Hindawi
Discrete Dynamics in Nature and Society
Volume 2018, Article ID 5676712, 16 pages
https://doi.org/10.1155/2018/5676712

Research Article

Terrorist Group Behavior Prediction by Wavelet Transform-Based Pattern Recognition

Ze Li[1], **Duoyong Sun**[1], **Bo Li**[2], **Zhanfeng Li**[1] and **Aobo Li**[3]

[1] *College of Information System and Management, National University of Defense Technology, Changsha 410072, China*
[2] *Xi'an Hi-Tech Research Institute, Hongqing Town, Xi'an 710025, China*
[3] *Space Engineering University, Beijing 101400, China*

Correspondence should be addressed to Ze Li; plalize@nudt.edu.cn

Received 24 August 2017; Revised 17 December 2017; Accepted 31 December 2017; Published 28 January 2018

Academic Editor: Seenith Sivasundaram

Predicting terrorist attacks by group networks is an important but difficult issue in intelligence and security informatics. Effective prediction of the behavior not only facilitates the understanding of the dynamics of organizational behaviors but also supports homeland security's missions in prevention, preparedness, and response to terrorist acts. There are certain dynamic characteristics of terrorist groups, such as periodic features and correlations between the behavior and the network. In this paper, we propose a comprehensive framework that combines social network analysis, wavelet transform, and the pattern recognition approach to investigate the dynamics and eventually predict the attack behavior of terrorist group. Our ideas rely on social network analysis to model the terrorist group and extract relevant features for group behaviors. Next, based on wavelet transform, the group networks (features) are predicted and mutually checked from two aspects. Finally, based on the predicted network, the behavior of the group is recognized based on the correlation between the network and behavior. The Al-Qaeda data are investigated with the proposed framework to show the strength of our approaches. The results show that the proposed framework is highly accurate and is of practical value in predicting the behavior of terrorist groups.

1. Introduction

A terrorist group is fundamentally a social system. The group is formed as a unified whole by fanatics determined to inflict civilian and economic damage on specific targets in pursuit of their extremist goals [1]. Currently, as terrorist groups are becoming more international, allied, and networked, the social systems are transforming into complex sociotechnical systems. For a continuous active terrorist group, the behavior is influenced by both the interactional environment and the organizational mechanism and thus is a continuously evolving phenomenon [2]. The structure and efficiency of the group will fluctuate and finally reach a relatively stable state because of its covert nature and self-defense mechanism [3]. Even though it is as a complex system, the terrorist group is also dynamic. The dynamics result from multiple change processes, such as natural evolutionary processes including learning, birth, and aging, as well as intervention processes, such as altering the set of individuals who lead a group [4]. The relationships and interactions between terrorists at the microlevel leads to continuous development of the group behavior at the macrolevel [5]. The process in which terrorists look for and cooperate with other terrorists, which has a multitude of purposes, such as propaganda, training, defending, or sanctuary, also drives the system to change dynamically. Thus, studies on terrorist group behavior are becoming complex dynamic system problems, which require new methods for understanding the system behavior and dynamics.

At present, there is an intense interest in predicting what a terrorist group behavior will be in the future. Predicting terrorist group behavior is of great importance, especially for attack behavior. Once such behavior is predicted, we are able to monitor the dynamics of the group and detect early warning signs of the behavior change [6]. We can also have the intervention strategy and counterterrorism policy implemented before the attack is executed. Several studies on behavior prediction have been effectively employed by various researchers and research groups. Studies have

suggested that although the predictors of terrorist behavior are unclear, there are still factors that can provide early warning signals of future terrorist threats [7]. These studies focus on developing a model of the behavior of the terrorist group and using that to predict what the group might do in the future. Specifically, Enders and Sandler [8] use classical time-series analysis techniques to propose a threshold autoregressive model and study both the short-run as well as the long-run swells in world terrorist activity. Raghavan et al. [9] quantitatively classify the group dynamics into *Active* and *Inactive* and use the Hidden Markov Model (HMM) to track and predict the state of terrorist groups. Subrahmanian et al. [10] introduce Temporal Probabilistic (TP) rules and machine leaning techniques to predict terrorist behaviors and major terror attacks by a Pakistani-backed terrorist group, Lashkar-e-Taiba. Furthermore, these researchers develop a Stochastic Temporal Analysis of Terrorist Events (STATE) system based on the IP rule-mining engine for predicting terrorist attacks by Indian Mujahideen [11]. Najgebauer et al. [12] propose an early warning system of semantic network analysis that is based on an ontology data model to predict terrorist action preparation activities. Xue et al. [13] propose a prediction algorithm based on context subspace (PBCS) of terrorist attacks. The proposed algorithm first extracts the context subspace according to the association between the context attributes and the behavior attributes; then, it predicts the terrorist behavior based on the extracted context subspace. Tutun et al. [14] propose an ESALLOR model to select key features for similarity function and use the similarity function to understand how terrorist groups will attack in the future.

Several of the studies focus on modeling the intraorganizational relationships into networks and applying social network analysis (SNA) to predict the group behavior. Discovering suspicious and illicit behavior in social networks has become a significant problem in SNA [15]. These studies focus on the correlation between external behavior and the internal network [16]. Correlation-based SNA studies are now being extended to more comprehensive frameworks with other techniques, offering ever-increasing power to identify characteristic patterns of terrorist group in organizational behaviors [17]. Social networks that knit terrorists and constitute terrorist groups are a resource for analysis system emergence produced by the individual interactions. There is growing evidence that strengthening of the terrorists' connection may lead to some of the attack behaviors, and, thus, it is much easier to predict the group behavior by predicting the networks [18, 19]. Specifically, Carley [4] uses dynamic network analysis (DNA) to predict the dynamic relations among various entities such as actors, events, and resources and the impact of such dynamics on individual and group behavior. Mcdaniel and Schaefer [20] design an approach based on SNA and activity analysis to detect and predict anomalous terrorist activities. Clauset and Gleditsch [21] use group-level dynamic analysis and a simulation model to make quantitative predictions of the frequency and severity of the group attacks by taking the correlation with organization size. Desmarais and Cranmer [22] integrate a deterministic, similarity-based, and link prediction framework into a probabilistic modeling approach and show its ability to accurately forecast during a terrorist campaign and the onset of terrorist hostilities between a source and a target. McCulloh and Carley [6] apply multiagents to simulate the group dynamics in the social network and predict the potential terrorist events.

Related work has yielded important insights into how the behavior of a terrorist group is predicted with different models. First, it has been established that SNA is a powerful tool capable of providing a predictive and explanatory value to the field of terrorism studies [23]. Second, time-series analysis can be used to predict the future behavior, such as autoregression and the Markov model. Some possible terrorist activities in the future could be tracked by analyzing the characteristics of previous events [24]. Third, the machine leaning and pattern recognition approach can be used to predict the future behavior once the useful features are extracted [10, 11]. However, previous studies have also left blind spots. First, these studies have relatively low accuracy and efficiency in predicting the future behavior of terrorist group. In terms of common properties of the system, terrorist behavior falls somewhere between the purely chaotic and the fully deterministic realms, which is represented as a nonlinear dynamical system, characterized by a low-order chaotic attractor [25]. As terrorist behavior is in a nonlinear and nonstationary dynamic process, traditional analysis approaches, such as traditional SNA, link analysis, and autoregressive analysis, are limited in their ability to handle the dynamic data that are needed to characterize terrorist networks [4], while several methods, such as agent based simulation, have deficiencies in setting parameter values, which produce high false positives or incorrect predictions [24]. The reason lies in the complex mechanism of terrorism: terrorism has multiple political, cultural, economic, and social facets, as well as individual psychological and ideological dimensions [26]. On the other hand, previous studies are not designed particularly for terrorist groups. Several of the specific features of the terrorist activities, such as periodicity, which terrorist group behavior has, are not taken into consideration. Consequently, research that goes beyond traditional methods and considers the dynamic characteristics of terrorist behavior needs to be improved.

Inspired by previous studies, we integrate SNA, wavelet transform, and pattern recognition approaches into a comprehensive framework. We approach the problem of predicting terrorist behavior from a network analytic perspective with the supposition that the internal structure of the group network may be a good predictor of its external behavior. We use the wavelet transform framework as the time-series predictor for group's dynamic network from two aspects: qualitative inference and quantitative prediction. After the group network is predicted, a supervised classification and pattern recognition technique, Support Vector Machines (SVM), is used to recognize the attack behavior based on the correlation between the network and behavior.

The remainder of the paper is organized as follows. In Section 2, we provide a brief description of the problem characteristics. In Section 3, the research framework is introduced. In Section 4, the wavelet transform-based prediction method is demonstrated in detail. In Section 5, we introduce the

experimental design. In Section 6, the Al-Qaeda group data are described, and the results are presented with the implications discussed. Section 7 presents the paper's conclusions.

2. Problem Characteristics

Different from general social groups, operation-oriented terrorist groups have some specific characteristics. Only with thorough understanding of the characteristics can we effectively predict its behavior. In this section, we analyze the dynamic characteristics of the terrorist group from two aspects: the periodic features of the group and the correlation between the behavior and the network.

2.1. Periodic Features. A recent discovery in terrorism studies has highlighted that terror activities have some regularities, such as periodicity [27] and tendency [28]. Moreover, terrorist behavior has multiple time-scale characteristics in the nonlinear and nonstationary time series [29]. These regularities are results of both internal interactions and the external environment of the social system and are also a critical property of terrorist behavior.

Intuitively, terrorists' communication patterns may change in cycles over time [6]. Terrorists tend to interact and communicate frequently with each other during the attack or at a certain time before the attack during the planning phase [30]. Terrorists and the government are in a larger complex social system. They have interactive rational choice, where adversaries (terrorists and governments) must take actions to anticipate the responses of each other [31]. To prepare for an attack, there are several steps that terrorist groups take carefully towards the ultimate operation, such as recruiting, training, and looking for financial support. During these processes, terrorists are facing intervention from the government. However, the intervention repeats and oscillates cyclically as the focus of the government goes up and down. As terrorists will trade off risk and return when choosing their targets [31], thus, the strategies of terrorist group shift dynamically to avoid being eliminated [27]. On the other hand, terrorist groups are deeply covert, and their scale usually oscillates gradually and periodically on large time-scales (years or decades). As both the scale of the terrorist group and the group behavior are periodic features, it becomes easier to predict the future trends of the network once the periodic features are obtained.

