A Survey for Big Data Computings of Anomaly Detections in the Military

Nikom Koprach, Wichai Pawgasame
Data Communication Division
Defence Technology Institute
Pakkret, Nonthaburi, Thailand
nikom.k@dti.or.th

***Abstract*—Anomaly Detection is a tool that detects anomalies in a big data. Anomaly detection acts as frontline of defense for security demanded system. Early detection of anomaly data pattern can prevent severe damages from taking place. Anomaly detection has found many potentials in Military Operations, where protection against anomaly behaviors is the first priority. Most of the data that anomaly detections are dealing with are big data, which has large volume, large variety, high velocity, and high veracity. Processing such big data requires huge amount of computing resources. This is infeasible with a single processing unit. This article explores the characteristics and applications of anomaly detections in military. In addition, the big data computing technologies are also presented as potential solutions to anomaly detections .**

***Index Terms*—Anomaly Detections, Big Data Computings, Parallel Computing, Distributed Computings**

I. Introduction

Protection against threats is the military's first priority to defend the nation. Threats can be in many forms. There can be threats in citizen life, society, economy, or classified information. Some threats may be easier to identified, while many of the threats are difficult to be identified. For example, a secondary radar system interrogates all aircrafts flying over the country's air space. The enemy aircraft with transponder can be identified by its response. In contrast, an aircraft without transponder or broken transponder cannot be certainly identified as a threat. A stealth aircraft may avoid being detected by a radar system. In social and economy perspective, a person who robs a bank is certainly a threat. However, if there is a suspicious transaction over a customer's bank account, it is not obvious whether this transaction is a threat or just a mistake by a bank or a system. Threats may be difficult to detected and identified in some situations. Hence, threat detection and identification are challenging. By the glimpse of data analyst, threats are abnormal activities that may cause inferior consequences. A word "anomaly" or "outliner" may referred to a threat, in which they means an activity that is outside the scope of normal activities.

To prevent an anomaly from causing undesired consequences, we must suppress its actions. However, an anomaly must be detected and identified before we can take action to suppress it. The tasks of anomaly detection become very challenging nowadays, because we are moving towards the world of unlimited information. Information is the basis of our everyday life. Anomalies exist in information. Their existences may be obvious or obscure, but there would be some patterns indicating their existence. The ultimate goal of anomaly detection is to capture the patterns of anomalies, which is more difficult as information is growing in volume, variety, velocity and veracity. In other words, anomaly detection are tended to be applied on the big data. Such process requires immense computing power and storages.

This article explores the characteristics of anomaly detections in military, as they are applied extensively in defense application. The big data computing technologies and their applications to anomaly detections are also explored. This article is organized as follows. Section II gives the brief description of anomaly detection and its application in military. Section III presents the current big data computing technologies. Section IV explores the research in data computings for anomaly detections. Finally Section V concludes the study.

II. Anomaly Detection

Anomalies are patterns in data that do not conform to the normal pattern of data [1]. Anomaly may be referred to as outliners or noises in some literatures [2]. Malicious activities such as fraudulent behaviors, intrusions and unexpected activities can induce anomalies in the data. Some anomalies may be induced by system faults, human errors or natural deviations. It is critical that anomalies are detected and identified before they can cause disastrous consequences. Anomaly detection is related to anomaly suppression, however anomaly detection is the front line of defense method that will detect and identify anomalies before they are suppressed.

A. Applications in Military

Anomaly detection is applicable in a variety of applications, especially in safety critical system [2]. As anomaly detection could detect anomalies in the system, it would prevent the system from being in catastrophic state. In military, safety of a country's secrets and its citizens is the first priority. Hence, anomaly detection is very crucial in military. Some of anomaly detection applications are discussed as follows:

1) Detecting anomalies in communication: Anomalies can refer to noises in radio communication. Noises are unwanted signals that tend to disturb the transmission and processing of signals in radio communication [3]. The source of noises