Proceedings of the 2016 Industrial and Systems Engineering Research Conference
H. Yang, Z. Kong, and MD Sarder, eds.

An Agent Based Approach for Understanding Complex Terrorism Behaviors

Salih Tutun
Department of Systems Science and Industrial Engineering
Turkish Military Academy, Ankara, Turkey, and Binghamton University, Binghamton, NY

Haifeng Wang
Department of Systems Science and Industrial Engineering
State University of New York at Binghamton, Binghamton, NY

Zhao Liu
Department of Electrical and Computer Engineering
State University of New York at Binghamton, Binghamton, NY

Mehmet F. Yıldırım
Department of Systems Science and Industrial Engineering
Turkish Military Academy, Ankara, Turkey, and Binghamton University, Binghamton, NY

Sina Khanmohammadi
Department of Systems Science and Industrial Engineering
State University of New York at Binghamton, Binghamton, NY

Abstract

Understanding the behavior of a terrorist group is a complex phenomenon because of the uncertainty in strategies and tactics used by terrorists. Current literature suggests that terrorism has an evolutionary nature and terrorist groups change behavior according to a government's counter-terrorism policies. The goal of this research is to model how terrorist groups and government influence each other. In this regards, an agent-based modeling with network topology is used to model the system composed of interacting agents (attacks) and groups. The terrorist groups' tactics are modeled based on the success rate of attacks and the defense level of a particular location. The proposed model is validated using real-world data of suicide attacks in Iraq. The model can be used to support governmental counter-terrorism policy-making.

Keywords
Agent Based Modeling (ABM), Suicide Attacks, Human Behavior, Networks

1. Introduction
In recent years, suicide attacks have been increasing because they have a high probability of success. Preventing these attacks is a significant challenge for governments due to the uncertain tactics and behavior of terrorist groups. Terrorist groups' behaviors change dynamically over time and affect individual terrorist behaviors. Therefore, an essential aspect of studying terrorism is to analyze dynamic organizational behaviors that change over time [1]. A strategic analysis of terrorist activity is made to understand interactions of terrorist organizations by using non-cooperative game theory [2]. In addition, a behavioral analysis of terrorist activities is conducted, in order to understand campaigns, by using a multidimensional Scalogram Analysis technique [3]. Despite this fact, most of the current studies focus on understanding the relational structure of a terrorist group using network analysis [4]-[7]. These studies provide qualitative and quantitative results that may be helpful to understand relational structure. However, it is clear that terrorist

organizations are complex, and their behavior cannot be fully understood using structural analysis [8].

In this regards, Agent Based Modeling (ABM) simulates the changing interactions among agents and can model emergent collective behaviors. ABM has been shown to be an efficient tool for analyzing evolutionary dynamics of terrorism networks and interactions [9]. In this study, we simulate events (terrorist attacks) by using ABM with proposed network topology to understand the behaviors of complex terrorism behaviors. Evolutionary dynamics of networks and relational structure are used to build the model. At the same time, a defense level of cities by government after attacks is defined to simulate real system for terrorism.

In this research, the ABM is developed to analyze the behavior of suicide attacks by competing terrorist groups such as ISIS and Al-Qaeda. We validated our model by comparing terrorism data set and counter-terrorism tactics for controlling the oil regions in Iraq and how different tactics spread among terrorist organizations. The rest of the paper is organized as follows. Section 2 provides the materials and methodology of this study. In Section 3, the results and discussion are provided, followed by the conclusion in section 4.

2. Materials and Methods

The method consists of two parts including network construction and ABM. In network construction, we construct a network based on the relationship of different attacks in our data set. Then, we formulate the problem as ABM to understand the dynamics of the topological changes of terrorist and counter-terrorist organizations. The details of each section are provided below.

