Volume 2, No. 6, Nov-Dec 2011

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Statistical Data Mining for Security System Allocation in Terrorist Attacks

Senthamarai Kannan.K*, Manikandan.M
*Professor, Department of Statistics
Research Scholar, Department of Statistics,
Manonmaniam Sundaranar University, Tirunelveli, India.
senkannan2002@gmail.com*, manikandanmsu@gmail.com

Abstract: Data mining is the process of posing queries and extracting patterns, often previously unknown from large quantities of data using pattern matching or other reasoning techniques. It has many applications in security including for national security as well as for cyber security. Security allocation is one of the possibilities of averting terrorist attacks. This paper examines the effect of framing on decision making in a homeland security across the highly terrorist attacking countries to propose a formal model to allocate the security forces. The allocation is mainly based on the probability of attacking countries to prevent the attack.

Key words: Data mining, security allocation, counterterrorism.

I. INTRODUCTION

Data mining is the art and science of extracting hidden information from large data sets. This is a description of artificial intelligence, has primarily been used to analyze business and scientific data. Later than 2001 9/11 attacks, the U.S. government developed interested in likely applications of data mining techniques to counterterrorism. They increased government interest in technological approaches to preventing terrorism and brought it into public scrutiny. In February, 2002, the U.S. Office of Science and Technology Policy convened government representatives and industry leaders to discuss how they could use data mining as a counterterrorism tool. Terrorism is increasing severely with the growth of the global superhighways of communication, resulting in the loss of billions of dollars and victims for worldwide each year.

Although prevention technologies are the best way to reduce terrorist attack, fraud, fraudsters are adaptive and given time, will usually find ways to circumvent such measures. Statistics and machine learning provide effective technologies have been applied successfully to detect terrorist activities such as bomb explosion, money laundering, e-commerce credit card fraud, telecommunications fraud and computer intrusion, etc,. Terrorism is hard to ignore. Every day television news shows, newspapers, magazines, and Websites run and re-run pictures of dramatic and usually bloody acts of violence carried out by cruel looking terrorists or claimed by shadowy militant groups. It is often hard not to be scared when we see people like us killed or maimed by terrorist attacks at fast food restaurants, in office buildings, on public buses and trains, or along normal-looking streets. Some parts of the world have remained unharmed by the current gesture of terrorism that began in the late 1960's. This paper will explore the aspects of highly terrorist affected countries are taken. The definitions of terrorism:

"Terrorism is the unlawful use or threat of violence against persons or property to further political or social objectives. it is usually intended to intimidate or coerce a government, individuals or groups, or to modify their behavior or politics[5]. - Vice-president's task force, 1986

Although terrorism is an inevitable reality in the present scenario, when the whole world is the cruel jaws of it, but this ineluctable reality cannot be curtailed through the more terrorism or on the same pace; as many countries of the present world are trying to do it in this way. Researchers have studied terrorist attacks and proposed suggestions and models to avert the attacks from earlier years. The connections between criminals and terrorists and the potential overlap and meshing of their networks and considers the implications of these intersections for counterterrorism policies and actions [2]. An advanced time series method to identify the dynamic properties of three hostage taking series. The immediate and long run multipliers of three covariates - successful past negotiations, violent ends, and deaths - are identified. Each hostage series responds differently to the covariates. Past concessions have the strongest impact on generating future kidnapping events, supporting the conventional wisdom to abide by a stated no-concession policy [3].

The missile defence problem as a resource allocation problem and framing on decision making in a home land missile defense context across three tasks of varying complexity [6]. Identified the factors that help explain terrorist success in hostage-taking events, two measures of success is examined: logistical success and negotiation success. They also sketches the choice-theoretic model faced by a terrorist during the planning and negotiating stages of a hostage mission [7]. A standard research framework in behaviour decision making is to use forms of expected utility theory as a benchmark for performance [1].

The undertaking of optimally assigning military regulation to enemy targets, frequently termed the Weapon Target Allocation (WTA) problem; this has become a major focus of modern military thought where a cost effective allocation is required without degrading the required kill performance. A probabilistic approach is used for three main weapon allocation techniques namely uniform weapon allocation, first-in-first weapon allocation and shoot-look-shoot weapon allocation [4].

