted and alerted by increasing their TTL as well. There is a communication among the groups and within each group. This communication is shown in Fig 1 as a loop or correlation between birds in the local group as well as in the whole flock. The bird with the infinite time to live in each group has the possibility of spawning more birds. This can be represented in steps shown next:

1. Initialize all the possible positions and particles (birds) with randomly chosen positions and velocity.
2. Calculate the fitness value of each particle in the group (time to live in millisecond or nanosecond)

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf

3. If the time to live of the particle *i* runs out terminate *i* else continue i
4. If particle *i* in the group detect anomaly, Time To Live x = xx
5. XX = the local best
6. The local best from two groups compared = global best
7. Else if no anomaly & no packet & Time To Live runs out terminate
8. If 5 of the *i* in the group are terminated, the remaining $i = \infty i$
9. If more packets are flowing in, each ∞i spawn ~ 200 more *i* .

Fig 5 explains the general algorithm flowchart. It started with the free scale correlation in the flock that allows information to pass on to all the groups. This is the group of six birds based on topological range.

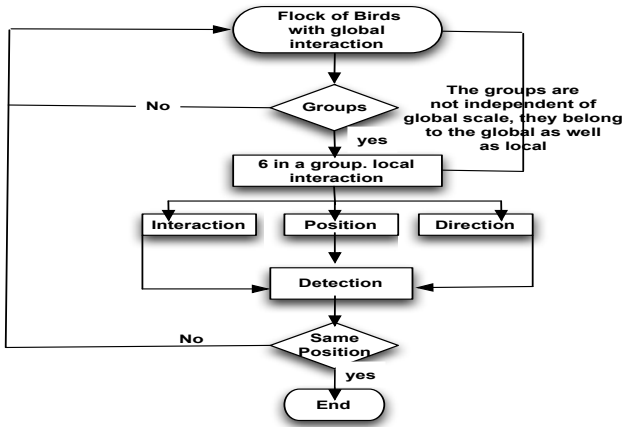


Fig. 5 Flowchart of the Algorithm Approach

The three important factors in determining the groups are their position, direction of motion and interaction as seen in (7) and (8). With the six interacting birds, detection is done simultaneously. However, birds move and changes position, therefore position is very important in determining the interacting bird. Fig. 6 explains the detection approach.

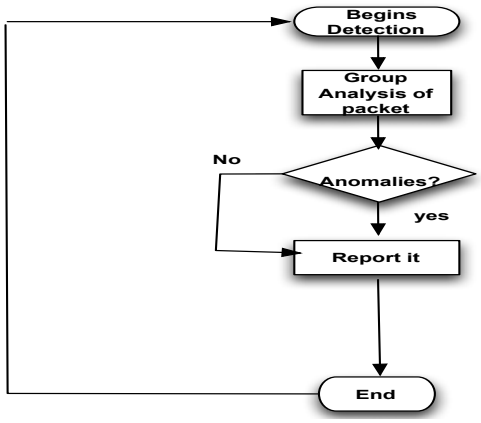


Fig. 6 Detection Approach

VII. Conclusions

This study presents the idea of using PP approach found in flocks of Starlings birds in securing ICS. Due to the time we are living, the speed at which technological development is moving has posed many security challenges such as Big Data, Cyber attack, Integration of SCADA online, IoT and many more. Researchers and industries are engaged in minimizing these issues by deeply finding new detection mechanisms for such advanced cyber attacks and data management. However, the current and future research for IDS are looking into using some idea inspired by biological means such as social insects, fish, birds and others. Current researches are focused on the way these animals solve complex problems and reaching their goals such as food foraging and predator detection by flocks of birds. These behaviors can be modeled in addressing these issues. Approach of [12] was used the ACCM in protecting ICS. However, PP approach in birds have not been explored in IDS and it has a very good potentials in tackling the current issues faced in ICS,

SCADA systems have evolved from single monolithic entity to IoT; therefore, many issues are manifesting such as buffer overflow and many other advanced cyber attacks. According [34], 245 known attacks were recorded from September 2014 to February 2015 in USA and this signifies the increase in the attack. The attack on the Iranian plant was a wake up call to protect process control systems. Hence, any deviation from the normal operation will put life at risk and the cost can be very high.