2.1 Data

The National Consortium for the study of terrorism and responses to terrorism (START) is employed in this study [11]. We used part of this data set that includes 3,795 attack events. Based on the decision tree (e.g., ID3 algorithm), nine attributes are selected for each attack event: attack type, weapon type, target type, the number of people killed, the number of people wounded, location, terrorist group, property damage, and attributes factor. Moreover, rules for successful attacks are defined by using a decision tree for each agent. We also have fitted a probability distribution for the attack type, weapon type, target type, property damage, terrorist group, the number of people killed and wounded, corresponding distributions. The probability distributions will be used in the proposed ABM.

2.2 Network Construction

The network model is built to model the behaviors and changes of attack events in the time domain. Each node in the network represents an attack event at a certain time. The connections between any two nodes are explained as the similarity (learning behavior) of the two attacks, which is judged based on attribute factor and the attack behavior of the two attacks. For each node, nine attributes are applied: (1) Terrorist group, two terrorist groups are considered in the model, and they are encoded as 0 and 1, (2) Attack type, nine candidate attack types are applied: 'Assassination', 'Hijacking', 'Kidnapping', 'Barricade Incident', 'Bombing/Explosion', 'Unknown', 'Armed Assault', 'Unarmed Assault' and 'Facility/Infrastructure Attack', (3) Weapon type includes 11 categories: 'Biological', 'Chemical', 'Radiological', 'Nuclear', 'Firearms', 'Explosive/Dynamite', 'Fake Weapons', 'Incendiary', 'Melee', 'Vehicle' and 'Sabotage', (4) Target type contains 12 types: 'Business', 'Government', 'Police', 'Military', 'Abortion-Related', 'Airports', 'Government (Diplomatic)', 'Educational Institution', 'Food Water Supply', 'Media', 'Maritime' and 'NGO (non-government organization)', (5) Number of killings means the number of people killed in the attack, (6) Number of wounded indicates the number of people wounded by that attack, (7) Location is the position of that attack, (8) Attribute factor describes the attack pattern for each event, 0 or 1, (9) Property damage indicates whether the attacks cause property damage, 1 represents yes and 0 shows no.

The similarity between different attack events (edges of the network) is calculated as follows:

$$S_{simi} = \sum_{i=1}^{9} w_i x_i + \exp(-d_{a,b})(Dfl_a + Dfl_b) \tag{1}$$

where w_i represents the weight for each attributes, x_i represent the similarity for i^{th} attribute. x_i equals to 1 if attack type, weapon type, and target type are the same, and x_i equals 0 if they are different. For the number of people killed

and wounded, if the difference is less than 20 percent of the mean value of the distribution than x_i is equal to 1, otherwise 0. $d_{a,b}$ is the distance between the location of attack a and b. Dfl_a and Dfl_b represent the defense level of corresponding location for attack a and b, respectively. S_{simi} represents the similarity between two nodes. If S_{simi} is greater than a predefined threshold, then an edge will be added to them. We use the information obtained from this network to construct our ABM.

2.3 Agent Based Modeling

An ABM is developed to express the behavior of attacks in each year. Hence, all agents in our ABM have the same time point. The notations of the variables used in the ABM are given in Table 1. In this research, the variables are divided into basic and control variables, where we mainly considered the impact of these control variables to the terrorist attack behaviors.

Table 1: The notations of the variables used in the ABM

Notations	Definition	Type	Category
$nEvent_j$:	Number of candidate attack events for terrorist group j	Discrete	
p:	Population factor of the world, indicates population size	Continuous	
nK_j:	Number of people killed in the last five years for terrorist group j	Discrete	
Dfl_l:	Defense level of location l in the world	Continuous	Basic variables
W:	World size	Continuous	
f:	Attribute factor	Binary	
s_{jl}:	Success rate of an attack from terrorist group j at location l	Continuous	
df:	Defense factor of the world, an effort factor of government	Continuous	
a_j:	Aggressive factor for terrorist group j	Continuous	Control variables
dc:	Cooling factor of the defense	Continuous	

The process of constructing our ABM is as follows:

