Int. J. Appl. Math. Comput. Sci., 2019, Vol. 29, No. 2, 363–373
DOI: 10.2478/amcs-2019-0027

LYAPUNOV–BASED ANOMALY DETECTION IN PREFERENTIAL ATTACHMENT NETWORKS

DIEGO RUIZ [a,b,*], JORGE FINKE [c]

[a]Department of Mathematics
University of Cauca, Calle 5 # 4-70, Popayán, Colombia
e-mail: dfruiz@unicauca.edu.co

[b]School of Systems Engineering and Computer Science
University of Valle, Calle 13 # 100-00, Cali, Colombia
e-mail: ruiz.diego@correounivalle.edu.co

[c]Department of Electrical Engineering and Computer Science
Pontifical Xavierian University, Calle 18 # 118-250, Cali, Colombia
e-mail: finke@ieee.org

Network models aim to explain patterns of empirical relationships based on mechanisms that operate under various principles for establishing and removing links. The principle of preferential attachment forms a basis for the well-known Barabási–Albert model, which describes a stochastic preferential attachment process where newly added nodes tend to connect to the more highly connected ones. Previous work has shown that a wide class of such models are able to recreate power law degree distributions. This paper characterizes the cumulative degree distribution of the Barabási–Albert model as an invariant set and shows that this set is not only a global attractor, but it is also stable in the sense of Lyapunov. Stability in this context means that, for all initial configurations, the cumulative degree distributions of subsequent networks remain, for all time, close to the limit distribution. We use the stability properties of the distribution to design a semi-supervised technique for the problem of anomalous event detection on networks.

Keywords: network formation models, discrete event systems, stability, anomalous event detection.

1. Introduction

The problem of detecting anomalous events on networks is of increasing interest for developing large-scale applications on distributed platforms. Approaches range from monitoring changes in network topology to defining detection signatures (Chandola *et al.*, 2009; Gogoi *et al.*, 2011; Savage *et al.*, 2014; Ranshous *et al.*, 2015; Yu *et al.*, 2016) based on spectral (Hirose *et al.*, 2009), information (Host-Madsen and Zhang, 2018) and distance measures (Shoubridge *et al.*, 2002; Koutra *et al.*, 2016). In the work of Koutra *et al.* (2016), for example, anomalies are detected based on similarity functions that capture a measure of affinity between nodes. Despite the numerous approaches to detect network anomalies, none of them makes use of a stability analysis of topological properties. In general, little attention has been paid to designing algorithms based on formal criteria derived from dynamic network models; yet such model-based approaches enable us to evaluate the performance of anomalous event detection algorithms under the effects of topological variations.

A common approach in modeling networks has been to characterize the evolution of topological properties as an outcome of stochastic mechanisms (Barabási and Albert, 1999; Caldarelli *et al.*, 2002; Shao *et al.*, 2006; Moriano and Finke, 2012; Choromanski *et al.*, 2013). These mechanisms define how nodes tend to establish and remove links, giving rise to particular measures or measure distributions (Bianconi and Barabási, 2001; Chen and Shi, 2004; Jackson and Rogers, 2007; Tong *et al.*, 2009). The Barabási–Albert (BA) model uses a linear preferential attachment mechanism to generate networks

*Corresponding author

in which the probability that a node (selected uniformly at random) has a degree equal to k is proportional to k^{-3}. That is, for a random variable K that characterizes the degree of a randomly selected node, the limit distribution of K satisfies a power law. In particular, $P[K = k] \propto k^{-3}$ indicates high heterogeneity in the degree of nodes of the BA model.

There exist important relationships between the degree and other centrality measures (Lee, 2006; Valente *et al*., 2008; Kudělka *et al*., 2015). Lee (2006) identifies a strong correlation between the centralities of degree and betweenness in empirical networks. Similarly, Valente *et al*. (2008) show that the centralities of degree and eigenvector are strongly correlated. Despite growing efforts to define such relationships, addressing the challenge of how to detect anomalous events based on analytical properties of centrality measures requires the development of a framework that explains (i) how centrality measures emerge from particular mechanisms and (ii) how they evolve under constantly acting perturbations (e.g., edge perturbations).

Recent efforts have focused on the effect of edge perturbations in static models. In particular, Segarra and Ribeiro (2016) evaluate the condition of Lipschitz continuity for different centrality measures. If a centrality measure is Lipschitz continuous, then the addition or removal of an edge results in a bounded variation in that measure. For betweenness centrality, for example, this condition is not satisfied, so small perturbations can lead to unbounded differences in the betweenness measure of a node. Characterizing how a network responds to perturbations over time requires a dynamic model which enables us to benchmark the effects of adding or removing edges on particular measures and measure distributions.

This paper studies the response of the Lipschitz continuous measure of degree centrality to edge perturbations using the notion of stability in the sense of Lyapunov. A perturbation represents a deviation, but a plausible outcome, from an invariant measure in the *process* of establishing edges; an anomaly indicates an outcome that cannot be explained by the model. Stability of the invariant, a set of states representing the probability distribution function of the degree centrality, implies that small perturbations from that set must remain small for all time. The stability analysis enables us to introduce a new approach to the problem of detecting anomalies on networks.

The contribution of our work is twofold. First, we characterize stability properties of the degree distribution of the BA model. In particular, we show that the invariant set of the limit behavior of the complementary cumulative degree distribution is not only a global attractor, but is also stable in the sense of Lyapunov (i.e., asymptotically stable). To our knowledge, there are no previous studies that describe the stability properties of the degree distribution of the BA model. Second, we apply the stability results to the problem of identifying the instances at which network anomalies occur (i.e., outcomes that cannot be explained by the BA model). An anomaly is reported whenever the evolution of the average degree of the network contradicts the properties of the Lyapunov function (Ruiz and Finke, 2013).

The remainder of this paper is organized as follows. Section 2 reviews some properties of the degree distribution of the BA model which are needed to define the invariant set. Section 3 presents the stability result. Section 4 introduces three types of anomalous events, each representing different types of anomalies. It also defines conditions under which each type of event is detected. Section 5 presents simulation results that illustrate the evolution of the network and the performance of the detection algorithm, and compares the performance of the proposed algorithm with the approach of Koutra *et al*. (2016). Finally, Section 6 draws some conclusions and future research directions.

2. Barabási–Albert model

At time t, consider an undirected network $\mathcal{G}_t = (V_t, E_t)$ with a set of nodes V_t and a set of edges E_t. Let K denote a random variable that characterizes the degree of a randomly selected node. Moreover, $p(k) = P[K = k]$ denotes the probability that K equals k. In some cases, we characterize the probability that K is less than k, which is denoted by $F(k) = P[K < k] = \sum_{x<k} p(x)$. The complementary cumulative distribution is denoted by $\bar{F}(k) = P[K \geq k] = 1 - F(k)$. Let $p_t(k)$ specify the probability $p(k)$ at time t (similarly, $F_t(k) = P[K_t < k]$ and $\bar{F}_t(k) = P[K_t \geq k]$ refer to the cumulative distributions at a particular time t). Finally, let $k(u)$ denote the degree of a node u, $d_0 = \sum_{u \in V_0} k(u)$ the total degree of the initial network $\mathcal{G}_0$, and $n_t = |V_t|$ the number of nodes in $\mathcal{G}_t$. Note that $n_t = n_0 + t$.