Although terror activities often appear irrational, studies demonstrate that rational choice explanations are nevertheless useful for understanding the phenomenon of periodicity [32]. Crenshaw [33] characterizes terrorist violence as "an expression of political strategy," and Sandler and Arce [34] suggest that the predictable responses of terrorist groups to changes in sanctions and rewards aimed at constraining their behavior are strong evidence for their rationality. However, the regularity and rationality are overlooked by researchers when predicting their future behavior, and the corresponding methods remain rare in terrorism studies.

2.2. Correlation between the Network and Behavior. The internal structure and interactions among terrorists within the group drive the behavior to change dynamically. The social network can model the internal interactive pattern of elements within the social system. Previous studies have proven that there exists a correlation between group behavior and the network [6, 35]. From the system dynamics perspective, issues within the system can lead to the dynamics of the behavior. From the dynamic network analysis perspective, adding and dropping of nodes and/or relations of the network will have positive and negative influences on the group and the overarching goals [36]. In other words, the group behavior is driven by the interactive evolution of terrorists in the network and the social network model as the group structure reacts to the interactive patterns in the system. In this paper, we are not concerned with all of the behaviors, but rather only behaviors that are highly related to terrorist events, which are regarded as attack behavior. Attack behavior is defined as one kind of terrorist behavior that occurs when the group executes a terrorist attack. For example, the terrorist attack in the United States on September 11, 2001, is regarded as an attack behavior of the Al-Qaeda terrorist group. Otherwise, the behavior is regarded as normal behavior. A correlation between the network and behavior exists; therefore, the structures of corresponding networks are different. Figure 1 gives the description of the correlation. From the figure, a group's network with abnormal connections may lead to an attack behavior of the group, providing evidence for the "correlation." From the perspective of system dynamics, the behavior of the system is predicted by referencing the interactive patterns of the elements within the system. After the internal structure is predicted, we can then translate them into external behavior with the pattern recognition mechanism. As we use pattern recognition to identify the attack behavior, then a group has an attack behavior if its feature set matches the abnormal pattern. Consequently, the prediction problem is transformed into a pattern classification problem with two classes of results.

3. Research Framework

Based on the characteristics of the problem, in this section, we design a behavior prediction framework, as depicted in Figure 2. The framework tightly integrates group network and group behavior with respect to both the network prediction and behavior recognition dimensions. We are not predicting the group behavior directly, but rather predicting the group behavior through the group network. By extracting behavior-related features (a measure set) from the group network and efficiently predicting the group network, we can recognize the future behavior of the group.

There are two logic flows in the framework: the behavior recognition flow and the network predicting flow. The behavior recognition flow is designed to mine the behavior pattern of the group, which is based on the correlation between the group network (GN) and group behavior (GB), as mentioned in Section 2.2. We are convinced of the importance of measuring the structural properties of evolving networks to characterize how the behavior patterns of the investigated group change over time. Therefore, the behavior prediction

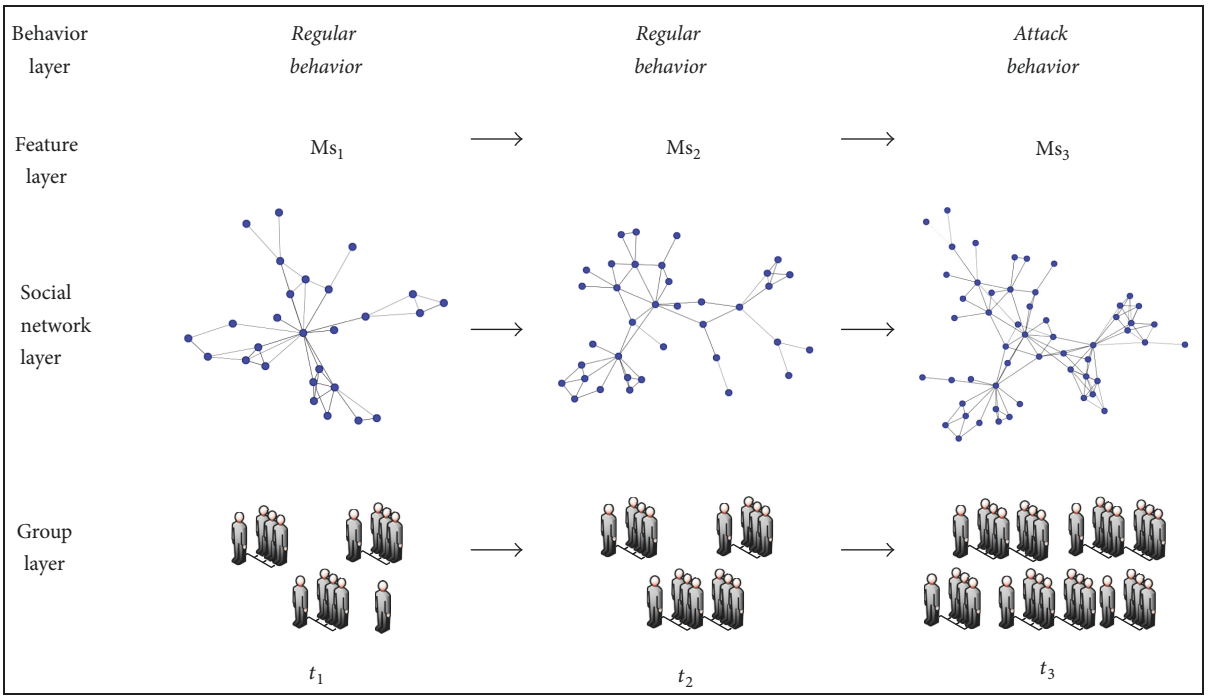

Figure 1: Descriptive figure of correlation between the network and behavior of a terrorist group.

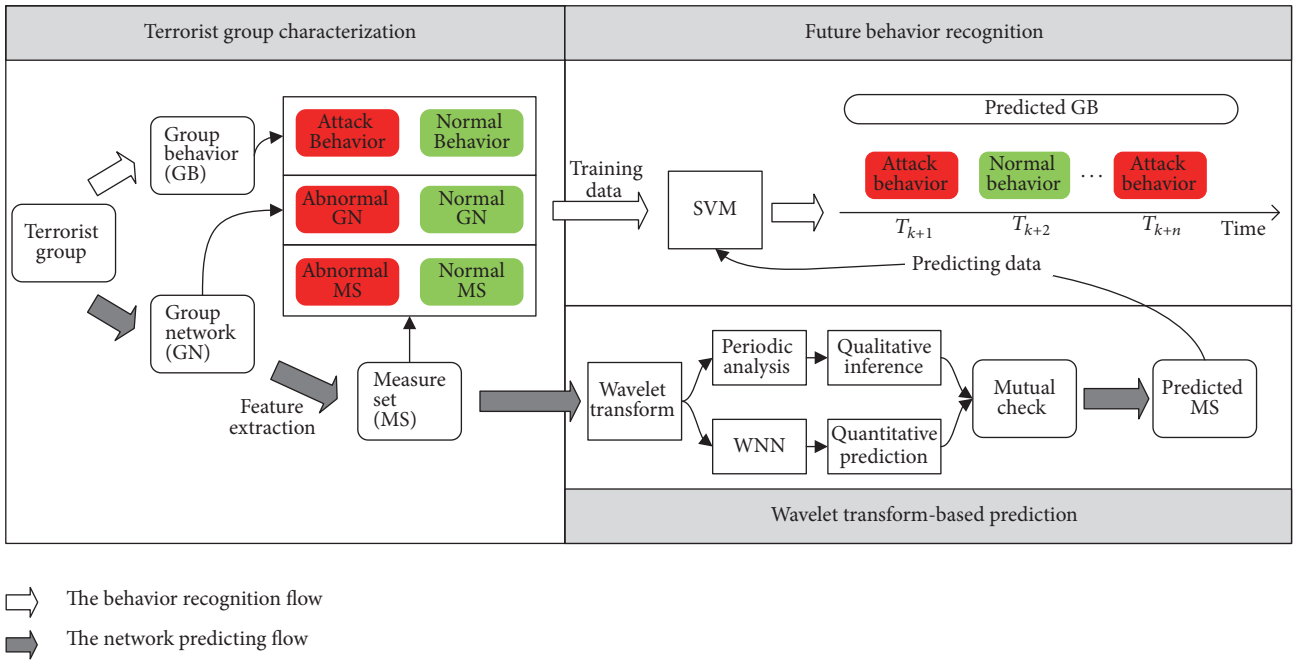

Figure 2: Framework of predicting attack behavior of a terrorist group through the group network.

problem is transformed into a behavior pattern recognition problem on the basis of effective network predictions. As shown in Figure 2, we propose two classes of behavior patterns of terrorist group: *Attack behavior* and *Normal behavior*. Thus, the behavior recognition problem can be regarded as a pattern classification problem. In this paper, the extracted features of the group network are represented by a measure set (MS). Each measure presents a specific topological feature of the network and highly influences the dynamics of processes executed on the network [12]. Network measures are therefore essential in our investigation. As is shown in Figure 2, the measure set is also classified into two classes: *Abnormal* and *Normal*. Here, as there is a consistent one-to-one match between each class of the measure set and

each pattern of behavior, then we can detect whether a group has an *Attack behavior* by matching its measure set to the patterns.

