Study on Agents Based Meta-Heuristic Approach for Cyber Security Defense Mechanism

Suruchi Sinha*
Shukun Tokas**

Abstract

Oxford defines cyber security as 'the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this'. Authors' attempts here to describe an agent based meta heuristic approach to infrastructure cyber defense mechanism where a team of human and software ants mitigate security threat posed in the cyber world. The DigitalAnts™ system architecture will wander through entire network in identifying the invaders i.e. viruses, trojan horses etc which are said to create a potential threat to our systems. Paper discusses a theoretical version of this concept.

Keywords: Agents, DigitalAnts™, Digital Pheromone, Security

Introduction

Background

The era of Internet started in 1990's, its craze shoots in the veins of every part of the globe. As science is said to be creator as well as a destroyer, a strong protection mechanism building requirement came in when the approach started developed in a wrong means.

Cyber Security (CS) is prime area of concern where the scientist are hooked to develop a new approach to avoid cyber crimes such as stealing information, hacking system, cracking passwords etc. [1]

A time the strong cryptography technique turns into failure.

Motivation

Nature is a powerful paradigm. The real time observation in natural happenings has led to solve acutest problem such as space-time optimization. As perceived, Cyber Security is again a challenging area. Research Scientist and Professors of Pacific Northwest National Laboratory studied the theory of natural ants by Marco Dorigo. As said by Prof Erin W Fulp, Wake Forest University, Computer Science Department, NC, USA that the ants are the biggest invaders to their threat, the same concept can be linked and implemented in the Cyber World.

Related Concepts

The section discusses the application field and variety of techniques under the scope of this field.

Cyber Security

Cyber security is basically collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. [2] Cyber Security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets

Suruchi Sinha*
IINTM, GGSIPU
Shukun Tokas**
IINTM, GGSIPU

against relevant security risks in the cyber environment. The general security objectives comprise the following:

- *Availability*
- *Integrity, which may include authenticity and non-repudiation*
- *Confidentiality*

Swarm Intelligence

Over the past two decades meta-heuristic techniques have been the area of research of keen interest by scientist, academicians and engineers. Heuristic algorithms typically intend to find a good solution to an optimization problem by 'trail and error' in an adequate amount of time.

There are two important components in modern met heuristics i.e. Intensification and Diversification. For an algorithm to be successful it must able to generate diverse range of optimal solution and intensify its search around neighborhood of an optimal solution.

Some Popular Meta-Heuristic are following:

Ant Colony Algorithm

Ants are the social insects that work in groups to find food. The Ant Colony Optimization (ACO) algorithm studies the behavior of ants and makes use of their self organizing principles with highly coordinated behavior that helps in solving complex problems. Ants travel from their nests in search of food (action) and return to their nests in minimum possible time by travelling the minimum distance (goal) The ants while on their route leave a chemical substance known as *pheromone*. This chemical has a property of evaporating. Ants despite being blind, they follow each other with the help of pheromone trail. So, the duality of action and goal projects a rational decision making process. [3]

Bio Geography Based Optimization

Nature of biological species, to migrate to a place, which suits their interest more, is commonly seen. This behavioral activity of theirs, has deduced an optimization technique called the Biogeography Based Optimization. Geographical areas that are well suited as residences for biological species are said to have a high habitat suitability index (HSI) Majorly, the conditions that are the deciding factor for the HSI value includes, rainfall, diversity of vegetation and diversity of topographic features, land area and temperature. Habitats with a high HSI tend to have a large number of species, while those with a low HSI have a small number of species. [3]

Firefly Algorithm

It was developed by Xin-She Yang 2007, which is actually idealization of the flashing characterization of fireflies. There are three components in firefly algorithm.

a) The firefly will attract to brighter firefly and at the same time they will move randomly.

b) The attractiveness is proportional to the brightness of flashing light which will decrease with the distance.

c) The decrease of light intensity is controlled by light absorption.

Harmony Search Algorithm

Harmony Search Algorithm was first developed by Zong Woo Geem et al. in 2001. It is a jazz music based meta heuristic algorithm which was inspired by an observation that aims to find the perfect state of harmony. A musician always tends to plays a music which has a perfect harmony (accurate frequency matching amplitude band width and pitch). [4]

Prototype Development

Every computer attack is a battle between the owners of a computational infrastructure and adversaries bent on using these resources for their own purposes. To address this challenge, the Pacific Northwest National Laboratory (PNNL) has developed a