Starting from a simple network $\mathcal{G}_0$ (i.e., without parallel edges or self-loops), the evolution of $\mathcal{G}_t$ follows two mechanisms (Barabási and Albert, 1999):

M1 *Growth*: A new node with m undirected edges is added to the set of nodes.

M2 *Attachment*: The new node chooses m different nodes, connecting to a node with degree k in V_{t-1} with probability

$$\pi(k) = \frac{k}{\sum_{u \in V_{t-1}} k(u)}. \tag{1}$$

Equation (1) is known as linear preferential attachment. Note that the attachment mechanism depends only on the degree of a node (new nodes tend to connect to the more highly connected ones). Because the initial

network is a simple one, the resulting network is also simple.

To ensure a well-defined formation process, consider the following assumption:

A1 The degree of any node u of the initial network $\mathcal{G}_0$ satisfies $m \leq k(u) \leq d_0/m$.

Assumption A1 imposes bounds on the degree of the nodes of the initial network. In particular, $k(u) \geq m$ implies that $n_0 \geq m$, and $k(u) \leq d_0/m$ that $mk(u) \leq d_0 + 2tm$ for all $t \geq 0$ and any node $u \in V_t$.

Note that $\mathcal{G}_t$ has total degree

$$\sum_{u \in V_t} k(u) = d_0 + 2tm. \tag{2}$$

The second term on the right-hand side of (2) corresponds to the contribution by new nodes, which adds m edges every time. Using (2), the expected degree of a node, selected uniformly at random at time t, is characterized as

$$\mathrm{E}[K_t] = \frac{d_0 + 2tm}{n_t},$$

and, as time approaches infinity,

$$\lim_{t \to \infty} \mathrm{E}[K_t] = 2m. \tag{3}$$

Note that $\mathrm{E}[K_t]$ is strictly increasing if $d_0 < 2mn_0$, strictly decreasing if $d_0 > 2mn_0$, and remains constant if $d_0 = 2mn_0$.

Next, just like Dorogovtsev *et al*. (2000) or Barabási and Pósfai (2016), we present expressions for the expected number of nodes in the network with degree $k \geq m$. These expressions capture how mechanisms M1 and M2 affect nodes with degree k and $k-1$ (either a new node increases the degree of a node with degree k or a new node increases the degree of a node with degree $k-1$). According to (1) and (2), the probability that at time t a new node connects to a node with degree k is

$$m\pi(k) = \frac{mk}{d_0 + 2(t-1)m}. \tag{4}$$

Based on Assumption A1, note that $m\pi(k) \leq 1$. Now, the expected number of nodes with degree k to which a new node establishes an edge at time t is given by $m\pi(k)n_{t-1}p_{t-1}(k)$. Using (4), we have

$$m\pi(k)n_{t-1}p_{t-1}(k) = \frac{mkn_{t-1}p_{t-1}(k)}{d_0 + 2(t-1)m}.$$

Thus the expected number of nodes with degree $k > m$ at time t equals

$$n_t p_t(k) = n_{t-1}p_{t-1}(k) - \frac{mkn_{t-1}p_{t-1}(k)}{d_0 + 2(t-1)m} + \frac{m(k-1)n_{t-1}p_{t-1}(k-1)}{d_0 + 2(t-1)m}. \tag{5}$$

The first term on the right-hand side of (5) corresponds to the expected number of nodes with degree k at time $t-1$. The second and third terms correspond to the expected numbers of nodes with degree k and $k-1$ to which the new node connects.

Since there are no nodes with a degree less than m (i.e., $p_t(k) = 0$ for all $0 < k < m$ and $t \geq 0$), the expected number of nodes with degree $k = m$ at time t equals

$$n_t p_t(m) = n_{t-1}p_{t-1}(m) - \frac{m^2 n_{t-1}p_{t-1}(m)}{d_0 + 2(t-1)m} + 1. \tag{6}$$

The first term on the right-hand side of (6) represents the expected number of nodes with degree m at time $t-1$. The second term corresponds to the expected number of nodes with degree m that connect at time t with the new node. Finally, the third term captures the effect of the node joining the network with degree m.

Using (5) and (6), the following theorem guarantees the convergence of $p_t = (p_t(m), p_t(m+1), \ldots)$ as t approaches infinity.

Theorem 1. *As $t \to \infty$, the limit of p_t exists.*

Proof. Proceeding by induction over k, we show that the limit of $p_t(k)$ exists for all $k \geq m$. Consider the base case $k = m$. Using (6), note that

$$p_t(m) = \frac{n_{t-1}}{n_t}\left(1 - \frac{m^2}{d_0 + 2(t-1)m}\right)p_{t-1}(m) + \frac{1}{n_t}$$

with initial condition $p_0(m)$. By induction, it can be shown that

$$p_t(m) = \frac{d_0 + 2mt}{m(m+2)n_t} + \left(\frac{m(m+2)n_0p_0(m) - d_0}{m(m+2)n_t}\right) \times \left(\frac{\Gamma\left(\frac{d_0}{2m}\right)\Gamma\left(\frac{d_0}{2m} - \frac{m}{2} + t\right)}{\Gamma\left(\frac{d_0}{2m} - \frac{m}{2}\right)\Gamma\left(\frac{d_0}{2m} + t\right)}\right), \tag{7}$$

where $\Gamma(\cdot)$ represents the gamma function. Assumption A1 guarantees that $p_t(m)$ is well defined. Applying the squeeze theorem, we know that

$$\lim_{t \to \infty} \frac{\Gamma\left(\frac{d_0}{2m} - \frac{m}{2} + t\right)}{\Gamma\left(\frac{d_0}{2m} + t\right)} = 0.$$

Moreover,

$$\lim_{t \to \infty} \frac{1}{m(m+2)n_t} = 0.$$

Thus, using (7), we get

$$\lim_{t \to \infty} p_t(m) = \frac{2}{m+2}.$$

Assume that $\lim_{t\to\infty} p_t(k)$ exists for $k > m+1$. Using (5) for $k+1$, the expected number of nodes with degree $k+1$ is

$$n_t p_t(k+1) = \left(1 - \frac{m(k+1)}{d_0 + 2(t-1)m}\right) n_{t-1} p_{t-1}(k+1) + \frac{mk n_{t-1} p_{t-1}(k)}{d_0 + 2(t-1)m}. \quad (8)$$