We intend to classify the group behavior through the network measures. Our objective is to develop a detection model:

$$f : \mathrm{MS} \longmapsto \mathrm{GB} = f(\mathrm{MS}). \tag{1}$$

Suppose there are a total of T timestamps included in the time-series dataset of the terrorist group $\{\mathrm{MS}_j, \mathrm{GB}_j \mid j = 1, 2, \ldots, T\}$, where MS_j denotes the extracted features associated with the jth network. For timestamp j, the measure set can be represented as $\mathrm{MS}_j = [m_j^1, m_j^2, \ldots, m_j^q]^T$, where m_j^i, $i \in [1, q]$ denotes the ith measure in the set and q denotes the total number of extracted measures. $\mathrm{GB}_j \in \{0, 1\}$ denotes the behavior pattern of the terrorist group. The group behavior pattern is also known as the classification label, such that $\mathrm{GB}_j = 1$ if and only if the group is determined as having an *Attack behavior*. In the simplest example of behavior pattern recognition, the group's behavior is recognized with the states reflecting a normal pattern of behavior ($\mathrm{GB}_j = 0$) and an abnormal pattern of behavior ($\mathrm{GB}_j = 1$). In this paper, we use the supervised classification and pattern recognition method SVM as $f(\cdot)$ due to its superior detection accuracy, computing efficiency, and modeling flexibility [37]. $f(\cdot)$ is used to assign classification labels (0/1) for the behavior pattern of the group, and equivalently,

$$f(\mathrm{MS}) = \begin{cases} 1, & \text{Attack behavior} \\ 0, & \text{Normal behavior.} \end{cases} \tag{2}$$

In summary, the behavior pattern recognition problem can be expressed as follows.

Input. Time sequence of extracted measure set MS of the terrorist group network.

Output. Set of group behaviors, denoted by behavior pattern set GB.

Our framework for predicting behavior in group networks via some network measures focuses on the future behaviors of the terrorist group. We are not recognizing the current nor historical behavior, but rather efficiently identifying how the group will behave in the future. To this end, we will introduce the network predicting flow in the next section. As mentioned in Section 2.1, there is some regularities in the terrorist group dynamic process. We believe that the group networks exhibit periodicity over time, and the periodic variations can be used to predict future trends of the group network. In addition, a future measure set of the network can be predicted from the current and historical data. In this paper, we design a wavelet transform-based framework to predict the networks, which is discussed in detail in the following section.

4. Wavelet Transform-Based Prediction Method

The key component of the framework proposed in Section 3 is to predict the group network efficiently. As a complex social system, group network prediction is quite challenging, especially for terrorist groups. Usually, the terrorist data are based on open source information. The limitations of the terrorist data make it a difficult prediction problem because we cannot be sure that all the communication and cooperation networks are included. Therefore, the best approach is not simply to predict the network from the quantitative analysis, but to combine both the qualitative and quantitative predictions. Here, we proposed an integrated method with wavelet transform for the prediction. Wavelet transform has been applied in the signal processing studies, as well as in other time-series analyses [29, 38–40]. Here, we are the first to explore the application of wavelet transform theory to better understand the structural changes in terrorist group networks. The proposed method with wavelet transform theory combines qualitative and quantitative predictions to characterize the terrorist group network in terms of its structural and functional features.

Firstly, we apply wavelet transform to obtain the periodic features of the network. Based on the wavelet transform, the nonlinear and nonstationary process of terrorist network dynamics can be decomposed into quasi-stationary by multiscale characteristics for time-series prediction. By the presence of multiscale decomposition, the advantage is automatically localized time-frequency by wavelet transform [29]. After determining both the dominant modes of variability and how those modes vary in time, we have the qualitative inference of the network trend in the future. Then, a combination of wavelet transform and Artificial Neural Network (ANN), that is, Wavelet Neural Network (WNN), is used to predict the network from the quantitative aspect. The concept of time-series predicting with a wavelet is simply predicting by using the data which are preprocessed through the wavelet transform. Finally, the predictive future networks are combined and mutually checked by both qualitative inference and quantitative prediction.

4.1. Periodic Analysis-Based Qualitative Inference. The qualitative inference can be implemented based on periodicity analysis. The application of wavelet theory in particular may provide insight into the periodic behavior of network dynamics. Given the multiple time-scale characteristics of each measure, large-scale periods may be used to characterize the future trends, while small-scale periods provide detailed characterizations of the measure change within the large-scale periods [33].

The wavelet transform of a time series is its convolution; the local base functions or wavelets can be stretched and translated with a flexible resolution in both frequency and time [38]. Choosing a proper mother wavelet is the key to wavelet transform analysis. This depends on the nature of the signal and on the type of information to be extracted from the signal. Here, the *Morlet* wavelet, a complex nonorthogonal

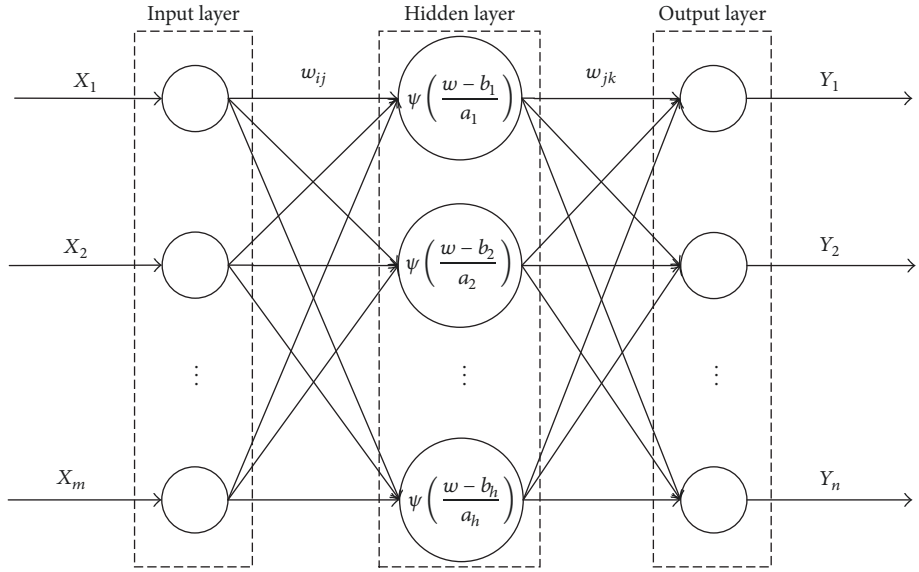

Figure 3: The network topology of WNN.

continuous wavelet, is applied to analyze inherent periodicity and to qualitatively appraise the trends of MS of the network. As a complex wavelet transform, the *Morlet* wavelet provides a good balance between time and frequency localization and can provide both amplitude and phase simultaneously.

The *Morlet* function, representing a wave modulated by a Gaussian envelope, is defined as [40]

$$\psi(t) = e^{-ict}e^{-t^2/2}, \tag{3}$$

where i is the unit of an imaginary number and $i^2 = -1$; c is the constant number. The Constant Wavelet Transformation (CWT) of time series $f(t) \in L^2(R)$ is defined as [40, 41]

$$W_f(a,b) = -|a|^{-1/2}\int_R f(t)\,\overline{\psi}\left(\frac{t-b}{a}\right)\mathrm{d}t, \tag{4}$$

where $W_f(a,b)$ is the wavelet transform coefficient; $f(t)$ is a signal or square integrable function; $\psi(t)$ is the mother wavelet and $\overline{\psi}(t)$ denotes the complex conjugate function of $\psi(t)$; a is scale factor, as the length of the wavelet period, and b is the time factor, as the translation time. The variation characteristics and the range of the periodic changes of the select measures at different time-scales can be analyzed based on the isograms about $W_f(a,b)$.

In this paper, we also introduce the wavelet variance and wavelet power spectrum to further identify the dominant and local periods. The wavelet variance is defined as the integral of any wavelet coefficient of different time-scales in the time domain. The equation of wavelet variance is defined as

$$\mathrm{var}(a) = \int_{-\infty}^{+\infty}\left|W_f(a,b)\right|^2\mathrm{d}b. \tag{5}$$

The dominate time-scales of a certain time series, namely, the significant periods dominating network evolution, will be verified through tests of wavelet variance. The wavelet variance change with scale factor a is represented by a wavelet variance graph. Each peak in the graph corresponds to a significant period [38]. The diagram of wavelet variance and wavelet power spectrum along with the isograms of the wavelet transform coefficient could be used to identify the periodic features efficiently. With the periodic features of the measures detected, their future trends can be qualitatively inferred.

4.2. WNN-Based Quantitative Prediction. In the quantitative prediction aspect, we use WNN for time-series prediction. WNNs are recently developed neural network models and have been successfully applied to forecasting, modeling, and function approximations [42]. WNN models combine the strengths of wavelet transform and ANNs processing to achieve strong nonlinear approximations [39]. WNNs are generally divided into the relax-type and the close-type by the different wavelet-basis functions. In this paper, we adopt the close-type WNN with a three-layer structure, as is shown in Figure 3.

The main difference between WNNs and ANNs lies in the activation functions of the hidden layer—as ANNs are with tangent sigmoids, while WNNs are with discrete wavelet functions. We select WNNs rather than ANNs because the ANNs have some potential disadvantages when applied to complex nonlinear optimization problems, including slowness in convergence and an inability to escape local optima. Furthermore, because WNNs combine the function of time-frequency localization by wavelet transform and self-studying by ANNs, the network capacity is approximate and robust [39]. In this paper, the WNN was designed with one hidden layer (Figure 3). We select *Morlet* as the mother wavelet function in the node activation function, as in (3).

We design a time-series prediction approach based on the hypothesis that the current value of the network measure can be captured completely by certain attributes of the historical

values [9]. Let $m_j^i = g(M_j^i)$, and $M_j^i = (m_{j-1}^i, m_{j-2}^i, \ldots, m_{j-t}^i)$, that is, the values of extracted measure m^i at past t timestamps. $g(x)$ is our prediction function and is represented by WNN with its hidden layer of the *Morlet* wavelet. For the WNN, the input variable is M_j^i and the output variable is m_j^i. Finally, the predicted results are mutually checked from the two aspects of qualitative inference and quantitative prediction to obtain more reasonable results.

5. Experimental Design

5.1. Feature Extraction. In both the two flows, a key phase is to extract features from the group networks. As we use network measures (MS) as the features, this implies the very important question of how to choose the most appropriate measures for the given network, which are directly related to the behavior pattern and affect the prediction performance [12]. The extracted measures should not only help us understand the characteristics of the networks but also help us predict the group behavior. As the terrorist network data are usually of low quality, we should extract multidimensional measures (a measure set) as the input variables to adequately represent the whole network. As discussed in Section 4.2, WNNs can achieve a high accuracy with the ability to address multiple inputs and overcome the local convergence problem for nonlinear optimization problems. However, in the pattern recognition flow, too many features involved would create the problem of the curse of dimensionality [43]. The problem increases as the number of extracted features increases exponentially. To alleviate this problem, we can apply a feature selection phase that selects only discriminating and relevant features for each class [44].