A model for averting the terrorist attacks is proposed in this paper, the section II describes the proposed the model.

In section-III the results are discussed, the concluding remarks are given in section IV

II. BACKGROUND THREAT

Security allocation is the distribution of resources. In this paper how to allocate security forces in terrorist attacks countries using data mining technique. The Counter terrorism is mainly about developing counter measures to threats occurring from terrorist activities. The information on terrorist threat we have presented has been obtained entirely from unclassified news paper articles and news reports that have appeard over the years.

A. Threat:

The threats can be defined as non information related threats and information related threats, bio logical threat, and chemical attacks. Non-information related threat is people attacking bombs and guns. Information related terrorism is threat due to the existence of computer system and networks. These are illegal intrusion and viruses as well as computer related vandalism. Information related thread also known as cyber terrorism. These are terrorist attacks caused by bio logical substance, chemical and nuclear attacks. Allocating the security system to protect critical infrastructure, cities, peoples require measuring the threat posed to specific types of attacks. Probability can be used measure the attacks will occur. The threat is defined as

Threat = probability of attacks occur
= Pr [attacks occurs]

III. PROPOSED MODEL FOR COUNTER TERRORISM

The terrorist attacks can be averted if the plan of attack is known. The plan of attack is normally not revealed by the terrorists. In order to get a glimpse of attack the communication links between terrorists are monitored by security agencies. If there is a lack of security agencies it is hard to identify the plan of terrorist attack. The allocation of security forces for countries helps in identifying the plan of terrorist attack and counters the attacks. The loss incurred by a terrorist attack is estimated. If the expected loss is very high for a particular country then it would be better to allocate more security forces.

The loss is occurred only if the terrorist attack is carried out successfully. The probability of successful terrorist attack is also depends on lack of security forces and the attack method. The probability of attacking a country is computable from the historical data of previous attacks. The attacking a country is not guaranteed. Even if the attack is carried out it can be defended by security forces. The probability of defending the attack is based on number of available security forces. The probability of attacking the country(x) is P(x). The probability of defending the attack is D(x). The loss can be estimated according to Sungsoon Park and Ling Rothrock (2007) as

$$L(x) = P(x) * (1 – D(x))^N(x)$$

Where N(x) is the allocated number of security forces. The N(x) is selected based on the given algorithm.

A. Computational Algorithm for Security Allocation :

Step1: Compute Probability of attacking a country (P(x)).
Step2: Compute the probability of successful prevention of attack if attacks plan is known.
Step3: Get the available security forces.
a).allocate the security force progressing to every country.
b). if the allocation is invalid go to 3a
Step 4: Select the allocation, if the loss is lesser than the earlier.
Step 5: Otherwise go to step 4.
Step 6: The selected allocation is the optimal allocation of security forces.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The algorithm described in this paper is implemented in IDL. The program is executed with different countries data. Initially the data in table-I is number of attack from 2004 to 2010 by taking the probability to defend the attack as 0.7. The ‘attacks’ column indicates the total number of attacks made in a specified period of time in a country.

Table 1: Total number of Attacks from 2004 to 2010.

Country	Attack
Iraq (C1)	25678
India (C2)	6096
Afghanistan (C3)	9495
Nepal (C4)	3712
Bangladesh (C5)	284
France (C6)	340
Pakistan (C7)	7088
Russia (C8)	2139
Thailand (C9)	4205
Colombia (C10)	2911

Table 2: Possible loss of attacks

Allocation of security force										Loss L(X)
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	
1	0	2	0	1	0	1	0	5	0	0.376178
0	1	2	0	1	0	1	0	5	0	0.574978
0	0	3	0	1	0	1	0	5	0	0.627947
2	0	0	1	1	0	1	0	5	0	0.384928
1	1	0	1	1	0	1	0	5	0	0.401448
0	2	0	1	1	0	1	0	5	0	0.643368
1	0	1	1	1	0	1	0	5	0	0.367148