Let $a_t \sim b_t$ denote the asymptotic equivalence between two positive sequences $\{a_t\}$ and $\{b_t\}$, that is, $a_t \sim b_t$ if and only if $\lim_{t\to\infty} a_t/b_t = 1$. Since $p_{t-1}(k) \sim p_t(k)$, using (8), we have that, for t large enough,

$$p_t(k+1) \sim \frac{\frac{mk}{d_0+2(t-1)m} n_{t-1}}{n_t - \left(1 - \frac{m(k+1)}{d_0+2(t-1)m}\right) n_{t-1}} p_t(k). \quad (9)$$

Moreover, because $\lim_{t\to\infty} p_t(k)$ exists and the limit as $t \to \infty$ of the coefficient of $p_t(k)$ in (9) equals $k/(k+3)$, we get

$$\lim_{t\to\infty} p_t(k+1) = \frac{k}{k+3} \lim_{t\to\infty} p_t(k).$$

Therefore, $\lim_{t\to\infty} p_t(k)$ exists for all $k \geq m$. ■

Based on Theorem 1, it is possible to derive a closed formula for the asymptotic value of the cumulative degree distribution.

Corollary 1. *The asymptotic value of the complementary cumulative degree distribution equals*

$$\bar{F}_\infty(k) = \frac{m(m+1)}{k(k+1)}.$$

Proof. Let $p_\infty(k) = \lim_{t\to\infty} p_t(k)$. Using Theorem 1, we know that

$$p_\infty(k) = \begin{cases} \dfrac{k-1}{k+2} p_\infty(k-1) & \text{if } k > m, \\ \dfrac{2}{m+2} & \text{if } k = m. \end{cases}$$

For $k > m$, $p_\infty(k)$ is defined as a recurrence with initial condition $p_\infty(m)$. For $k \geq m$, we have

$$p_\infty(k) = \frac{2m(m+1)}{k(k+1)(k+2)}. \quad (10)$$

Note that (10) captures the asymptotic behavior of the degree distribution of the BA model (Dorogovtsev *et al.*, 2000). Moreover, as $t \to \infty$,

$$F_\infty(k) = \lim_{t\to\infty} P[K_t < k] = \sum_{j=m}^{k-1} \frac{2m(m+1)}{j(j+1)(j+2)}.$$

By induction, it can be shown that

$$\sum_{j=1}^{k-1} \frac{2m(m+1)}{j(j+1)(j+2)} = \frac{m(m+1)(k-1)(k+2)}{2k(k+1)},$$

which implies that, for $k \geq m$,

$$F_\infty(k) = \frac{m(m+1)(k-1)(k+2)}{2k(k+1)} - \frac{(m-1)(m+2)}{2} = 1 - \frac{m(m+1)}{k(k+1)}$$

and

$$\bar{F}_\infty(k) = P[K \geq k] = 1 - F_\infty(k) = \frac{m(m+1)}{k(k+1)}. \quad (11)$$

■

Equation (11) represents the *complementary limit distribution* of the BA model. Next, we show that this limit distribution is an invariant set, which is not only a global attractor, but also a stable one. That is, adding or removing edges to all initial configurations such that $\bar{F}_0(k) \neq \bar{F}_\infty(k)$ for some k, yields complementary cumulative degree distributions that remain, for all time, close to $\bar{F}_\infty$.

3. Stability properties of the Barabási–Albert model

Define the state of the network at time t as an infinite dimensional vector $x_t = (x_t(1), x_t(2), \ldots)$, where $x_t(k) = \bar{F}_t(k)$. Let $\mathcal{X}$ be the set of states such that the only sequence that satisfies $\sum_{k=1}^{\infty} x(k) = 2m$ is the limit distribution, that is, $\mathcal{X}$ is the set

$$\left\{ x \in [0,1]^\infty : \sum_{k=1}^{\infty} x(k) = 2m \Rightarrow x(k) = \bar{F}_\infty(k) \right\}.$$

Based on (11), the state $x^e = (x^e(1), x^e(2), \ldots)$ represents the limit distribution $\bar{F}_\infty$. Note also that $x^e(k) > 0$ for all $k > 0$. Furthermore, since

$$\mathrm{E}[K_t] = \sum_{k=1}^{\infty} x_t(k), \quad (12)$$

using (3) we know that

$$\lim_{t\to\infty} \mathrm{E}[K_t] = \lim_{t\to\infty} \sum_{k=1}^{\infty} x_t(k) = \sum_{k=1}^{\infty} \bar{F}_\infty(k) = 2m,$$

that is,

$$\sum_{k=1}^{\infty} x^e(k) = 2m. \quad (13)$$

Now, let

$$\mathcal{X}_B = \left\{ x \in \mathcal{X} : \sum_{k=1}^{\infty} x(k) = 2m \right\}.$$

According to Lemma 3.1 of Khalil (2001), it can be shown that $\mathcal{X}_B$ is a non-empty invariant set. First, note that $x^e \in \mathcal{X}_B$. Second, because $x_t = \bar{F}_t$ and $x^e \in \mathcal{X}_B$, if $x_t = X(x_0, t)$ denotes the state reached at time t starting from $x_0 \in \mathcal{X}$, then $x_t \to x^e$ as $t \to \infty$. This implies that $\mathcal{X}_B$ corresponds to a positive limit set of the BA model. That is, there exists a sequence $\{t_i\}$ and an initial state $x_0 \in \mathcal{X}$ such that $x^e = X(x_0, t_i)$, for $t_i \to \infty$. We also know that $X(x_0, t_i + t) = X(X(x_0, t_i), t)$ for all t. Thus we get

$$\lim_{t_i \to \infty} X(x_0, t_i + t) = \lim_{t_i \to \infty} X(X(x_0, t_i), t) = X(x^e, t).$$

Because

$$\lim_{t_i \to \infty} X(x_0, t_i + t) = x^e,$$

we have $X(x^e, t) = x^e$ for all t. That is, $\mathcal{X}_B$ is invariant.

Next, to prove the stability of $\mathcal{X}_B$, we first need to define a metric between any pair of states in $\mathcal{X}$.