It is notably challenging to determine proper measures to characterize the network. As the field is still in its formative stages, we do not yet know which specific measures best differentiate behavior patterns or change the most in the dynamic process. In previous research [6, 12, 35], measures are extracted subjectively by manual selection and may not be significant characteristics of the network.

In this paper, we initially consider using the following criteria to extract measures from the time sequence. The first criterion is *Spearman's Rank Correlation* coefficient. With this criterion, measures that have top correlation coefficients with the group behavior are extracted. The second criterion is *Information Entropy* based selection of discriminating measures [45]. The Information Entropy $\mathrm{IE}(m^i)$ of extracted measure m^i is expressed as follows:

$$\mathrm{IE}\left(m^i\right) = -\sum_{k=1}^{H} p_k \log\left(p_k\right), \tag{6}$$

where p_k is the probability of a measure's visit into each region H_k, divided uniformly from the range of the minimum and maximum values of the measure. The $\mathrm{IE}(m^i)$ value gives the total information that could be obtained from m^i. The larger the entropy is, the more uncertainty and complexity the measure has. With (6), the measures with larger *Information Entropy* values are extracted. With the above two criteria for extracting measures, we are then able to perform the network prediction as well as the behavior recognition.

5.2. Measure Prediction. For the measure prediction, we apply the method proposed in Section 4 to obtain the prediction results for the MS. To demonstrate the superiority of our method, we compare the performance with several models, including ARIMA, BP, GABP, ANFIS, SVR, and RBF. To evaluate the prediction ability and efficiency of the different methods, we apply MAE and RMSE to compare the predicted and actual values, defined as

$$\begin{aligned} \mathrm{MAE} &= \frac{1}{N}\sum_{j=1}^{N}\left|pm_j^i - m_j^i\right|, \\ \mathrm{RMSE} &= \sqrt{\frac{1}{N}\sum_{j=1}^{N}\left(pm_j^i - m_j^i\right)^2}, \end{aligned} \tag{7}$$

where pm_j^i and m_j^i denote the predicted and actual values of the extracted measure m^i at timestamp j, N denotes the number of timestamps for the prediction, and $j \in [1, N]$. For each MAE and RMSE, a smaller value indicates better prediction accuracy.

5.3. Behavior Recognition and Risk Assessment. The predicted results of the extracted measures are then imported into functions (1) and (2) for future behavior recognition. To reduce the randomness of the analysis, we run the behavior pattern recognition with SVM many times and use the ratio of the times of *Attack behavior* ($\mathrm{GB}_j = 1$) by the total times (L) to assess the future attack risk (R_j) at timestamp j, defined as

$$R_j = \frac{\sum_L \mathrm{GB}_j}{L}. \tag{8}$$

6. Results and Discussion

6.1. Data and Network Creation. We test the proposed framework on the data from the *JJATT* database [46]. *JJATT* is a transnational terrorism database on a selection of radical Islamists, their associates, and case studies on their collective behavior. We use the data from the Al-Qaeda attack series to analyze the terrorist group behaviors. The Al-Qaeda data are collected from open source. However, in theory, the data include all of the information and are as complete as reliable, open source data allow. These data are chosen primarily because Al-Qaeda is a typical terrorist group that shares representative characteristics of militant Islamist organizations. The other reason is that Al-Qaeda data include attack data to describe the terrorist events that terrorists participated in, which is useful for testing how relevant social relationships are to *Attack behaviors*.

Al-Qaeda data in *JJATT* describe the members who have directly contributed to a "core" network and relationships that core members shared. Hence, the data are useful for developing networks describing group structure

Table 1: Extracted measures for Al-Qaeda Networks.

Criteria	Node count	Component size	Clustering coefficient	Clique count
Correlation coefficient	0.578*	0.778*	0.562*	0.563*
Information entropy	1.555	1.845	1.594	1.915

*Significant at 1% level (2-tailed).

Table 2: Comparison of selected measures between networks with *Normal* and *Attack behaviors*.

Measures	Normal behavior		Attack behavior		p value
	Mean	SD	Mean	SD	
Node count	156.767	48.797	204.765	13.419	0.0002
Component size	12.443	3.117	17.707	1.269	$8.7E-09$
Clustering coefficient	0.254	0.103	0.365	0.021	$4.6E-05$
Clique count	66.395	32.164	97.529	5.501	0.0002

and understanding the group's behavior. Al-Qaeda data also have individual interaction information according to the time axis, which makes it possible to build the dynamic networks of the group. The data are collected by year, but in this study, we further refine the data into quarters, and the networks are constructed quarterly after preprocessing. The time domain is 1989~2003; thus the time domain is divided into 60 timestamps (T_1–T_{60}). For each timestamp, a group network is created. The network's nodes are defined as terrorists, and edges are defined as relationships among the terrorists. Here, the edges are labeled by binary values (0/1), such that the value is equal to 1 if the two nodes are connected and is equal to 0 otherwise. In other words, the Al-Qaeda networks are undirected simple networks. Consequently, we build a time sequence of 60 networks, which are labeled with the IDs of $GN_1, GN_2, \ldots, GN_{60}$.

6.2. Results Summary

6.2.1. Feature Extraction. The *Attack behaviors* of Al-Qaeda refer to the verified terrorist events. For example, the event *"WTC bombing in New York City, USA, on February 26, 1993"* [46] is an *Attack behavior* of Al-Qaeda in T_{17}; therefore, $GB_{17} = 1$. Under this rule, the 60 timestamps (T_1–T_{60}) are assigned labels of 0/1, in which 17 GNs and GBs are labeled "1" and the rest are labeled "0." Using the measure extraction criteria from Section 5.1, we extract four significant measures of the Al-Qaeda network: *Node count*, *Component size*, *Clustering coefficient*, and *Clique count*. Table 1 shows the performance of the four extracted measures.

Figure 4 plots the trends of the extracted features. This figure intuitively illustrates the sparsely connected networks with *Normal behaviors*, qualitatively, compared to those with *Attack* behaviors. Figure 5 plots the distributions of the four measures of *Attack* and *Normal behaviors*.

From Figure 5, we can find that the differences are obvious between relevant features of networks with *Normal* and *Attack behaviors*. To verify that the given behaviors are caused by the given patterns of the extracted measures, we further apply Student's t-test with 95% confidence (p *value* < 0.05). Table 2 shows the p *values* of the t-tests performed to compare the measures between the groups with *Normal* and *Attack behaviors*.

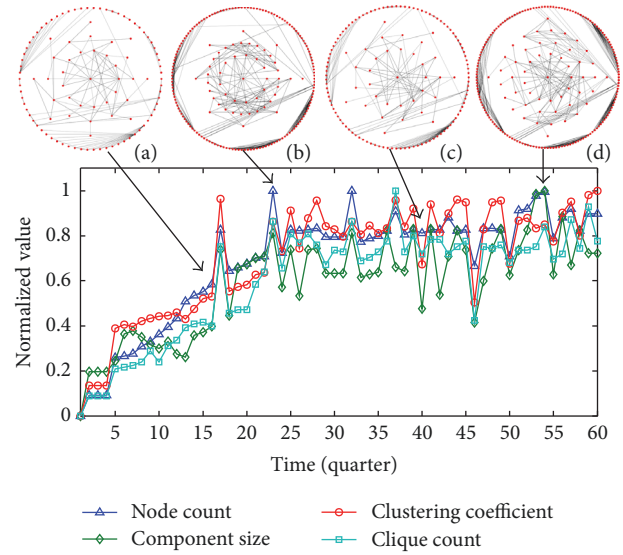

Figure 4: Trends of the extracted features of Al-Qaeda networks. The four measures are normalized within [0, 1]. (a), (b), (c), and (d) are examples of network snapshots with IDs of GN_{16}, GN_{23}, GN_{40}, and GN_{54}, while $GB_{16} = 0$, $GB_{23} = 1$, $GB_{40} = 0$, and $GB_{54} = 1$.

Unexpectedly, the four measures are significantly higher in networks with *Attack behaviors*, relative to networks with *Normal behaviors* (p *value* < 0.05). From Figures 4 and 5 and Table 2, we can infer that when *Attack behaviors* happen, the extracted relevant features of Al-Qaeda networks will have some visible differences. We find that the measured differences between the two classes are statistically significant. This finding provides evidence regarding the rationality of the extracted measures.

6.2.2. Measure Prediction

(1) Qualitative Inference. As mentioned in Section 4.1, the qualitative inference of the extracted measures is implemented based on wavelet transform. First, we need