1. The data structure to store the attributes of the agents:
   Each agent corresponds to a node in our constructed network in the previous section. Therefore, each agent represents an attack event, which also includes nine attributes.
2. The data structure to store the states of the environment:
   The environment is a discrete world map, where each location has an attribute called defense level (Dfl) to represent the degree of danger in that location. Initially, the world is safe, so all the defense levels are zero. The higher defense level indicates a lower chance of attack and a smaller success rate for the following attacks. We also include another parameter called df, which indicates a government's willingness to prevent terrorist attacks.
3. Rules for how agents interact with each other:
   In this model, the interaction of agents represents the learning behavior of terrorist groups. The learning behavior of terrorists modeled using the attribute of "number of people killed in last five years". The mathematical formulation of learning behavior model is as follows:

$$nK_j = \sum_{t=now-5}^{now} pk_t \tag{2}$$

4. Rules for how agents interact with the environment:
   The interaction between agents and environment is modeled using defense level. When an attack happens, the defense level around that area increases. In the model, the defense level of the government is defined as an exponential function and the severity of attack events follows an exponential decay along the distance. The defense level is formulated as Equation (3).

$$Dfl_l = df \exp||n-e|| \tag{3}$$

   where n represents the neighborhood of the newly generated attack, and e is the attack center.

5. Rules for the dynamics of the environment:
   At each iteration, the defense level of the environment follows a constant decay in the whole map. The decay is described as a cooling factor of the defense, denoted as dc.
6. Rules for the dynamics of the agents:
   Each agent represents an attack generated by a terrorist group. For each terrorist group, the aggressive factor is used to indicate the aggressiveness, which describes the likelihood that terrorist groups generate attacks. Hence, the aggressive factor is influenced by whether an attack can be successfully generated. The aggressive factor gets updated based on four assumptions. First, the aggressive factors will decrease after a terrorist attack happened due to the potential loss of manpower and other resources. Second, the aggressive factors will increase if one attack attempt fails. Third, the aggressive factor of terrorist group A will increase when other terrorist group has more successful attacks than A. This assumption is based on the fact that terrorist groups want to keep their influence in the world by having more successful attacks than other group. Fourth, the aggressive factor will decrease if a terrorist group launches more attacks than other group. The reason is that the group launching more attacks will draw more attention from the government and will become the primary target of the government and counter-terrorism agencies.
   The number of new attacks (agents) is generated based on the aggressive factor, population, learning, and defense level as shown in Equation (4).

$$nEvent_j = a_j\left(\frac{p}{\sum(Dfl)} + \frac{nK_j}{p} - \log\left(\frac{\sum(Dfl)}{df \cdot W}\right)\right) \tag{4}$$

   After determining the number of candidate attacks that could happen ($nEvent_j$), we need to evaluate the success rate of each attack to judge whether the candidate attack will happen or not. This criteria is formulated as Equation 5.

$$s_{jl} = f + nK_j - \frac{Dfl_l}{df} \tag{5}$$

After constructing the ABM, the model needs to be initialized by generating initial agents (attacks) and setting their properties. The properties of initial attacks are set according to the distribution of each property obtained from real data. The initial location properties are generated randomly. During the simulation process, in each iteration, new attack events are generated for two different terrorist groups according to Equation (4). The maximum number of attacks for each group at one iteration is restricted by a limiting factor defined using the mean value of defense level. The location of each new attack is assigned randomly, and the number of people killed and wounded is regenerated based on the previously fitted normal distribution. These new attack events also use the attack success rate as the criteria to judge if the attack event will happen or not.

3. Results and Discussion

The results of the ABM for two terrorist groups (indicated by blue and red colors) are shown in Figure 2. As seen in the figure, at the beginning terrorist groups are competitive as they want to take control of different locations. As one group starts to take control of a location by launching more attacks, the other group begins to become more aggressive. This competition continues until the government takes action by increasing the mean defense level for a particular location. The interesting fact is that after this counter-terrorism measure takes effect, the terrorist groups start to cooperate with each other to gain control of the location. This cooperation is apparent in the phase space of the aggressive factors, where the aggressive factor of groups is balanced indicating that both groups are acting together as one terrorist group rather than competing each other.