Lemma 1. *Consider the function* $\rho : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_0^+$,

$$\rho(x, y) = \left| \sum_{k=1}^{\infty} (x(k) - y(k)) \right|,$$

and define an equivalence relation on $\mathcal{X}$ *as* x *being related to* y *if* $\rho(x, y) = 0$. *Let* $[x]$ *denote the equivalence class of* x *and* $\mathcal{X}^* = \{[x] : x \in \mathcal{X}\}$ *the set of all equivalence classes. Let* $\rho^* : \mathcal{X}^* \times \mathcal{X}^* \to \mathbb{R}_0^+$ *be defined as* $\rho^*([x], [y]) = \rho(x, y)$. *Then* $(\rho^*, \mathcal{X}^*)$ *is a metric space.*

Proof. Let $w, x, y, z \in \mathcal{X}$. First, we show that ρ is a pseudometric. In particular, note that $\rho(x, y) \geq 0$ and $\rho(x, y) = \rho(y, x)$. To verify that ρ satisfies the triangle inequality, note that

$$\begin{aligned} \rho(x, y) &= \left| \sum_{k=1}^{\infty} (x(k) - y(k)) \right| \\ &= \left| \sum_{k=1}^{\infty} (x(k) - z(k)) + \sum_{k=1}^{\infty} (z(k) - y(k)) \right| \\ &\leq \rho(x, z) + \rho(z, y). \end{aligned}$$

In general, $x \neq y$ does not imply that $\rho(x, y) \neq 0$ (i.e., ρ is a pseudometric). Second, we show that for the equivalence relation over $\mathcal{X}$, ρ^* is well-defined; that is, if $([x], [y]) = ([z], [w])$, then $\rho^*([x], [y]) = \rho^*([z], [w])$. In particular, if $([x], [y]) = ([z], [w])$, then $[x] = [z]$ and $[y] = [w]$. Because ρ satisfies the triangle inequality, note that $\rho(x, y) \leq \rho(z, w)$ and $\rho(z, w) \leq \rho(x, y)$, that is, $\rho(x, y) = \rho(z, w)$, which implies that $\rho^*([x], [y]) = \rho^*([z], [w])$. Finally, we verify sufficient conditions for $(\rho^*, \mathcal{X}^*)$ to be a metric space. Let $[x], [y], [z] \in \mathcal{X}^*$. In particular, using the fact that ρ is a pseudometric, note that ρ^* satisfies the following:

1. For $[x] \neq [y]$, we know that $\rho^*([x], [y]) = \rho(x, y) = |\sum_{k=1}^{\infty} (x(k) - y(k))| > 0$.
2. For $x \in [x]$ and $y \in [y]$, note that $\rho^*([x], [y]) = 0$ if and only if $\rho(x, y) = 0$; that is, if and only if $|\sum_{k=1}^{\infty} (x(k) - y(k))| = 0$, which implies that $y \in [x]$ and $x \in [y]$. Therefore, $\rho^*([x], [y]) = 0$ if and only if $[x] = [y]$.
3. For $x, y \in \mathcal{X}$, we know that $\rho^*([x], [y]) = \rho^*([y], [x])$ because $\rho(x, y) = \rho(y, x)$.
4. For $x, y, z \in \mathcal{X}$,

$$\begin{aligned} \rho^*([x], [y]) &= \rho(x, y) \\ &\leq \rho(x, z) + \rho(z, y) \\ &= \rho^*([x], [z]) + \rho^*([z], [y]). \end{aligned}$$

■

We use Lemma 1 to characterize the stability properties of $\mathcal{X}_B$.

Theorem 2. *The invariant set* $\mathcal{X}_B$ *is globally asymptotically stable.*

Proof. Note that $\mathcal{X}_B = \{x^e\}$. Let

$$\mathcal{V}(x) = \rho(x, x^e) \tag{14}$$

be a Lyapunov candidate function. Note that $\mathcal{V}(x^e) = 0$. Moreover, according to the definition of $\mathcal{X}$, we know that $[x^e] = x^e$. Because $\mathcal{X}^*$ forms a partition of $\mathcal{X}$, if $x \in \mathcal{X}$ is such that $x \neq x^e$, then $x^e \notin [x]$. Thus, for all $x \neq x^e$,

$$\mathcal{V}(x) = \rho(x, x^e) = \rho^*([x], [x^e]) > 0.$$

The following four conditions guarantee the asymptotic stability of x^e (Burgess and Passino, 1995).

Existence of a lower bound: For all $\varepsilon_1 > 0$, there exists a $\delta_1 = \varepsilon_1 > 0$ such that for all $x \in \mathcal{X}$, if $\rho(x, x^e) > \varepsilon_1$, then $\mathcal{V}(x) > \delta_1$.

Existence of an upper bound: For all $\varepsilon_2 > 0$, there exists a $\delta_2 = \varepsilon_2 > 0$ such that for all $x \in \mathcal{X}$, if $\rho(x, x^e) < \delta_2$, then $\mathcal{V}(x) \leq \varepsilon_2$.

$\mathcal{V}$ is nonincreasing along all possible state trajectories: Note that for all $x_t \in \mathcal{X}$ we have

$$\mathcal{V}(x_t) = |\mathrm{E}[K_t] - 2m|. \tag{15}$$

Note also that if $x_0 \notin \mathcal{X}_B$, then $d_0 \neq 2mn_0$ for all $x \in \mathcal{X}$. Consider the following cases based on the

total degree of the initial network. If $d_0 < 2mn_0$, then $\mathrm{E}[K_t]$ is strictly increasing for all $t \geq 0$. Using (12), (13) and (15), we know that

$$\mathcal{V}(x_t) = 2m - \mathrm{E}[K_t]$$

and $\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) = \mathrm{E}[K_{t-1}] - \mathrm{E}[K_t] < 0$. Similarly, if $d_0 > 2mn_0$, then $\mathrm{E}[K_t]$ is strictly decreasing for all $t \geq 0$ and

$$\mathcal{V}(x_t) = \mathrm{E}[K_t] - 2m,$$

which implies that $\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) < 0$.

Convergence of $\mathcal{V}$: Let $x_0 \in \mathcal{X}$ such that $\sum_{k=1}^{\infty} x_0(k) \neq 2m$ (i.e., $d_0 \neq 2mn_0$). Because $x_t(k) = \bar{F}_t(k)$ and $x^e(k) = \bar{F}_\infty(k)$, we have $\lim_{t\to\infty} x_t = \bar{F}_\infty$. That is, $x_t \to x^e$ as $t \to \infty$ and so $\lim_{t\to\infty} \mathcal{V}(x_t) = 0$.

Because $x_t \to x^e$ as $t \to \infty$ for all possible state trajectories, $\mathcal{X}_B = \{x^e\}$ is globally asymptotically stable. ■

The next section establishes criteria for the detection of events representing unexpected edges that cannot be explained by the model. These criteria are derived based on the properties of the Lyapunov function.

4. Effects of anomalous events on the stability properties

We want to identify the instances at which anomalous events take place. Let $m_i > 0$ for $i = 1, 2, 3$, and consider the following types of events:

T1 The new node connects to $m_1 \neq m$ nodes based on the M2 mechanism.

T2 Existing nodes create m_2 additional edges.

T3 Existing nodes remove m_3 edges.

The detection of anomalous events is based on two criteria:

C1 $\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) > 0$,

C2 $n_t n_{t-1}(\mathcal{V}(x_{t-1}) - \mathcal{V}(x_t)) > |d_0 - 2mn_0|$.

