Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 114 (2017) 132–138

Procedia Computer Science

www.elsevier.com/locate/procedia

Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems, CAS
October 30 – November 1, 2017, Chicago, Illinois, USA

An Outlier-Based Intention Detection for Discovering Terrorist Strategies

Salih Tutun[a,*], Murat Akça[b], Ömer Bıyıklı[b], Mohammad T. Khasawneh[a]

[a]*Department of Systems Science and Industrial Engineering, Binghamton University, New York, 13850, USA*
[b]*Department of Industrial Engineering, Gazi University, Ankara, 06420, Turkey*

Abstract

Terrorist groups (attackers) always strive to outmaneuver counter-terrorism agencies with different tactics and strategies for making successful attacks. Therefore, understanding unexpected attacks (outliers) is becoming more and more important. Studying such attacks will help identify the strategies from past events that will be most dangerous when counter-terrorism agencies are not ready for protection interventions. In this paper, we propose a new approach that defines terrorism outliers in the current location by using non-similarities among attacks to identify unexpected interactions. The approach is used to determine possible outliers in future attacks by analyzing the relationships among past events. In this approach, we calculate the relationship between selected features based on a proposed similarity measure that uses both categorical and numerical features of terrorism activities. Therefore, extracting relations are used to build the terrorism network for finding outliers. Experimental results showed that the comparison of actual events and the detected patterns match with more than 90% accuracy for many future strategies. Based on the properties of the outliers, counter-terrorism agencies can prevent a future bombing attack on strategic locations.

Keywords: Outlier Detection; Similarity Function; Link Formation; Network Analysis; Counter-terrorism

* Corresponding author.
E-mail address: stutun1@binghamton.edu

1. Introduction

Terrorism is a new kind of war that is increasingly characterized with uncertainty. In this war, terrorist groups (attackers) often change their strategies in an effort to surprise and shock defenders (counter-terrorism agencies) for more successful attacks. Defenders are always under pressure to learn new strategies in order to have a strong counter-terrorism strategy [1]. Moreover, terrorism has significantly increased after the September 11 attack because the uncertainties associated with such events make their prevention a very complex effort to manage [2]. Defenders need to know how to create strategies to prevent this kind of attacks, and they need to adopt more accurate approaches to investigate terrorist activities [3]. Intelligence gathering is the cornerstone through which uncertainty is reduced.

Current literature suggests that terrorism has an evolutionary nature and attackers change their behavior according to defenders' counter-terrorism policies. The behavior of attackers evolves over time, and they often copy the behavior of other attacks [4]. For instance, each attacker learns tactics from past attacks whether they were successful or not. After learning certain tactics, they seek to shock defenders through attacks that are unexpected when compared with past events. Only when defenders have the ability to predict unexpected future events is the prevention of terrorism plausible.

In the literature for understanding strategies of terrorism, network-based approaches are used to understand complex interactions [5, 6]. These approaches are becoming increasingly popular [7] because they are proving to be effective methods for understanding terrorism [8]. Moreover, many researchers have studied the behavior of people (attackers) to find the leader of attackers (with their leader). Therefore, existing network-based approaches in the literature focused on prosecution instead of prevention [9, 10]. In this research, we focus on the finding relationships between different attacks instead of connections and relationships between people [11].

This research aims to propose a new approach by analyzing relations of attacks to develop predictive capabilities. The network of attacks is modeled in the approach to understand future strategies. More specifically, a new outlier-based similarity function is proposed to find relations that will help construct a network for events. Furthermore, this similarity function is used to estimate relationships among interactive events by using non-similar attacks [11, 12]. This method extracts attacker interaction from network properties to obtain a better understanding of the attacker activity. The results could potentially help in the understanding of future attacks and enable counter-terrorism agencies to propose proactive strategies [11, 13].

The remainder of the paper is organized as follows. In Section 2, data analysis and collection are explained, and the methods used in the new approach are presented. A detailed description of how the proposed approach is used to understand complex interactions is also presented. In Section 3, experimental results that show the proposed approach works to understand attacker activities efficiently are presented. Finally, Section 4 presents a discussion to highlight the improvement in modeling terrorism and the contribution of the research.

2. Materials and Methods

Terrorist attacks listed in the Global Terrorism Database (GTD) are used in this research. The data includes various events between 1970 and 2015 [2]. The data is prepared by removing missing values and incorrect events. The following section provides details of the proposed approach. Moreover, bombing (with explosives weapons) attacks, as seen in Fig. 1 and Fig. 2, are used against defenders' agencies (e.g., Military, Police, etc.). This type of attack was chosen because they constitute half of all attacks [11].

In the collected dataset, the variable names are explained as follows: Extended incident (extended) is defined as yes (1) if there is an extension for more than 24 hours or no (0). Doubt of terrorism proper (doubtterr) is defined as yes (1) or no (0). Part of multiple incidents (multiple) is determined as yes (1) or no (0). Location of events is defined using countries, regions, state, and city. Vicinity (vicinity) is used as yes (1) if the event happens near the city or no (0) if it is in the city center. Specificity is determined at the geospatial resolution of the latitude and longitude areas with five different categories. Attack type (attackttype1)is defined as a Bombing/Explosion attack. Successful Attack (success) is defined based on whether the event is successful (1) or not (0). Weapon type (weaptype1) is defined as which weapons are used for attacks. Target type (targettype1) is determined by which targets the attackers pursue. The number of killings (nkill) means the number of people killed in the attack. Hostage