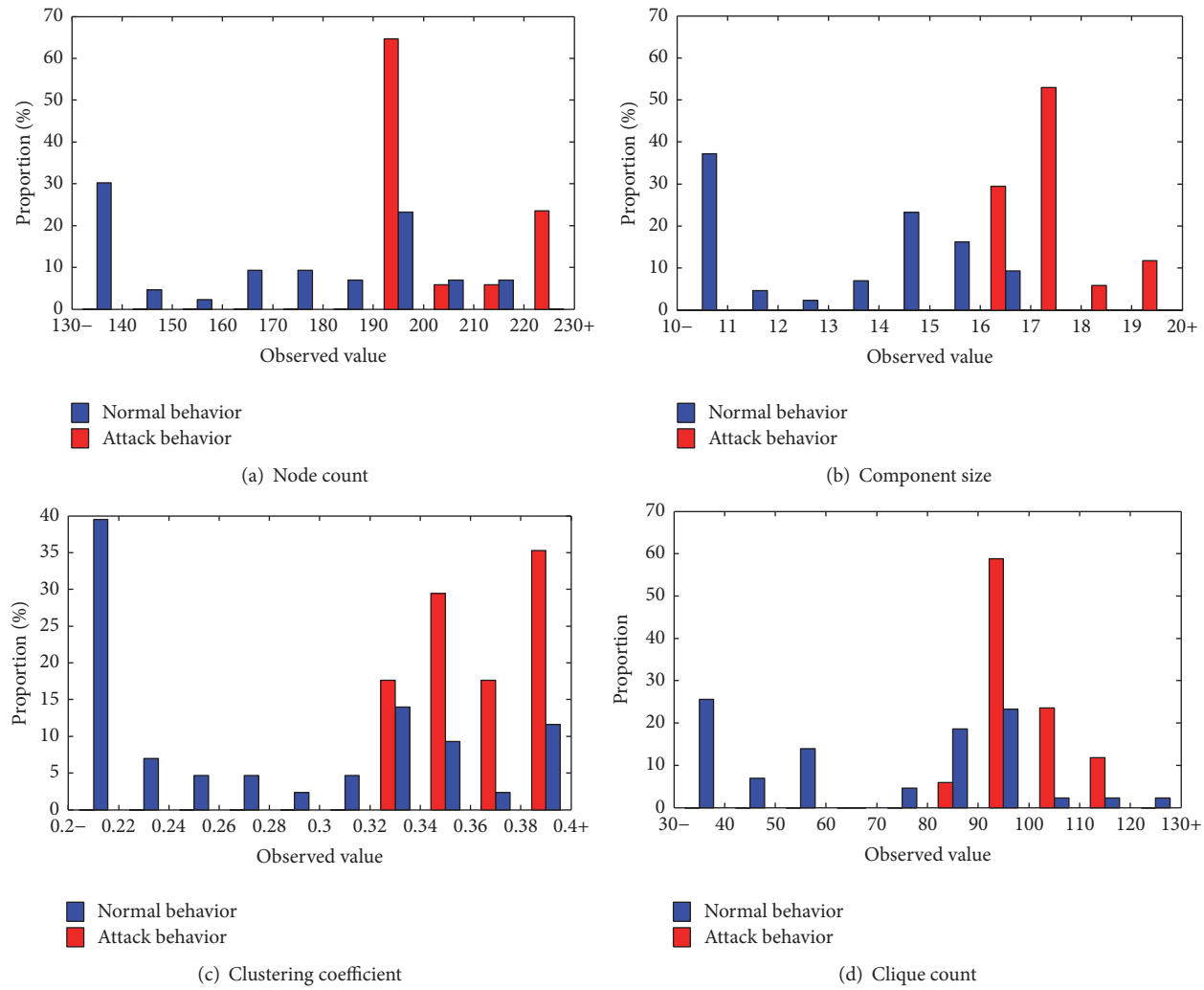

Figure 5: Distributions of the select measures of Al-Qaeda network.

to evaluate the presence and evolution of various periodicities from three aspects: wavelet transform coefficients (Figures 6(a)(1)–6(a)(4)), wavelet power spectrum (Figures 6(b)(1)–6(b)(4)), and wavelet variance (Figures 6(c)(1)–6(c)(4)).

We take the *Node count* as an example. First, from the high and low pattern of measures at different time-scales in the time-frequency structure of the wavelet coefficient in Figure 6(a)(1), it is clear that the *Node count* has significant periodic features. The contours in Figure 6(a)(1) provide information about the levels of the wavelet transform coefficient, with each one corresponding to a variation for different time periods [38]. We find that the upper contours are sparse, while the lower contours are dense, which means at the large time-scales, the range of the corresponding period is larger than that at the smaller ones. Periodic changes in Figure 6(a)(1) indicate that there are multiple time-scale characteristics of the time series of the *Node count*. At the time-scale approximately $22q$ (quarter), there are four and a half "low-high" cycles from T_1 to T_{60}. This period lasts for the entire time domain. At approximately $12q$, there are three "high-low" cycles only in the time domain T_{16}–T_{28} and T_{53}–T_{58}. At approximately $8q$, several "high-low" cycles occur only in the time domain T_{23}–T_{53}. Hence, three are three periodic variations of the *Node count*, where one of them is in a global period and the other two are in local periods.

Second, Figure 6(b)(1) of the wavelet power spectrum illustrates the oscillation power of the time series at different time-scales. From this figure, we find that at approximately $22q$, the power of the time series is the strongest, and the periodic feature is the most significant. The power at approximately $12q$ comes in second place, and its period is median significant, followed by $8q$.

Third, the main periods could be determined by wavelet variance using the corresponding peak values in Figure 6(c)(1). From the figure, we can conclude that the period at the $22q$ time-scale is the first significant period (or large-scale period) as it corresponds to the highest peak, denoted as P_1; the period at the $8q$ time-scale is the second significant period, denoted as P_2; and the period at the $8q$ time-scale is the third significant period, denoted as P_3. Both the P_2 and P_3 periods are small-scale periods.

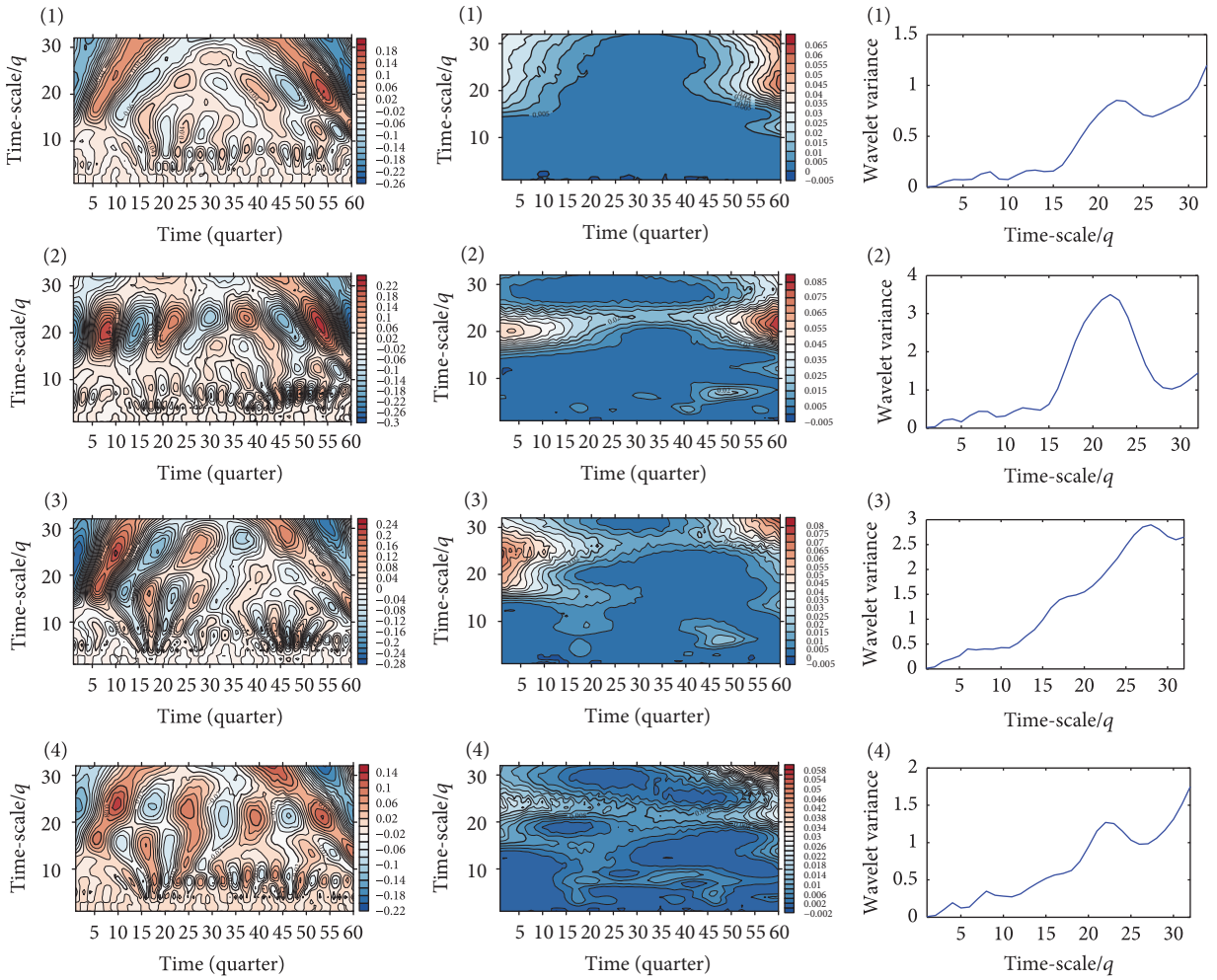

FIGURE 6: Time-frequency structures of wavelet transform coefficient (a), wavelet power spectrum (b), and wavelet variance (c) of the four select measures ((1) *Node count*, (2) *Component size*, (3) *Clustering coefficient*, and (4) *Clique count*). The blue areas in (a) and (b) correspond to negative wavelet transform coefficients, while red areas show regions with positive wavelet transform coefficients.

Finally, the wavelet transform coefficient curves at the three time-scales are shown in Figure 7(a). From Figure 7(a), we find that the average time of each period of P_1, P_2, and P_3 is 8, 6, and 3 quarters, respectively. With the same mechanism, the main periods and the average time period of the remaining three measures can be obtained, as shown in Figures 6 and 7 and Table 3.

With the periodic feature captured, the future trends of the extracted measures after T_{60} can subsequently be inferred qualitatively. The large-scale period P_1 in Table 3 and Figure 7 is used to characterize the future trends. In Figure 7, the positive or negative wavelet coefficients reveal the high and low values of measures in the time domain. Here, we also take *Node count* as an example. The wavelet coefficient of the *Node count* in T_{60} is located in a low period with an upward tendency, so the trend in subsequent timestamps will stay relatively low, before reverting to a high period in T_{64}. In contrast, For the P_2 period, as the corresponding wavelet coefficients in T_{60} are located in a high period with an upward tendency before T_{61}, they will then turn toward a downward tendency. The P_3 period is not considered as it only lasted for T_{23}–T_{53}. Hence, the *Node count* trend in the subsequent four timestamps (T_{61}–T_{64}) will be relatively low with weak oscillation. The trends of the remaining three measures can also be inferred similarly. The results are shown in Table 3.