To validate the proposed model, we compared the actual suicide attack data of two major terrorist groups in Iraq (ISIS and Al-Qaeda) to our simulation results. As shown in Figure 1, Al-Qaeda started to increase the number of attacks after the September 2001 attack. However, the number of attacks by this group and ISIS is balanced until 2010. After ISIS gained control of most of the oil resources in 2010, the two groups engaged in a competition between 2010 and 2012 by launching more attacks to take over oil resources in Iraq. However, after the international community took further action against ISIS in 2012, both groups started to cooperate and launched an equivalent number of attacks against government targets in Iraq. This pattern is similar to what we observed in our simulation results (Figure 2). This information can be used by counter-terrorism agencies to take proper and timely action to prevent cooperation

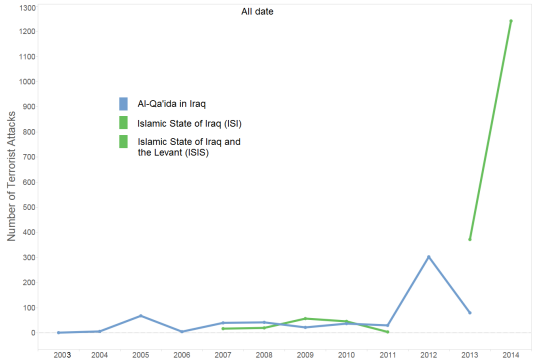

Figure 1: Actual behaviors of ISIS and Al-Qaeda in the data. Note: Al-Qaeda and ISIS are showed by the blue line and the green line, respectively

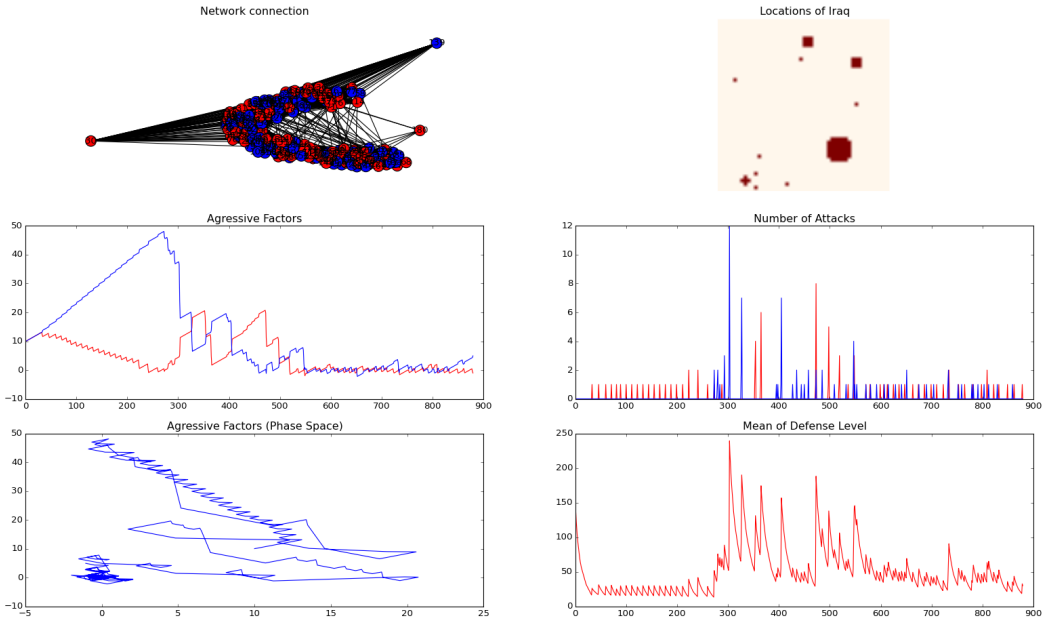

Figure 2: Simulation results of groups' terrorism behaviors

between terrorist groups and to increase the security level at potential targets, thus ultimately preventing future terrorist attacks.