C1 and C2 capture an evolution of the state x_t which contradicts the properties of the Lyapunov function $\mathcal{V}$. In particular, Criterion C1 implies a contradiction in the stability properties. Criterion C2 reflects a decrease in $\mathcal{V}$ by an amount larger than allowed. Note that it must be the case that

$$\mathcal{V}(x_{t-1}) - \mathcal{V}(x_t) \leq \rho(x_{t-1}, x_t) = \frac{|d_0 - 2mn_0|}{n_t n_{t-1}}.$$

Algorithm 1. Detection of anomalies in the BA model.

Input: A sequence of networks $\mathcal{G} = \{\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_t\}$ and the Lyapunov function $\mathcal{V}$ given in (14).

Output: A Boolean array A

1: $n_0 \leftarrow |V_0|$ and $d_0 \leftarrow \sum_{u\in V_0} k(u)$
2: Calculate $\mathcal{V}(x_0)$
3: **for** j from 1 to t **do**
4: $n_j \leftarrow n_{j-1} + 1$
5: Calculate $\mathcal{V}(x_j)$
6: $\mathcal{V}_j \leftarrow \mathcal{V}(x_j) - \mathcal{V}(x_{j-1})$
7: **if** $\mathcal{V}_j > 0$ or $-n_j n_{j-1}\mathcal{V}_j > |d_0 - 2mn_0|$ **then**
8: $A[j] \leftarrow$ **true**
9: $n_0 \leftarrow n_j$ and $d_0 \leftarrow \sum_{u\in V_j} k(u)$
10: **else**
11: $A[j] \leftarrow$ **false**
12: **end if**
13: **end for**
14: **return** A

Algorithm 1 describes the steps to identify the instances at which anomalous events take place in a sequence of undirected networks $\mathcal{G} = \{\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_t\}$. Recall that $\mathcal{G}_j = (V_j, E_j)$, for all $j \geq 0$. Line 1 counts the total number of nodes and sums the degrees of all nodes in $\mathcal{G}_0$. Computing these values requires a complexity $O(|V_0|)$ and $O(|E_0|)$. Line 2 calculates $\mathcal{V}(x_0)$, which, based on (15), runs in $O(|E_0|)$. These instructions are evaluated in a single instance. Next, note that instructions in lines 4, 6, and 7 are basic operations that run in $O(1)$. These instructions are evaluated t times. Based on (15), for each j from 1 to t, line 5 runs in $O(|E_j|)$. The instructions in lines 8, 9, and 11 are evaluated a finite number of times bounded by t. In particular, the instructions in lines 8, 11, and the first condition in line 9 run in $O(1)$. The second instruction in line 9 runs in $O(|E_j|)$. For $j \geq 0$, we can suppose that $|E_j| \approx |E_0| + mj$, so in the worst scenario the time required for Algorithm 1 is given by

$$c\sum_{j=1}^{t} |E_j| = c\sum_{j=1}^{t}(|E_0| + mj) = c\left(t|E_0| + m\frac{t(t+1)}{2}\right) \in O(t|E_0| + t^2),$$

for some constant $c > 0$.

Next, the following theorem presents conditions on m_i which guarantee that Algorithm 1 detects anomalous events of each type.

Theorem 3. *Let*

$$f_1(t) = \frac{2n_t(2mn_0 - d_0) + d_0 - 2mn_0}{2n_{t-1}},$$

$$f_2(t) = \frac{d_0 - 2mn_0}{2n_{t-1}}.$$

An anomaly of type T1 is detected by C1 for

1. $d_0 < 2mn_0$ *if* $m_1 > f_1(t) + m$ *or* $m_1 < f_2(t) + m$,
2. $d_0 > 2mn_0$ *if* $m_1 > f_2(t) + m$ *or* $m_1 < f_1(t) + m$;

by C2 for

1. $d_0 < 2mn_0$ *if* $m < m_1 < 2mn_0 - d_0 + m$,
2. $d_0 > 2mn_0$ *if* $2mn_0 - d_0 + m < m_1 < m$.

An anomaly of type T2 is detected by C1 for

1. $d_0 < 2mn_0$ *if* $m_2 > f_1(t)$,
2. $d_0 > 2mn_0$ *if* $m_2 > f_2(t)$;

and by C2 for $d_0 < 2mn_0$ *if* $m_2 < 2mn_0 - d_0$.

Finally, an anomaly of type T3 is detected by C1 for

1. $d_0 < 2mn_0$ *if* $m_3 > -f_2(t)$,
2. $d_0 > 2mn_0$ *if* $m_3 > -f_1(t)$;

and by C2 for $d_0 > 2mn_0$ *if* $m_3 < d_0 - 2mn_0$.

Proof. See Appendix. ■

The next section presents simulations of the model and the performance of the proposed detection algorithm.

5. Simulations

First, we show the asymptotic behavior of the degree distribution and the Lyapunov function over time. Figure 1 illustrates the evolution of $x_t(k)$ for $k \in \{m, \dots, 7\}$ using an initial network $\mathcal{G}_0$ with $m = 2$, $n_0 = 4$, $d_0 = 8$. Note that the asymptotic values are derived using (11). Simulations correspond to an average of 100 runs of the model. Figure 2 depicts the evolution of the Lyapunov function $\mathcal{V}$ for $m = 2, 3, 4$. Note that $\mathcal{V}$ is a decreasing function and approaches to 0 for large values of t.

Second, we illustrate the regions of anomaly detection for the initial network $\mathcal{G}_0$. According to Theorem 3, Fig. 3 shows the regions in which anomalies of type T1, T2, and T3 can be detected. A labeled region represents the criterion that detects an anomaly of size m_1, m_2, or m_3; regions without a label indicate the sizes of anomalies which cannot be detected by Algorithm 1. Note that the algorithm detects anomalies of almost any size.

Third, we evaluate the performance of Algorithm 1 for a sequence of 200 networks considering the occurrence of 15 anomalies; five of them being anomalies of type T1 which occur at $\{50, 80, 110, 140, 170\}$, five of type T2 (at $\{60, 90, 120, 150, 180\}$), and five of type T3 (at $\{70, 100, 130, 160, 190\}$). The size of an anomaly is a randomly selected number between 3 and 6. Based on the evolution of the model, Algorithm 1 reports all anomalies

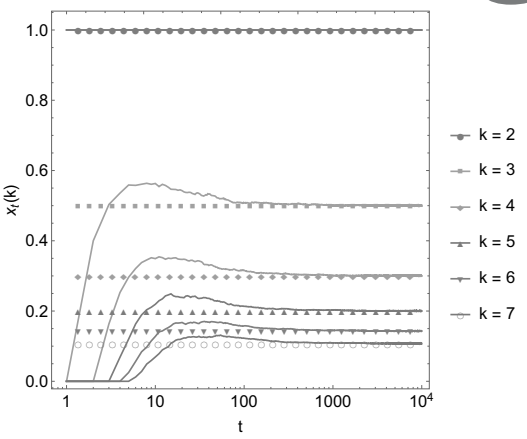


Fig. 1. Evolution of the complementary cumulative density function of the degree of nodes for $k \in \{m, \dots, 7\}$ and $\mathcal{G}_0$ with $n_0 = 4$, $d_0 = 8$ and $m = 2$. The marks represent the asymptotic values for the distributions obtained from (11).

