Counting triangles, tunable clustering and the small-world property in random key graphs (Extended version)

Osman Yağan, Member, IEEE and Armand M. Makowski, Fellow, IEEE

Abstract—Random key graphs were introduced to study various properties of the Eschenauer-Gligor key predistribution scheme for wireless sensor networks (WSNs). Recently this class of random graphs has received much attention in contexts as diverse as recommender systems, social network modeling, and clustering and classification analysis. This paper is devoted to analyzing various properties of random key graphs. In particular, we establish a zero-one law for the the existence of triangles in random key graphs, and identify the corresponding critical scaling. This zero-one law exhibits significant differences with the corresponding result in Erdős-Rényi (ER) graphs. We also compute the clustering coefficient of random key graphs, and compare it to that of ER graphs in the many node regime when their expected average degrees are asymptotically equivalent. For the parameter range of practical relevance in both wireless sensor network and social network applications, random key graphs are shown to be much more clustered than the corresponding ER graphs. We also explore the suitability of random key graphs as small world models in the sense of Watts and Strogatz.

Index Terms—Random key graphs; existence of triangles; clustering coefficient; wireless sensor networks; social networks.

1 INTRODUCTION

Random key graphs are random graphs that belong to the class of random intersection graphs [3], they are also called uniform random intersection graphs by some authors [3, 11, 12]. They have appeared recently in application areas as diverse as epidemics in social networks [2], clustering analysis [11, 12], collaborative filtering in recommender systems [18], and random key predistribution for wireless sensor networks (WSNs) [9]. In this last context, random key graphs naturally occur in the study of a random key predistribution scheme introduced by Eschenauer and Gligor [9]: Before deployment, each sensor in a WSN is independently assigned \( K \) distinct cryptographic keys which are selected at random from a large pool of \( P \) keys. These \( K \) keys constitute the key ring of the sensor node and are inserted into its memory module. Two sensor nodes can then establish a secure edge between them if they are within transmission range of each other and if their key rings have at least one key in common; see [9] for implementation details. If we assume full visibility, namely that nodes are all within communication range of each other, then secure communication between two nodes requires only that their key rings share at least one key. The resulting notion of adjacency defines the class of random key graphs; see Section 2 for precise definitions.

Much efforts have recently been devoted to developing zero-one laws for the property of connectivity in random key graphs. A key motivation can be found in the need to obtain conditions under which the scheme of Eschenauer and Gligor guarantees secure connectivity with high probability in large networks [32]. An interesting feature of this work lies in the following fact: Although random key graphs are not stochastically equivalent to the classical Erdős-Rényi graphs [8], it is possible to formally transfer well-known zero-one laws for connectivity in Erdős-Rényi graphs to random key graphs by asymptotically matching their edge probabilities. This approach, which was initiated by Eschenauer and Gligor in their original analysis [9], has now been validated rigorously; see the papers [3, 7, 24, 28, 33, 37] for recent developments. Rybarczyk [24] has shown that this transfer from Erdős-Rényi graphs also works for a number of issues related to the giant component and its diameter.

In view of these developments, it is natural to wonder whether this (formal) transfer technique applies to other graph properties. In particular, in the literature on random graphs there is long standing interest [4, 8, 15, 16, 23, 26] in the containment of certain (small) subgraphs, the simplest one being the triangle. This particular case is also of some practical relevance: The number of triangles in a graph is closely related to its clustering coefficient, and for random key graphs this has implications on network resiliency under the EG scheme (e.g., see [21]) and on its applicability and relevance in different domains including...
social networks – more on that later.

With these in mind, in the present paper we study the triangle containment problem in random key graphs. In particular, we establish a zero-one law for the existence of triangles and identify the corresponding critical scaling. By the help of this result (and its proof), we conclude that in the many node regime, the expected number of triangles in random key graphs is always at least as large as the corresponding quantity in asymptotically matched Erdős-Rényi graphs. For the parameter range of practical relevance in WSNs, we show that this expected number of triangles can be orders of magnitude larger in random key graphs than in Erdős-Rényi graphs, confirming the observations made earlier via simulations by Di Pietro et al. [2].