(2) Quantitative Prediction. WNN is then used to predict the future values of the four measures from the quantitative perspective. First, the best architecture of WNN should be observed. For the input layer, various numbers of nodes are checked in the input layer to identify the best one. As is shown in Figure 8, the number of nodes in the input layer, which leads to the lowest RMSE value, is chosen as the optimal one. As seen from this figure, when the number of nodes in the input layer of the *Node count* is 4, WNN yields the best results. In other words, the number of input variables in WNN for the *Node count* prediction is $M_j^1 = (m_{j-1}^1, m_{j-2}^1, m_{j-3}^1, m_{j-4}^1)$; that

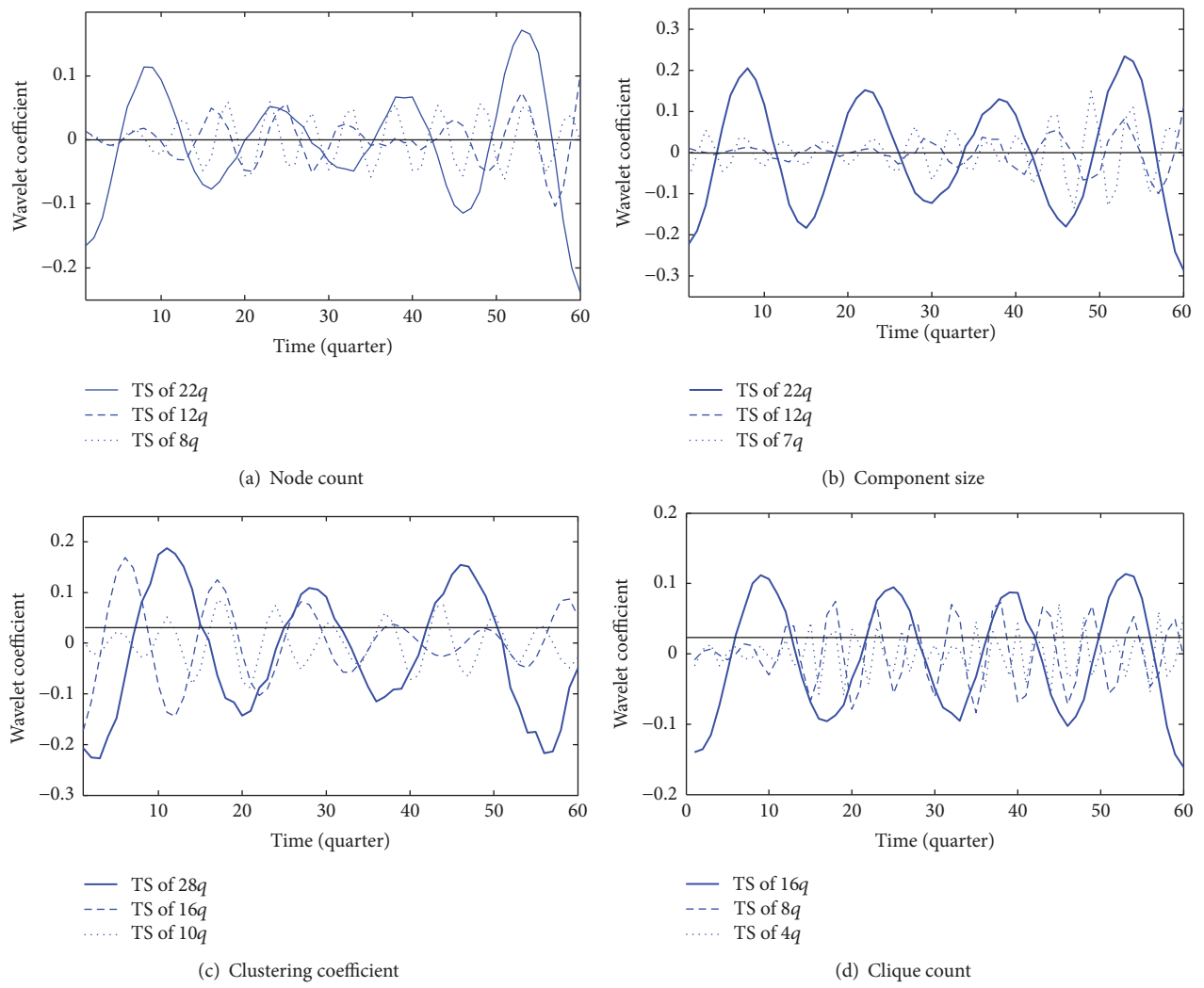

Figure 7: Wavelet transform coefficients of four measures at different time-scales.

Table 3: Main periods and trend inference of the four measures.

Select measures	Main period time Time-scale/average period time (quarter)			Trend inference			
	$P_1{}^*$	P_2	P_3	T_{61}	T_{62}	T_{63}	T_{64}
Node count	22/15	12/7.5	8/5	L	L	L	L
Component size	22/15	12/7.5	7/4.6	L	L	L	L
Clustering coefficient	28/18.5	16/10	10/6.3	L	L	H	H
Clique count	22/15	8/5	4/3	L	L	L	L

L and H denote low and high trends, and $*$ denotes large-scale period.

is, the values of the past 4 timestamps are used in the time-series prediction. Moreover, for the hidden layer, the number of the nodes should also be appropriate—if the number is too small, WNN may not reflect the complex function relationship between input data and output value; on the contrary, a large number may create such a complex network that might lead to an output error caused by overfitting of the training sample set [39]. After several trials, the suitable nodes in the hidden layer are set as 6. Thus, the architecture of WNN for the *Node count* is "4-6-1." Using the same method, the architectures of *Component size*, *Clustering coefficient*, and *Clique count* are also determined.

Second, to verify the superiority of our method, we apply the baseline methods to the same data to compare the results. We have the data divided into training and test samples. The data of the four measures include 60 timestamps (T_1–T_{60}). From these, 40 data timestamps are used for training for all the methods, and the remaining 20 data timestamps are

Table 4: Comparison of prediction results of different models.

Criteria	Prediction models						
	WNN	BP	ARIMA	GABP	ANFIS	SVR	RBF
MAE							
Node count	7.722	7.773	9.313	8.407	8.314	8.157	8.246
Component size	0.836	1.348	1.487	1.189	0.854	0.875	1.171
Clustering coefficient	0.019	0.025	0.028	0.018	0.033	0.022	0.026
Clique count	4.887	5.066	6.300	5.231	6.580	6.012	6.313
RMSE							
Node count	10.377	10.187	12.376	10.991	12.152	10.198	13.475
Component size	1.537	1.733	1.945	1.552	1.436	1.385	1.435
Clustering coefficient	0.026	0.035	0.038	0.028	0.044	0.028	0.030
Clique count	8.133	8.777	7.713	8.294	9.167	9.631	9.656

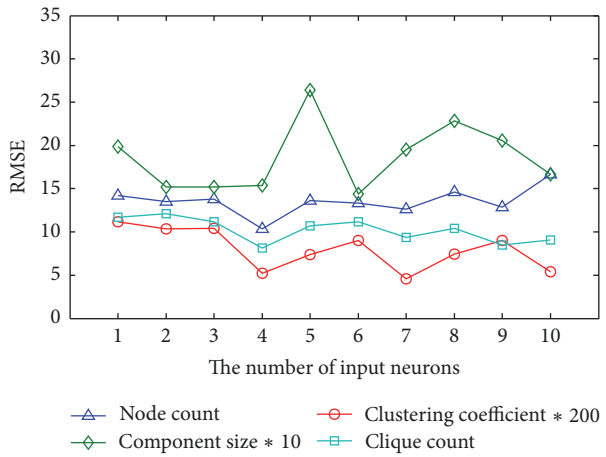

Figure 8: Dependence of RMSE on the number of neurons in the input layer.

used as the test dataset. After running 100 times with WNN and baseline methods, the average values of the prediction results are obtained. The MAE and RMSE of the models are presented in Table 4. We have several interesting observations which confirm our research motivation. First, the MAEs of WNN are lower than most of those of the baseline methods. Second, some baseline methods perform somehow better in RMSE. However, through a comprehensive comparison with the four measures, we find that the WNN still performs the best in RMSE. Finally, given the excellent performance of WNN in Table 4, we are convinced that the ANN with wavelet transform (WNN) has the best fitting capacity and the strongest capacity of time-series prediction in terrorist networks with nonlinear and multiple time-scale characteristics.

As the WNN has the best prediction performance, we then apply the WNN to quantitatively predict the measures in the subsequent four timestamps. We run the trained WNN 100 times, and the box plots in Figure 9 show the prediction results of the four measures with WNN.

Finally, we have the predictive future networks mutually checked by both qualitative inference and quantitative prediction. From Figure 9, we observe that the prediction values of the four measures by WNN are consistent with the trend we inferred qualitatively in Table 3. The actual values of *Node count*, *Component size*, *Clustering coefficient*, and *Clique count* in T_{60} are 209, 16.8, 0.41, and 97, respectively. The values of *Node count*, *Component size*, and *Clique count* in the following four timestamps are also located in a relatively low position and have weak oscillations. Meanwhile, the values of the *Clustering coefficients* in the following two timestamps are located in a relatively low position and then turn to a high position in the next two timestamps. Thus, we have mutually checked the predicted trends from the two aspects of qualitative inference (Table 3) and quantitative prediction (Figure 9).

6.3. Behavior Pattern Recognition. With the measures predicted, the next step is to recognize group behavior patterns and estimate the risk of attack in the future. The combined values of the predicted values of the extracted four measures are imported into SVM. Apply function (1); the future behavior of Al-Qaeda group is recognized. After running 100 times, the risk of terrorist attack in the subsequent timestamps is estimated with function (8), as is shown in Figure 10. Risk levels are categorized based on high ($R = 0.8$), medium ($R = 0.6$), and general ($R = 0.4$) thresholds. Then T_{61} and T_{64} are regarded as having high risk and larger probability of *Attack behavior* of Al-Qaeda than the rest of the timestamps; T_{62} is regarded as having the median risk of terrorist attack, while T_{63} is regarded as having a general risk of terrorist attack.

6.4. Discussion. The empirical study of the Al-Qaeda group shows that the proposed wavelet transform-based pattern recognition framework is of high accuracy and practical value in predicting the *Attack behavior* of terrorist groups.