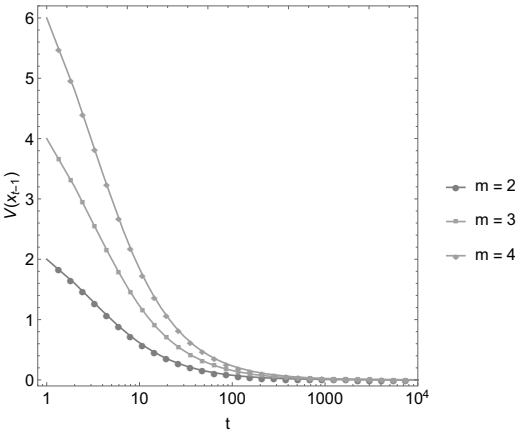


Fig. 2. Lyapunov function $\mathcal{V}$ for $m = 2, 3, 4$.

with a true positive rate (TPR) equal to 1 and a false positive rate (FPR) equal to 0. Figure 4(a) illustrates how the detection procedure identifies anomalies at various instances based on the differences $n_t n_{t-1}(\mathcal{V}(x_{t-1}) - \mathcal{V}(x_t))$. Note that an increase in $\mathcal{V}$ represents detection of anomalies based on C1, and a decrease—detection based on C2. Note also that, if no anomalies occur, then the expression $n_t n_{t-1}(\mathcal{V}(x_{t-1}) - \mathcal{V}(x_t))$ remains constant.

Finally, we compare the proposed algorithm with the approach of Koutra *et al.* (2016), which uses network similarity for detecting anomalies. Let $\mathcal{G}_i = (V, E_i)$ and $\mathcal{G}_{i+1} = (V, E_{i+1})$ be two consecutive networks, where $V = V_i \cup V_{i+1}$. In the work of Koutra *et al.* (2016), the following steps determine the similarity value between $\mathcal{G}_i$ and $\mathcal{G}_{i+1}$:

S1 *Affinity score*: For $\ell = i, i+1$, compute the matrix of

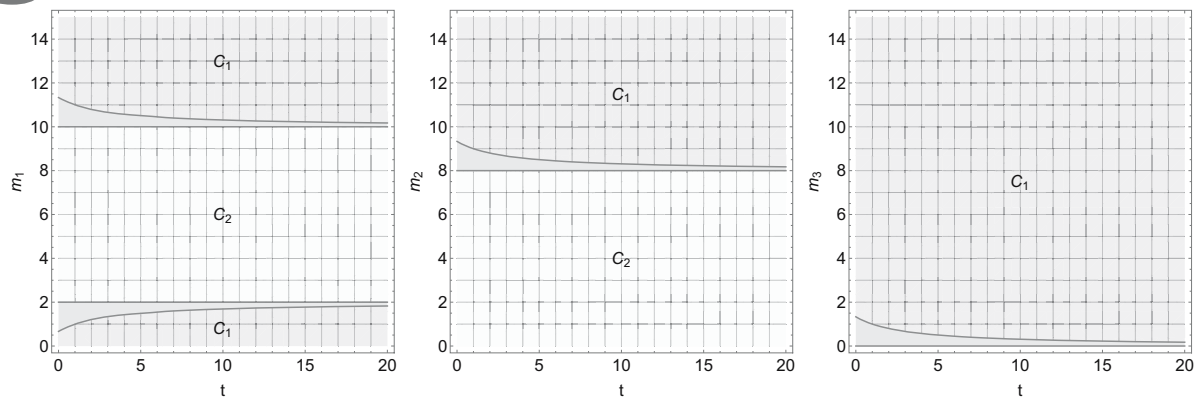


Fig. 3. Regions in which anomalous events of type T1 (a), T2 (b), and T3 (c) can be detected in the BA model with Algorithm 1 using an initial network $\mathcal{G}_0$ with $m = 2$, $n_0 = 4$ and $d_0 = 8$. Labeled regions represents the criterion than can be applied to detect an anomaly of size m_1, m_2, or m_3. Closed no-labeled regions illustrate the sizes of anomalies which cannot be detected.

node affinity

$$S_\ell = (I_\ell + \epsilon_\ell^2 D_\ell - \epsilon_\ell A_\ell)^{-1},$$

where I_ℓ is the identity matrix, A_ℓ the adjacency matrix of $\mathcal{G}_\ell$, $\epsilon_\ell = (1 + \max_{u \in \mathcal{G}_\ell} k(u))^{-1}$, and D_ℓ the diagonal matrix in which the main diagonal coincides with the vector of node degrees of $\mathcal{G}_\ell$.

S2 *Distance*: The distance $d(\mathcal{G}_i, \mathcal{G}_{i+1})$ between $\mathcal{G}_i$ and $\mathcal{G}_{i+1}$ is given by the sum of all elements of the matrix $\left(\sqrt{S_i} - \sqrt{S_{i+1}}\right)^2$.

S3 *Similarity*: The similarity s_i between $\mathcal{G}_i$ and $\mathcal{G}_{i+1}$ is

$$s_i = \frac{1}{1 + d(\mathcal{G}_i, \mathcal{G}_{i+1})}.$$

Now, we evaluate the performance of anomaly detection using similarity values in the sequence $\mathcal{G}$. Let M_i denote the median of the sample $s_1, \ldots, s_i$ and σ_i its standard deviation. Furthermore, let $\zeta_i^j = M_i + j\sigma_i$ represent a threshold around the median M_i, for $j = \pm 1, 2, 3$. Figure 4(b) depicts the similarity values between consecutive networks, including the thresholds ζ_i^j for each $i = 1, \ldots, 200$ and $j = \pm 1, 2, 3$. Table 1 shows true and false positives rates, which illustrates that, as the thresholds increase, the true and false positives rates decrease.

Table 1. Rate of true and false positives using similarity between consecutive networks.