The main objectives of this study are to show that PP approach can applied in intrusion detection for securing ICS. The background research as well as literature review reveals the viability of applying this approach in securing ICS. However, the approach was further incorporated into Hadoop framework by using MapReduce methodology in achieving the detection of anomalies using SCD approach.

Acknowledgment

This is an on going research that is supported with the grant from Thales Group in corroboration with the University of South Wales United Kingdom.

References

[1] R. McClanahan, "The Benefit of Networked SCADA Systems Utilizing IP-Enabled Networks". Arkansas, USA, 2002.
[2] B. Schneier, "Liars and outliers: Enabling the Trust That Society Needs To Thrive": Technological Advances, USA, John Wiley and Sons, 2012.
[3] R. Langner, "Stuxnet: Dissecting Cyberwarfare Weapon" *IEEE Security & Privacy*, Vol.9 (3), PP. 49-51, 2011.
[4] Sungard, "Big Data Challenges and Opportunities for the Energy Industry" 2015.
[5] K. Chakraborty, S. Jana, and T. Kar, "Global Dynamics and Bifurcation in a Stage Structured Prey-Predator Fishery Model With Harvesting": *Applied mathematics and Computation*, Vol.218 (18), 2012, PP. 9271-9290.
[6] K. Chakraborty, and T. Kar, "Effort Dynamics in a Prey-Predator Model with Harvesting": *International Journal of Information Systems Science*, Vol 6 (3), 2010, PP.318-332
[7] C. Chen, and C. Hsui, "Fishery Policy Considering the Future Opportunity of Harvesting": *Mathematical Bioscience*, vol. 207, 2007, PP. 138-160

[8] F. Zoratto, D. Santucci, and E, Alleva, "Theories Commonly Adopted to Explain The Anti-Predatory Benefits of the Group Life": The Case of Starling *(Sturnus Vulgaries*). *Rendiconti Lincei*, 2009, PP.1-14.

[9] C. Lenzen, and T. Radeva, "The Power of Pheromones in Ant Foragin", *1st Workshop on Biological Distributed Algorithm* (BDA), 2013

[10] M. Derigo, and T. Stutzle, "Ant Colony Optimization. *The MIT Press*", 2004.

[11] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, A. Ingle, and V. Ambhore, "Intelligent Perpetual Echo Attack Detection on User Datagram Protocol Port 7 Using Ant Colony Optimization". In *Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on*, 2014, pp. 419-424. IEEE.

[12] C. Tsang, and S. kwong, 'Multi-Agent Intrusion Setection System in Industrial Network using Ant Colony Clustering Approach and Unsupervised Feature Extraction'. *In IEEE International Conference on Industrial Technology*, ICIT, 2005, pp.51-56.

[13] D. Karaboga, "An Idea Based On Honey Bee Swarm for Numerical Optimization", T*echnical report-TR06*, Erciyes University, Faculty of Computing and Engineering, 2005.

[14] P. Amudha, S. Karthik, and Sivakumari "A Hybrid Swarm Intelligence Algorithm for Intrusion Detection Using Significant Features", *Scientific World Journal*, vol. 2015, 2015, PP.1-16.

[15] I. Couzin, J. Krause, R. James, G. Ruxton, and N. Franks, "Collective Memory and Spatial Sorting in Animal Froups", 2002.

[16] W. Potts, "The chorus-line hypotheses of manoeuvre coordination in a avaian flocks": *Nature 309*, 1984, pp. 344-345.