0	1	1	1	1	0	1	0	5	0	0.565948
0	0	2	1	1	0	1	0	5	0	0.598778
1	0	0	2	1	0	1	0	5	0	0.451708
0	1	0	2	1	0	1	0	5	0	0.650508
0	0	1	2	1	0	1	0	5	0	0.616208
0	0	0	3	1	0	1	0	5	0	0.708706
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
0	0	1	0	1	1	0	5	0	2	0.725655
3	1	2	0	0	0	2	0	1	1	0.182944
3	**1**	**2**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**0.166774**
2	2	2	0	0	0	2	0	1	1	0.187900
1	3	2	0	0	0	2	0	1	1	0.260476
0	4	2	0	0	0	2	0	1	1	0.519213
3	0	3	0	0	0	2	0	1	1	0.235913
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
0	0	0	1	0	0	0	0	1	8	0.774503
0	**0**	**0**	**0**	**10**	**0**	**0**	**0**	**0**	**0**	**0.893000**
0	0	0	0	0	1	0	0	0	9	0.851501
0	0	0	0	0	0	1	0	0	9	0.782901
0	0	0	0	0	0	0	1	0	9	0.833301
0	0	0	0	0	0	0	0	1	9	0.812301

The security allocation and possible loss if the attack is carried out successfully is given in Table II. The allocation column indicates the number of security forces allocated to ten countries. The 'loss' column indicates the loss incurred if the allocation of security forces for the countries in the corresponding row. The loss incurred is varying as the allocation varies. It can be observed that loss would be high if all the ten security forces are allotted to country C5. The corresponding row is indicated by red color in table II. The loss would be very less if 3 security forces are allocated to C1, 1 Security force for C2, 2 security force for C3, 1 security force for C4, 0 security force for C5, 0 security force for C6, 1 security force for C7, 0 security force for C8, 1 security force for C9, and 1 security forces for C10. The allocation in which the loss is very less is considered to be the best security system allocation. This is indicated by blue in color in table II.

The program is executed by giving the factual data given in table I with the assumption of 0, 4 for probability to defend the attack. The best security allocation of 10 security forces to these ten countries mentioned in table II is computed as (3,1,2,1,0,0,1,0,1,1) out of 92378 valid allocations. This indicates that the security system is allocate to based on loss in order keep the loss as minimum as possible (0.166774) with the available 10 security forces. The worst case allocation is computed as (0, 0, 0, 0, 10, 0, 0, 0, 0, 0). In the current scenario if all the 10 security force for C5 is allocated, the effective worst case loss is estimated as 0.89300.

V. CONCLUSION

The result reveals that the implemented algorithm computes the best allocation of security system to allocate the various countries based on the historical data and the available number security forces. This can be applied to security forces, to avoid the loss, to protect the people and taking decision making for allocating security system. The probability to defend the attack is assumed and this may be computed automatically in the future.

VI. ACKNOWLEDGEMENT

The authors thanks to University Grants Commission for financial support done by this work.

VII. REFERENCE

[1] MacCrimmon K.R., Part one: Discussions, in: Hillel J.Einhorn, R.M.Hogarth (Eds.). Insights in Decision Making: A Tribute, the University of Chicago Press, 1990, pp.66-89.

[2] Michael Stohl Networks, terrorists and criminals: the implications for community policing, journal of Crime Law Social Change, 2008, vol.50, No.1-2, pp. 59-72.

[3] Patrick T., Brandt, Todd Sandler, Hostage Taking: Understanding Terrorism Event Dynamics, Elsevier, 2008, pp 1-28.

[4] Prabhakar, et al., Weapon Allocation In Sam Systems, XXXII National Systems Conference, 2008.

[5] Robert Fischer J., Edward Halibozek, and Gion Green, Introduction to Security, eighth edition, Elsevier, 2008.

[6]Sungsoon Park, Ling Rothrock, Systematic analysis of framing bias in missile defense: Implication toward visualization design, European Journal of Operation Research, 2007, vol.182, No.3, pp.1383-1398.

[7]Todd Sandler and John Scott, Terrorist Success in Hostage: Taking Incident: An Empirical Study, The Journal of Conflict and Resolution, 1987, Vol.31, No.1, pp 35-53.