Therefore, the terrorist groups understand that they will lose control if they do not share information because when the groups attack, the government increases the defense level. They need to share information and power against the government. Afterwards, as seen in Figure 2, the phase space for aggressive factors are balanced because they behave as one terrorist group. This means that the groups act together for attacks. The groups balance for aggressive factors because they learn tactics and the government's behavior. For sensitivity analysis of the results, the actual data for ISIS and Al-Qaeda is compared so as to check our simulation results, as seen in Figure 1. Al-Qaeda started to increase the number of attacks after September 2001. By 2011, both groups were attacking with equal intensity. After 2011, however, as ISIS was losing power, Al-Qaeda increased attacks to control the locations. Then by 2013, ISIS again began increasing attacks. From 2013 onward, they behaved as one terrorist group in Iraq because Al-Qaeda lost power or agreed with ISIS to merge in Iraq. As tactics, to make successful attacks, the bombing of military and police became famous attacks in the simulation. At the same time, government can control aggressive factors to control the terrorist attacks before they happen. We understand that after the groups became professionalized in terms of tactics

and locations, they acted together against the government. As a result, if the government would like to take control of places, they need a policy which divides the groups' power.

4. Conclusion

In this research, we proposed an agent-based model to analyze the behavior of different terrorist groups and how their behavior changes according to government policies (defense level). This analysis helps to predict each terrorist group's future behavior according to current information. The proposed model was validated using real-world data of suicide attacks in Iraq. This research can help the government agencies to develop proper counter-terrorism polices according to the predicted future behavior of terrorist groups.

Acknowledgment

The authors wish to thank the Turkish Military Academy and the Global Terrorism Database for supporting research and their help in providing data, respectively. The authors would like to thank Dr. Hiroki Sayama for his valuable comments and suggestions about the research.

References

1. Li, B., Sun, D., Zhu, R. and Li, Z., 2015, "Agent Based Modeling on Organizational Dynamics of Terrorist Network," Discrete Dynamics in Nature and Society, retrieved from http://dx.doi.org/10.1155/2015/237809
2. Das, S. P., and Lahiri, S., 2006, "A Strategic Analysis of Terrorist Activity and Counter-terrorism Policies," Topics in Theoretical Economics, 6(1), 1-28.
3. Wilson, M. A., Scholes, A., and Brocklehurst, E., 2010, "A Behavioural Analysis of Terrorist Action the Assassination and Bombing Campaigns of ETA between 1980 and 2007," British Journal of Criminology, 50(4), 690–707.
4. Krebs, V. E., 2002, "Mapping Networks of Terrorist Cells," Connections, 24(3), 43–52.
5. Moon, I. C., and Carley, K. M., 2007, "Modeling and Simulating Terrorist Networks in Social and Geospatial Dimensions," Intelligent Systems, IEEE, 22(5), 40–49.
6. O'Neil, Patrick, 2012, "Dynamic, Covert Network Simulation," Social Computing, Behavioral-Cultural Modeling and Prediction, Springer, 239–247.
7. Wang, M. C. G. A., Chen, X. Z. H., and Mao, D. Z. W., 2011, "Intelligence and Security Informatics,". Pacific Asia Workshop (PAISI).
8. Carley, K. M., 2003, "Dynamic Network Analysis," 133-145.
9. Ilachinski, A., 2012, "Modelling Insurgent and Terrorist Networks as Self-organised Complex Adaptive Systems," International Journal of Parallel, Emergent and Distributed Systems, 27(1), 45–77.
10. Backus, G. A., and Glass, R. J., 2006, "An Agent-based Model Component to a Framework for the Analysis of Terrorist-group Dynamics," Sandia Report, SAND2006-0860P.
11. National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2015 "Global Terrorism Database," retrieved from http://www.start.umd.edu/gtd