The results show that Al-Qaeda networks with *Attack behaviors* have structure patterns that are different from those with *Normal behaviors* (Figures 4 and 5 and Table 2). We can infer that when *Attack behaviors* happen, the extracted relevant features of Al-Qaeda networks will have some visible differences. For instance, when the group carries out a terrorist attack, the scale of interaction between members will increase (Figure 4). As a result, the total number of *nodes* will grow and the *Component size* and *Clique count* will

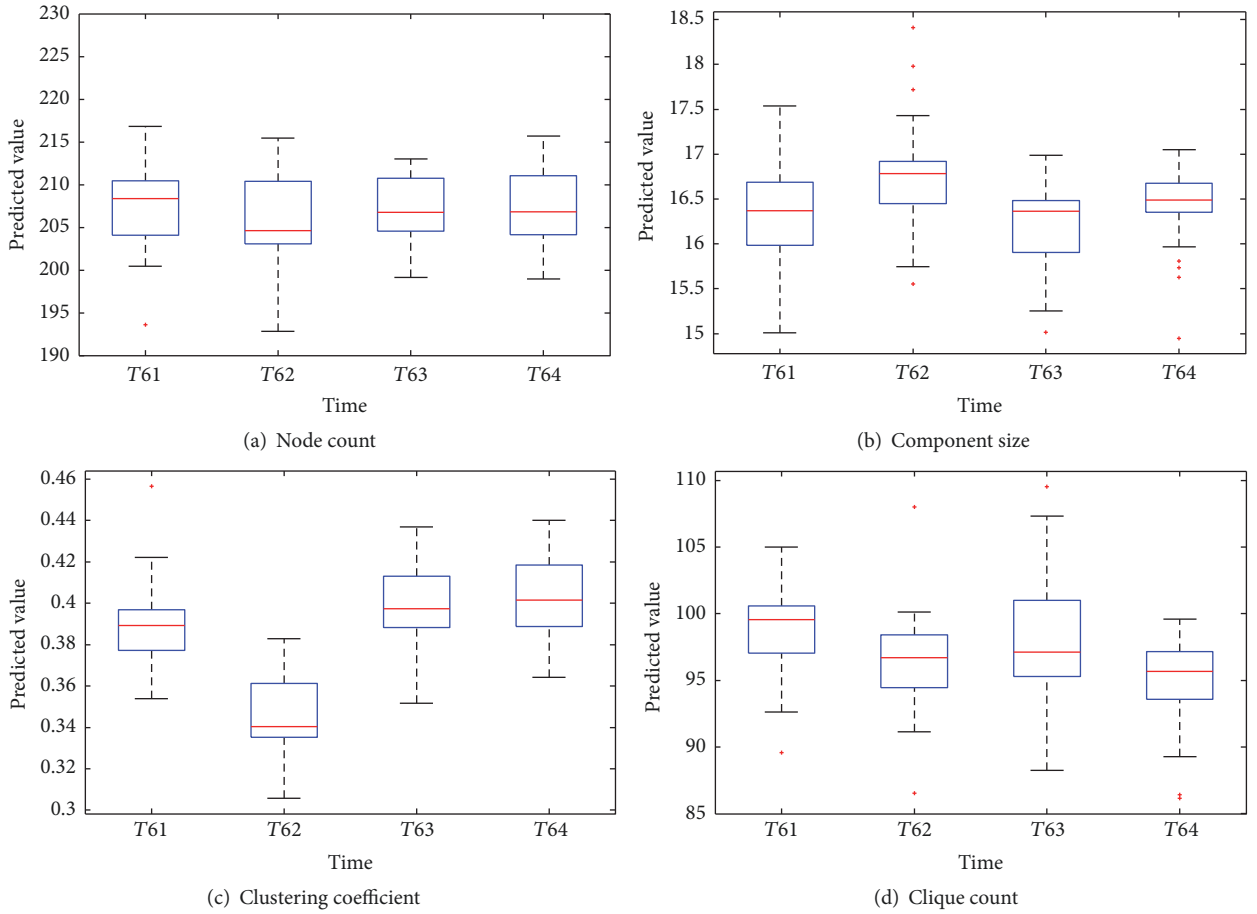

Figure 9: Prediction results of four measures by WNN for the subsequent four timestamps.

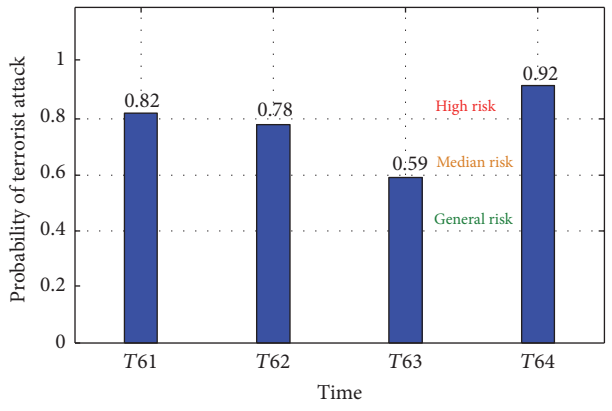

Figure 10: The risk of *Attack behavior* of the Al-Qaeda group in the subsequent timestamps.

also increase (Figure 5 and Table 2). We can also infer that when *Attack behaviors* happen, the local information diffuses faster, and the terrorists are likely sharing information and receiving intelligence from the communicators with a more decentralized infrastructure. In summary, the frequency and proportion of measures increase when *Attack behavior* happens. These observations verify the basics of this study; that is, a correlation exists between the social networks and events of Al-Qaeda. The four measures and their differences are potentially useful for recognizing the behavior patterns of Al-Qaeda.

The results also show that measures of the Al-Qaeda network share similar features with some natural phenomena in periodicity and that the wavelet transform-based method can recognize the periodicity effectively. Wavelet transform can identify the main periods of the time series from different time-scales (Figures 6 and 7). The nonlinear and nonstationary dynamic processes of terrorist group network measures are decomposed into quasi-stationary by multiscale characteristics by wavelet transform. Based on the periodic analysis, future trends (upward or downward trend) can be inferred from the qualitative aspect. On the other hand, WNN can quantitatively predict the future trends based on the wavelet transform. The results show that WNN can address the time-series prediction problem with a strong nonlinear approximation ability after being well trained with historical data (Table 4 and Figure 9). The results suggest that wavelet transform with periodic and prediction components is a meaningful approach and tool in the prediction for terrorist networks. The power of this kind of analysis lies in the fact that the quantitative analysis along with qualitative inference can provide more faithful results than empirical

Table 5: Time complexities for each technique.

Techniques	Time complexity
Social network analysis	
Node count	$O(n)$
Component size	$O(n)$
Clustering coefficient	$O(n^2)$
Clique count	$O(3^{n/3})$
Wavelet transform	
CWT	$O(n)$
WNN	$O(n^2)$
SVM	$O(n^3)$

or qualitative analysis. Moreover, with predicted measures and SVM, the behavior pattern recognition can provide a quantitative estimation of future risk (Figure 10). In summary, with the proposed framework, we can monitor the dynamics and further predict the *Attack behavior* of terrorist groups with high accuracy and efficiency.

By glancing at the framework in Figure 2, one might initially guess that the computational complexity would be relatively high since it involves many techniques, such as SNA, wavelet transform methods, and SVM. However, the feature extraction, measure prediction, and behavior recognition phases are implemented sequentially one after the other. To be clear, the time complexities for each technique are summarized in Table 5 [47, 48]. Fortunately, the networks of terrorist groups have not reached the level of complex networks. Assume there are m edges and n nodes. The range of n is generally between 1 and 1000, with an average size of 840 [49]. Moreover, the core networks are even smaller [50, 51], with a range of nodes between 43 and 228 in our study. The Al-Qaeda networks are also sparse networks with $m = kn$ and $k \leq 5$. Thus, the total complexity for predicting terrorist group behavior by our wavelet transform-based pattern recognition is within acceptable range.

The Al-Qaeda study suggests that our proposed framework is able to perform well even when the information is incomplete. In general, one challenge in terrorism studies is that it lacks terrorist data in depth due to confidentiality, and some data just do not exist. In our study, the Al-Qaeda data are collected from open source, and inevitably, they are incomplete representations of the relationships in the real-world terrorist group. The limitations of the terrorist data make it difficult to predict the behaviors because we cannot be sure that we included all communication and cooperation networks. However, even using this dataset, we are able to systematically predict the networks and behaviors, which highlights the value of the proposed models.

7. Conclusions

The steep rise in global terror necessitates deeper scientific understanding of the terrorist group and its behavior. Nowadays, preventing terrorist attacks before they happen is extremely important in counterterrorism. Governments need to understand how terrorist groups behave with terrorist attack in the future. In this paper, we proposed and applied a wavelet transform-based pattern recognition framework to investigate the dynamics and eventually predict the *Attack behavior* of terrorist group.

Specifically, the terrorist group is first modeled as social networks, and the relevant measures are extracted with the proposed criteria. Second, a wavelet transform-based prediction method is established to predict the extracted measures. Next, the *Attack behavior* of the group is recognized by behavior pattern recognition with SVM. Empirical research of Al-Qaeda data demonstrates that the proposed framework is a meaningful approach and tool in the prediction of terrorist group behavior.

In summary, we make the following contributions in this paper. (1) We analyze the dynamic characteristics of the terrorist group from two aspects: the periodicity of a group network and the correlation between the behavior and the network. (2) We design an effective wavelet transform-based pattern recognition framework that combines SNA, wavelet transform methods, and the pattern recognition approach to predict the *Attack behavior* of the terrorist group. (3) We propose a novel network prediction method with wavelet transform from two aspects: period analysis-based qualitative inference and WNN-based quantitative prediction. To our knowledge, this may be the first study to apply the theory of wavelet transform as associated with terrorist behaviors.

In light of the results and discussion presented up to now, the proposed framework enables us to derive several conclusions. (1) The terrorist networks have shown some periodic features during the dynamic process, and the features can be used to predict the future behaviors based on the correlation between the network and behavior. (2) The prediction framework we proposed performs well with the periodicity and correlation considered. (3) Wavelet transform-based prediction methods can effectively predict the networks of terrorist group from both the qualitative and quantitative aspects.