	$\zeta^{\pm 1}$	$\zeta^{\pm 2}$	$\zeta^{\pm 3}$
TPR	1	0.83	0.58
FPR	0.24	0.04	0.004

6. Conclusions

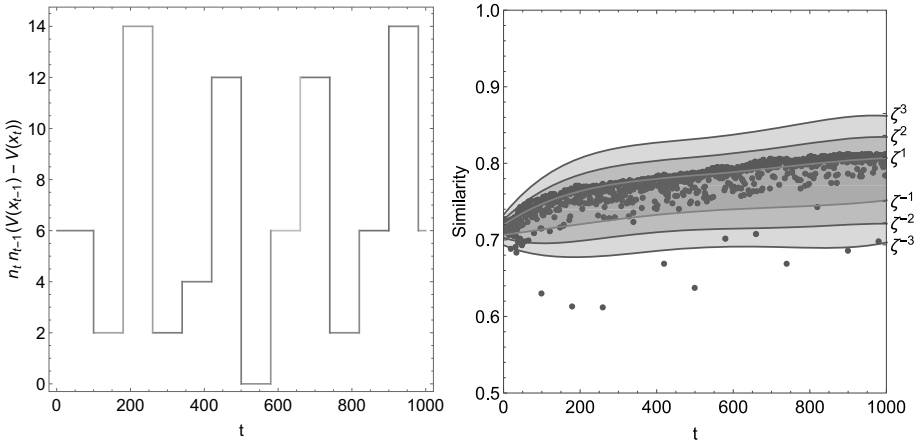
Our work characterizes the stability properties of networks generated by the Barabási–Albert model. In particular, at time t, we define the state of the system as an infinite dimensional vector $x_t = (x_t(1), x_t(2), \ldots)$, where $x_t(k)$ represents the probability of a randomly selected node having a degree greater than or equal to k. We show that the sum of all possible state component is always less than the average degree of the network; that is, for all $t < \infty$, we determine that $\sum_{k=1}^{\infty} x_t(k) < 2m$. Using this relationship, we show that the limit of the complementary cumulative degree distribution is not only a global attractor but also a stable invariant (in the sense of Lyapunov). We then use the Lyapunov function of the stability analysis to determine the occurrence of anomalous events across the network. Understanding the stability properties of other centrality measures, as well as the effect of variations of preferential attachment rules, remains a future research direction.

Acknowledgment

This research was supported in part by the Center of Excellence and Appropriation in Big Data and Data Analytics (CAOBA) at Pontifical Xavierian University, the Ministry of Information Technologies and Telecommunications of Colombia (MinTIC), and the Colombian Administrative Department of Science, Technology and Innovation (COLCIENCIAS), under the grant no. FP44842-546-2015.

References

Barabási, A.-L. and Albert, R. (1999). Emergence of scaling in random networks, *Science* **286**(5439): 509–512.



(a) (b)

Fig. 4. Anomaly detection in the sequence $\mathcal{G}$ using Algorithm 1 (a), where the differences $n_t n_{t-1}(\mathcal{V}(x_{t-1}) - \mathcal{V}(x_t))$ are computed changing the initial network at instants in which anomalies occur (increasing jumps represent detection of anomalies based on Criterion C1, and decreasing based on Criterion C2), and similarity values between consecutive networks (b).

Barabási, A.-L. and Pósfai, M. (2016). *Network Science*, Cambridge University Press, Cambridge.

Bianconi, G. and Barabási, A. L. (2001). Competition and Multiscaling in evolving networks, *Europhysics Letters* **54**(4): 436–442.

Burgess, K. and Passino, K. (1995). Stability analysis of load balancing systems, *International Journal of Control* **61**(2): 357–393.

Caldarelli, G., Capocci, A., De Los Rios, P. and Muñoz, M.A. (2002). Scale-free networks from varying vertex intrinsic fitness, *Physical Review Letters* **89**(25): 258702.

Chandola, V., Banerjee, A. and Kumar, V. (2009). Anomaly detection: A survey, *ACM Computing Surveys* **41**(3): 15:1–15:58.

Chen, Q. and Shi, D. (2004). The modeling of scale-free networks, *Physica A: Statistical Mechanics and Its Applications* **335**(1): 240–248.

Choromanski, K., Matuszak, M. and Miekisz, J. (2013). Scale-free graph with preferential attachment and evolving internal vertex structure, *Journal of Statistical Physics* **151**(6): 1175–1183.

Dorogovtsev, S.N., Mendes, J.F.F. and Samukhin, A.N. (2000). Structure of growing networks with preferential linking, *Physical Review Letters* **85**(21): 4633–4636.

Gogoi, P., Bhattacharyya, D., Borah, B. and Kalita, J.K. (2011). A survey of outlier detection methods in network anomaly identification, *The Computer Journal* **54**(4): 570–588.

Hirose, S., Yamanishi, K., Nakata, T. and Fujimaki, R. (2009). Network anomaly detection based on eigen equation compression, *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Paris, France*, pp. 1185–1194.

Host-Madsen, A. and Zhang, J. (2018). Coding of graphs with application to graph anomaly detection, *2018 IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA*, pp. 1829–1833.

Jackson, M.O. and Rogers, B.W. (2007). Meeting strangers and friends of friends: How random are social networks?, *American Economic Review* **97**(3): 890–915.

Khalil, H. (2001). *Nonlinear Systems*, 3rd Edn., Pearson, Upper Saddle River, NJ.

Koutra, D., Shah, N., Vogelstein, J.T., Gallagher, B. and Faloutsos, C. (2016). DELTACON: Principled massive-graph similarity function with attribution, *ACM Transactions on Knowledge Discovery Data* **10**(3): 28:1–28:43.

Kudělka, M., Zehnalová, Š., Horák, Z., Krömer, P. and Snášel, V. (2015). Local dependency in networks, *International Journal of Applied Mathematics and Computer Science* **25**(2): 281–293, DOI: 10.1515/amcs-2015-0022.

Lee, C.-Y. (2006). Correlations among centrality measures in complex networks, *arXiv:* 0605220.

Moriano, P. and Finke, J. (2012). Power-law weighted networks from local attachments, *Europhysics Letters* **99**(1): 18002.

Ranshous, S., Shen, S., Koutra, D., Harenberg, S., Faloutsos, C. and Samatova, N.F. (2015). Anomaly detection in dynamic networks: A survey, *WIREs Computational Statistics* **7**(3): 223–247.

Ruiz, D. and Finke, J. (2013). Invalidation of dynamic network models, *Proceedings of the American Control Conference, Washington, DC, USA,* pp. 138–143.

Savage, D., Zhang, X., Yu, X., Chou, P. and Wang, Q. (2014). Anomaly detection in online social networks, *Social Networks* **39**(C): 62–70.

Segarra, S. and Ribeiro, A. (2016). Stability and continuity of centrality measures in weighted graphs, *IEEE Transactions on Signal Processing* **64**(3): 543–555.

Shao, Z.-G., Zou, X.-W., Tan, Z.-J. and Jin, Z.-Z. (2006). Growing networks with mixed attachment mechanisms, *Journal of Physics A: Mathematical and General* **39**(9): 2035.

Shoubridge, P., Kraetzl, M., Wallis, W.D. and Bunke, H. (2002). Detection of abnormal change in a time series of graphs, *Journal of Interconnection Networks* **3**(01n02): 85–101.