[17] A. Rosen, and M. Hedenstrom, "Predator Vesus Prey: On Aerial Hunting and Escape Strategies in Birds", *Oxford Journals, Behavioural Ecology*, Vol. 12 (2), 2000, PP. 150-156.

[18] G. Powell, "Experimental Analysis of Social value of Flocking by Starlings (*Sturnus Vulgaris*) in Relation to Predation and Foraging", *Amin Behav* , 1974, 22:501-505.

[19] E. Fernandez-Juricic, S. Siller and A. Kacelnik "Flock Density, Social Foraging and Scanning" *An Experiment With Starlings. Behav Ecol* 15, 2004, PP. 371-379.

[20] E. Glueck "An Experimental Study of Feeding, Vigilance and Predator Avoidance in a Single Bird". *Oecologia*, 1987, PP. 268-272.

[21] G. Martins, "The Eye of a Passeriform Bird, The European Starling Eye Movement Amplitude, Visual Fields and Schematics" Optics, J Comp Physiol A, 1986, PP. 545-557

[22] M. Delm, Vigilance for Predators: detection and Dilution Effects. *Behavioural Ecology and Sociobiology*, 1990, p. 337-342.

[23] H. Pomeroy, and F. Heppner, "Structure of Turning in Airborne Rock Dove (*Columba Livia)* Flocks", *The Auk* 109 (2) 1992, PP.256-267.

[24] M. Ballerini, N. Calbibbo, R. Candeleir, A. Cavagna, E. Cisbani, I. Giardina, V. Lecomte, A. Orlandi, G. Parisi, A. Procaccini, M. Viale, and V. Zdravkovic. "Interaction ruling animal collective behavior depends on topological rather than metric distance: Evidence from a field study". *Proceedings of the National Academy of Sciences of the United States of America* 105: 2008, 1232–1237.

[25] E. Lawlor, "Discover Nature Close to Home: Things to Know and Things to do". *STACKPOLE BOOKS*, Harrisburg, 1993, PP.61.

[26] C. Devereux, M. Whittingham, E. Fernandez-Juricic, and J. Vickery, "Predator Detection and Avoidance by Starlings Under Differing Scenarios of Predation Risk": *Behaviour Ecology*, 2005, PP. 303-309.

[27] A. Cavagna, A. Cimarelli, I. Giardina, G. Parisi, R. Santagati, F. Stefanini, and R. Tavarone, "From Emperical Data to Inter-Individual Interactions": Unveiling the Rules of Collective Animal Behavior: *Mathematical Models and Methods in Applied Science*, Vol.20, 2010, PP.1491-1510.

[28] W. Bialek, et al "Statistical Mechanics for Natural Flocks of Birds, In Proceedings of the National Academy of Science of the United State of America", *PNAS*, Vol. 109 (13) 2012, PP. 4786-4791.

[29] A. Ratnaparkhi, "A Simple Introduction to Maximum Entropy Models for Natural language Processing": *Institute for Research in Cognitive Science*, 1997.

[30] E. Babovic and J. Velagic "Lowering SCADA development and implementation costs using PtP concept", *Information, Communication and Automation Technologies, 2009. ICAT 2009. XXII International Symposium on* 29-31 oct.2009. PP.1-7, Bosnia.

[31] S. Boyer "Scada: Supervisory Control And Data Acquisition" *4th Edition, International Society of Automation*, 2009, USA

[32] C. Lam, "Hadoop in Action" *Manning publishing*, 2011, Stanford, United State

[33] I. Aljarah, and S. Ludwig, "MapReduce Intrusion Detection System based on a Particle Swarm Optimisation Clustering Algorithm", *In proceeding of 2013 IEEE Congress on Evolutionary Computation*, 2013, PP. 955-962, Cacun Mexico

[34] ICS-CERT, "Incident Response/Vulnerability Coordination in 2014" 2015.

Open Science Index, Industrial and Manufacturing Engineering Vol:10, No:5, 2016 publications.waset.org/10004822/pdf