In conclusion, this study helps to elucidate the dynamics of terrorist groups using a wavelet transform-based pattern recognition framework. Such a framework tightly integrates the group network and behavior with respect to both the network prediction and behavior recognition dimensions. The approach used in this study provides analysts with greater analytical power and facilitates assessing dynamic, complex, and nonlinear sociotechnical systems. This paper also provides an effective method for predicting collective behavior in other extreme incidents, emergency, and security study domains. Overall, predicting terrorism is so challenging that the added mathematical methods are likely to enhance our understanding of the dynamic characteristics of its behaviors.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research is supported by the National Natural Science Foundation of China, nos. 71473263 and 71704184.

References

[1] M. Sageman, *Understanding Terror Networks*, University of Pennsylvania Press, 2004.

[2] A. Sliva, V. S. Subrahmanian, V. Martinez, and G. Simari, "CAPE: Automatically predicting changes in group behavior," *Mathematical Methods in Counterterrorism*, pp. 253–269, 2009.

[3] B. Li, D. Sun, R. Zhu, and Z. Li, "Agent based modeling on organizational dynamics of terrorist network," *Discrete Dynamics in Nature and Society*, vol. 2015, Article ID 237809, 2015.

[4] K. M. Carley, "A dynamic network approach to the assessment of terrorist groups and the impact of alternative courses of action," 2006, DTIC Document.

[5] B. Li, D. Sun, S. Guo, and Z. Lin, "Agent based simulation of group emotions evolution and strategy intervention in extreme events," *Discrete Dynamics in Nature and Society*, vol. 2014, Article ID 464190, 2014.

[6] I. McCulloh and K. M. Carley, "Detecting change in longitudinal social networks," 2011, DTIC Document.

[7] A. B. Krueger and J. Malečková, "Attitudes and action: public opinion and the occurrence of international terrorism," *Science*, vol. 325, no. 5947, pp. 1534–1536, 2009.

[8] W. Enders and T. Sandler, "Is transnational terrorism becoming more threatening? A time-series investigation," *Journal of Conflict Resolution*, vol. 44, no. 3, pp. 307–332, 2000.

[9] V. Raghavan, A. Galstyan, and A. G. Tartakovsky, "Hidden Markov models for the activity profile of terrorist groups," *The Annals of Applied Statistics*, vol. 7, no. 4, pp. 2402–2430, 2013.

[10] V. S. Subrahmanian, A. Mannes, A. Sliva, J. Shakarian, and J. P. Dickerson, *Computational Analysis of Terrorist Groups: Lashkar-e-Taiba*, Springer Science and Business Media, 2012.

[11] V. Subrahmanian, A. Mannes, A. Roul, and R. Raghavan, *Indian Mujahideen: Computational Analysis and Public Policy*, Springer Science and Business Media, 2013.

[12] A. Najgebauer, R. Antkiewicz, M. Chmielewski, and R. Kasprzak, "The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution," *Journal of Telecommunications and Information Technology*, pp. 14–20, 2008.

[13] A. Xue, W. Wang, and M. Zhang, "Terrorist organization behavior prediction algorithm based on context subspace," *Advanced Data Mining and Applications*, pp. 332–345, 2011.

[14] S. Tutun, M. T. Khasawneh, and J. Zhuang, "New framework that uses patterns and relations to understand terrorist behaviors," *Expert Systems with Applications*, vol. 78, pp. 358–375, 2017.

[15] P. V. Bindu, P. S. Thilagam, and D. Ahuja, "Discovering suspicious behavior in multilayer social networks," *Computers in Human Behavior*, vol. 73, pp. 568–582, 2017.

[16] I. A. McCulloh and K. M. Carley, *Defense Technical Information Center*, 2008.

[17] Z. Li, D. Sun, R. Zhu, Z. Lin, and Y. Deng, "Detecting event-related changes in organizational networks using optimized neural network models," *PLoS ONE*, vol. 12, no. 11, p. e0188733, 2017.

[18] D. Kasthurirathna, M. Piraveenan, and M. Harré, "Influence of topology in the evolution of coordination in complex networks under information diffusion constraints," *The European Physical Journal B*, vol. 87, no. 1, article no. 3, 2014.

[19] A. Anzo and J. Barajas-Ramirez, "Synchronization in complex networks under structural evolution," *Journal of The Franklin Institute*, vol. 351, no. 1, pp. 358–372, 2014.

[20] D. McDaniel and G. Schaefer, "A data fusion approach to indications and warnings of terrorist attacks," in *Proceedings of the Next-Generation Analyst II*, May 2014.

[21] A. Clauset and K. S. Gleditsch, "The developmental dynamics of terrorist organizations," *PLoS ONE*, vol. 7, no. 11, Article ID e48633, 2012.

[22] B. A. Desmarais and S. J. Cranmer, "Forecasting the locational dynamics of transnational terrorism: A network analytic approach," in *Proceedings of the 2011 1st European Intelligence and Security Informatics Conference, EISIC 2011*, pp. 171–177, Greece, September 2011.

[23] S. Koschade, "A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence," *Studies in Conflict and Terrorism*, vol. 29, no. 6, pp. 559–575, 2006.

[24] B. Zhan and R. Han, "Model based on hidden Markov model for predicting terrorism accident," *journal of Pla University of Science & Technology*, vol. 16, no. 4, pp. 385–393, 2015.

[25] P. V. Fellman and R. Wright, "Modeling terrorist networks, complex systems at the mid-range," https://arxiv.org/abs/1405.6989v1.

[26] Editorial, "Understanding and countering terrorism," *Nature Human Behaviour*, vol. 1, p. 134, 2017.

[27] P. J. Phillips, "The Life Cycle of Terrorist Organisations," *Social Science Electronic Publishing*, vol. 17, no. 4, pp. 369–385, 2010.

[28] W. Enders, G. F. Parise, and T. Sandler, "A A time-series analysis of transnational terrorism: Trends and cycles," *Defence and Peace Economics*, vol. 3, no. 4, pp. 305–320, 1992.

[29] K. K. Minu, M. C. Lineesh, and C. Jessy John, "Wavelet neural networks for nonlinear time series analysis," *Applied Mathematical Sciences*, vol. 4, no. 49-52, pp. 2485–2495, 2010.

[30] M. A. Ruiz Estrada and E. Koutronas, "Terrorist attack assessment: Paris November 2015 and Brussels March 2016," *Journal of Policy Modeling*, vol. 38, no. 3, pp. 553–571, 2016.

[31] T. Sandler, "New frontiers of terrorism research: An introduction," *Journal of Peace Research*, vol. 48, no. 3, pp. 279–286, 2011.

[32] G. LaFree, L. Dugan, M. Xie, and P. Singh, "Spatial and Temporal Patterns of Terrorist Attacks by ETA 1970 to 2007," *Journal of Quantitative Criminology*, vol. 28, no. 1, pp. 7–29, 2012.

[33] M. Crenshaw, "The logic of terrorism: Terrorist behavior as a product of strategic choice," in *Proceedings of the National Academy of Sciences of the United States of America*, vol. 98, pp. 15056–15061, 1998.

[34] T. Sandler and D. G. M. Arce, "Terrorism & game theory," *Simulation & Gaming*, vol. 34, no. 3, pp. 319–337, 2003.

[35] L. Peel and A. Clauset, *Detecting change points in the large-scale structure of evolving networks*.

[36] K. M. Carley, *Dynamic Network Analysis*, Alphascript Publishing, 2013.

[37] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Computation*, vol. 13, no. 7, pp. 1443–1471, 2001.

[38] S. Gao and Q. Wu, "Period analysis and trend forecast for soil temperature in the Qinghai-Xizang Highway by wavelet transformation," *Environmental Earth Sciences*, vol. 74, no. 4, pp. 2883–2891, 2015.

[39] H. Esen, F. Ozgen, M. Esen, and A. Sengur, "Artificial neural network and wavelet neural network approaches for modelling of a solar air heater," *Expert Systems with Applications*, vol. 36, no. 8, pp. 11240–11248, 2009.

[40] M. Farge, "Wavelet transforms and their applications to turbulence," *Annual Review of Fluid Mechanics*, vol. 24, no. 1, pp. 395–457, 1992.

[41] C. Torrence and G. P. Compo, "A practical guide to wavelet analysis," *Bulletin of the American Meteorological Society*, vol. 79, no. 1, pp. 61–78, 1998.

[42] Q. Zhang and A. Benveniste, "Wavelet networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 3, no. 6, pp. 889–898, 1992.

[43] P. Kumar, P. Radha Krishna, and S. Bapi Raju, "Pattern discovery using sequence data mining: Applications and studies," *Pattern Discovery Using Sequence Data Mining: Applications and Studies*, pp. 1–273, 2011.

[44] N. Lesh, M. J. Zaki, and M. Ogihara, *Mining Features for Sequence Classification*, 342–346.

[45] S. Nedeltchev and A. Shaikh, "A new method for identification of the main transition velocities in multiphase reactors based on information entropy theory," *Chemical Engineering Science*, vol. 100, pp. 2–14, 2013.

[46] John Jay and ARTIS., "ARTIS Transnational Terrorism Database," http://doitapps.jjay.cuny.edu/jjatt/data.php.

[47] E. Tomita, A. Tanaka, and H. Takahashi, "The worst-case time complexity for generating all maximal cliques and computational experiments," *Theoretical Computer Science*, vol. 363, no. 1, pp. 28–42, 2006.

[48] I. W. Tsang, J. T. Kwok, and P.-M. Cheung, "Core vector machines: fast SVM training on very large data sets," *Journal of Machine Learning Research*, vol. 6, pp. 363–392, 2005.

[49] S. B. Blomberg, K. Gaibulloev, and T. Sandler, "Terrorist group survival: Ideology, tactics, and base of operations," *Public Choice*, vol. 149, no. 3, pp. 441–463, 2011.

[50] R. Medina and G. Hepner, *Geospatial Analysis of Dynamic Terrorist Networks*, Springer, Netherlands, 2008.

[51] M. L. Ouellet, *Terrorist Networks and the Collective Criminal Career: The Relationship between Group Structure and Trajectories [Ph.D.thesis]*, Arts & Social Sciences: School of Criminology, 2016.