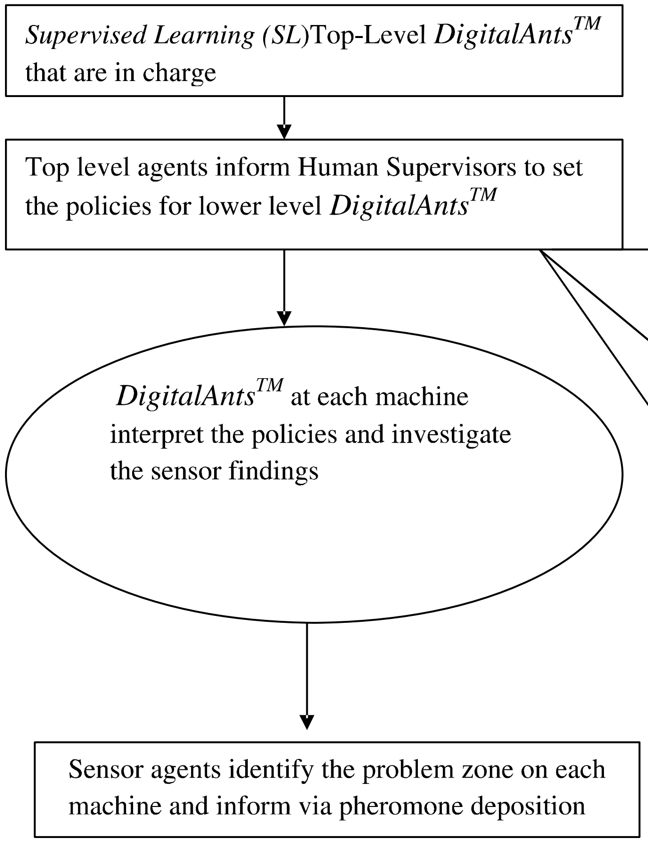
Supervised Learning (SL)Top-Level DigitalAnts^{TM} that are in charge
Top level agents inform Human Supervisors to set the policies for lower level DigitalAnts^{TM}
Machine 1
DigitalAnts^{TM} at each machine interpret the policies and investigate the sensor findings
Machine 2
Machine 3…n
Sensor agents identify the problem zone on each machine and inform via pheromone deposition

Fig. 1: Framework for Ant Colony developed on N number machines on Network

framework for decentralized coordination based on the eusocial behaviors seen in ant colonies. The eusocial organization in the ant colony provides a highly adaptive common *Cooperative Infrastructure Defense (CID)* that achieves emergent behavior via stygmergic communication.

As discussed in the Fig1 given bellow, we have applied these ant behaviors to cyber security in our Ant-Based Cyber *Cooperative Infrastructure Defense* where humans and various software agents share the responsibilities of securing an infrastructure comprised of enclaves that belong to member organizations. Supervised learning is the machine learning task of inferring a function from labeled training data. The training data consist of a set of *training examples*. In supervised learning, each example is a *pair* consisting of an input object (typically a vector) and a desired output value (also called the *supervisory signal*). [5]

Following are the barriers in proposed methodology:

- Cyber security solutions must not introduce latency issues.
- Cyber security solutions must accommodate the often limited computing resources of legacy control systems.

Conclusion

The Theory discussed above shows that our framework of Network System Control using hierarchy of agents and capabilities of Meta Heuristic Approaches (Swarm Intelligence) has greatly enhanced the security of key, critical, interconnected infrastructures.

Additionally, system supports for following:

a) Simulating a framework suitable for a typical topology based multi organizational cyber security.

b) A feedback system can be generated by back tracking the pheromone deposition of digital DigitalAnts™. It can be further pass on to the system for reducing the attacking capabilities.

Futuristic Research

Authors have discussed a typical framework of mapping the Swarm Based Technology in Cyber security field. An effort can be made by extending this work to a complete Distributed Network Level. The Next step would be deployment of the functionality of system using various others Computational Based Optimization Algorithm such as Harmony Search Algorithm, Biogeography Based Optimization, Pigeon Algorithm many others.

A comparative study of entire research built on Cyber Security can give us a fundamental theory of impact factor of Meta Heuristic Approach in Cyber Security.

Acknowledgement

Authors are really thankful to Dr. V.K. Panchal, Senior Scientist, Director, DRDO, New Delhi who shared their powerful wisdom on Swarm Based Meta Heurisitc Techniques which allowed us to implement it on typical areas like Cyber Security. The entire literature review discussed is based on the experiment conducted and published by Research Scientists of Pacific Northwest National Laboratory, WA USA and Prof Erin W Fulp, Wake Forest University, Computer Science Department, NC, USA. Authors are thankful to them for coining this concept and helping other researchers to investigate more in this field. We are also thankful to our colleagues and student scholars who are working together as team in relating concepts.

References

1. D. Frincke, A. Wespi, and D. Zamboni, “From intrusion detection to self-protection,” Computer Networks, vol. 51, 2007, pp. 1233–1238.
2. E.A.R. Dahiyat, “Intelligent agents and intentionality: Should we begin to think outside the box?” Computer Law Security Rep., vol. 22, 2006, pp. 472–480.
3. F. Bellifemine, G. Caire, D. Greenwood, Developing Multi-Agent Systems with JADE, Wiley & Assoc, 2007.
4. J. Haack., G. Fink, E. Fulp, and W. Maiden, “Cooperative Infrastructure Defense,” presented at the Workshop on Visualization for Computer Security (VizSec), 2008,
5. M.B. Scher, “On doing ‘being reasonable login”, vol. 31, 2006, pp. 40–47.