Tong, J., Hou, Z., Zhang, Z. and Kong, X. (2009). Degree correlations in the group preferential model, *Journal of Physics A: Mathematical and Theoretical* **42**(27): 275002.

Valente, T.W., Coronges, K., Lakon, C. and Costenbader, E. (2008). How correlated are network centrality measures?, *Connections* **28**(1): 16–26.

Yu, R., Qiu, H., Wen, Z., Lin, C.-Y. and Liu, Y. (2016). A survey on social media anomaly detection, *SIGKDD Explorations* **18**(1): 1–14.

Diego Ruiz received his BSc degree in mathematics from Universidad del Cauca, Popayán, Colombia, and his MSc degree in computer science from Pontificia Universidad Javeriana, Cali, Colombia. Currently, he is a PhD candidate in computer science at Universidad del Valle, Cali, and a professor of the Department of Mathematics at Universidad del Cauca.

Jorge Finke received his PhD in electrical engineering from Ohio State University in 2007. He is currently a professor of the Department of Electrical and Computer Engineering at Pontificia Universidad Javeriana, Cali, Colombia. His research focuses on network theory and its applications.

Appendix

Proof. (Theorem 3) Let

$$f_1(t) = \frac{2n_t(2mn_0 - d_0) + d_0 - 2mn_0}{2n_{t-1}},$$
$$f_2(t) = \frac{d_0 - 2mn_0}{2n_{t-1}}.$$

We show the detection of anomalous events of type T1. The proof of detection of anomalous events of types T2 and T3 follows a similar argument.

Note that if an anomalous event of type T1 occurs at time t, then

$$\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) = \left|\frac{d_0 - 2mn_0 + 2(m_1 - m)}{n_t}\right| - \left|\frac{d_0 - 2mn_0}{n_{t-1}}\right|.$$

Consider the following four cases:

If $d_0 < 2mn_0$ and $d_0 - 2mn_0 + 2(m_1 - m) \geq 0$, then

$$\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) = \frac{2n_t(d_0 - 2mn_0) + 2n_{t-1}(m_1 - m)}{n_t n_{t-1}} - \frac{d_0 - 2mn_0}{n_t n_{t-1}}. \quad \text{(A1)}$$

If $d_0 < 2mn_0$ and $d_0 - 2mn_0 + 2(m_1 - m) < 0$, then

$$\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) = \frac{d_0 - 2mn_0 - 2n_{t-1}(m_1 - m)}{n_t n_{t-1}}. \quad \text{(A2)}$$

If $d_0 > 2mn_0$ and $d_0 - 2mn_0 + 2(m_1 - m) \geq 0$, then

$$\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) = \frac{2mn_0 - d_0 + 2n_{t-1}(m_1 - m)}{n_t n_{t-1}}. \quad \text{(A3)}$$

If $d_0 > 2mn_0$ and $d_0 - 2mn_0 + 2(m_1 - m) < 0$, then

$$\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) = \frac{2n_t(2mn_0 - d_0) - 2n_{t-1}(m_1 - m)}{n_t n_{t-1}} - \frac{2mn_0 - d_0}{n_t n_{t-1}}. \quad \text{(A4)}$$

First, consider the detection based on Criterion C1. Using (A1), we have that $\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) > 0$ if and only if

$$m_1 > f_1(t) + m. \quad \text{(A5)}$$

Note that $f_1(t) + m$ is a decreasing function and tends to $2mn_0 - d_0 + m$ as t tends to infinity, so

$$f_1(t) + m > 2mn_0 - d_0 + m.$$

We have

$$m_1 > \frac{2mn_0 - d_0 + 2m}{2}$$

and

$$m_1 > f_1(t) + m.$$

Because

$$2mn_0 - d_0 + m > \frac{2mn_0 - d_0 + 2m}{2},$$

in this case the solution is given by (A5).

Using (A2), we know that $\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) > 0$ if and only if

$$m_1 < f_2(t) + m. \quad \text{(A6)}$$

Note that $f_2(t) + m$ is an increasing function and tends to m as t tends to infinity, so

$$f_2(t) + m < m.$$

We have

$$m_1 < \frac{2mn_0 - d_0 + 2m}{2}$$

and

$$m_1 < f_2(t) + m.$$

Because

$$m < \frac{2mn_0 - d_0 + 2m}{2},$$

in this case the solution is given by (A6). Thus, using (A5) and (A6), an anomaly of type T1 is detected by Criterion C1 for $d_0 < 2mn_0$ if

$$m_1 > f_1(t) + m \text{ or } m_1 < f_2(t) + m.$$

Using a similar argument, based on (A3) and (A4) it can be shown that an anomaly of type T1 is detected by Criterion C1 for $d_0 > 2mn_0$ if

$$m_1 > f_2(t) + m \text{ or } m_1 < f_1(t) + m.$$

Second, consider the detection based on Criterion C2. Using (A1), we have that $n_t n_{t-1}(\mathcal{V}(x_{t-1}) - \mathcal{V}(x_t)) > |d_0 - 2mn_0|$ if and only if

$$m_1 < 2mn_0 - d_0 + m.$$

Thus, in this case m_1 must satisfy

$$\frac{2mn_0 - d_0 + 2m}{2} \leq m_1 < 2mn_0 - d_0 + m. \quad \text{(A7)}$$

Using (A2), we have $n_t n_{t-1}(\mathcal{V}(x_{t-1}) - \mathcal{V}(x_t)) > |d_0 - 2mn_0|$ if and only if $m_1 < m$. In this case m_1 must satisfy

$$m < m_1 < \frac{2mn_0 - d_0 + 2m}{2}. \quad \text{(A8)}$$

Thus, using (A7) and (A8), an anomaly of type T1 is detected by Criterion C2 for $d_0 < 2mn_0$ if

$$m < m_1 < 2mn_0 - d_0 + m.$$

Using a similar argument, based on (A3) and (A4), it can be shown that an anomaly of type T1 is detected by Criterion C2 for $d_0 > 2mn_0$ if

$$2mn_0 - d_0 + m < m_1 < m.$$

Now, note that if an anomalous event of type T2 occurs at time t, then

$$\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) = \left|\frac{d_0 - 2mn_0 + 2m_2}{n_t}\right| - \left|\frac{d_0 - 2mn_0}{n_{t-1}}\right|, \quad \text{(A9)}$$

and if an anomalous event of type T3 occurs at time t, then

$$\mathcal{V}(x_t) - \mathcal{V}(x_{t-1}) = \left|\frac{d_0 - 2mn_0 - 2m_3}{n_t}\right| - \left|\frac{d_0 - 2mn_0}{n_{t-1}}\right|. \quad \text{(A10)}$$

Following similar arguments as in the proof of detection of anomalous events of type T1, using (A9) and (A10) we get the other results. ■

Received: 1 June 2018
Revised: 13 December 2018
Accepted: 18 January 2019