These results show that transferring results from Erdős-Rényi graphs to random key graphs by matching their edge probabilities is not a valid approach in general, and can be quite misleading in the context of WSNs. In particular, our results indicate that the asymptotic equivalence of random key graphs and Erdős-Rényi graphs (in the sense discussed in [25]) is possible only when the size of key rings is comparable to the network size, a case not very realistic in WSNs due to the severe constraints imposed on the memory and computational capabilities of sensors. This points to the inadequacy of Erdős-Rényi graphs to capture some key properties of the EG scheme in realistic WSN implementations, and reinforces the call for a direct investigation of random key graphs.

The number (and fraction) of triangles in a network is closely related to its clustering coefficient, a metric known to have a significant impact on the dynamics of many interesting processes that take place on the network, e.g., the diffusion of information and epidemic diseases [10], [20], [21], [88], [84], the propagation of influence [13], [89], and cascading failures [14]. With this in mind, we also study the clustering coefficient of random key graphs and compare it with that of an Erdős-Rényi graph. We observe that the clustering coefficient of a random key graph is never smaller than the clustering coefficient of the corresponding Erdős-Rényi graph with identical expected average degree. For the parameter range that is relevant for large scale social networks (as well as WSNs), we show that random key graphs are in fact much more clustered than Erdős-Rényi graphs when expected average degrees are asymptotically equivalent. Recalling the fact that random key graphs also have a small diameter [24], [31], we then conclude that random key graphs are small-worlds in the sense introduced by Watts and Strogatz [27]. This reinforces the possibility of using random key graphs in a wide range of applications including social network modeling.

In line with results currently available for other classes of graphs, e.g., Erdős-Rényi graphs [15] Chap. 3] and random geometric graphs [25] Chap. 3], it would be interesting to consider the containment problem for small subgraphs other than triangles in the context of random key graphs. To the best of our knowledge, this issue has not been considered in the literature. Future work may also consider other properties of random key graphs that might be relevant in various applications; e.g., Hamiltonicity, spectral radius, percolation, etc.

The paper is organized as follows: We formally introduce the class of random key graphs in Section 2 with various definitions for the clustering coefficient presented in Section 2.2. In Section 2.3, we evaluate the first and second moments of the number of triangles in random key graphs. Our main results are presented in Section 3. A zero-one law concerning the containment of triangles in random key graphs is discussed in Section 3.2 while its clustering coefficient is computed in Section 3.3. Relevant definitions and facts concerning Erdős-Rényi graphs are given in Section 4. Section 5 and Section 6 are devoted to comparing random key graphs and Erdős-Rényi graphs in terms of their number of triangles and clustering coefficients, respectively. Section 7 and Section 8 discuss the implications of our results on utilizing random key graph in the context of WSN and social network applications, respectively. The proofs of the main results of the paper are available in Section 10 while some technical results are established in Section 9.

A word on the notation and conventions in use: Unless specified otherwise, all limiting statements, including asymptotic equivalences, are understood with n going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple (Ω, F, P); its construction is standard and omitted in the interest of brevity. Probabilistic statements are made with respect to this probability measure P, and we denote the corresponding expectation operator by E. We denote almost sure convergence (under P) by a.s. The indicator function of an event E is denoted by 1[E]. For any discrete set S we write |S| for its cardinality. We denote almost sure convergence by a.s.

2 Model and Definitions
2.1 Random key graphs
Pick positive integers K and P such that K ≤ P, and fix n = 3, 4, . . . . We shall group the integers P and K into the ordered pair θ ≡ (K, P) in order to lighten the notation.

The model of interest here is parametrized by the number n of nodes, the size P of the key pool and the size K of each key ring. For each node i = 1, . . . , n, let K_i(θ) denote the random set of K distinct keys assigned to node i. Thus, under the convention that the P keys are labeled 1, . . . , P, the random set K_i(θ) is a subset of {1, . . . , P} with |K_i(θ)| = K. The rvs K_1(θ), . . . , K_n(θ) are assumed to be i.i.d., each of which is uniformly distributed with

\[ P[K_i(θ) = S] = \left(\frac{P}{K}\right)^{-1}, \quad i = 1, \ldots, n \]

for any subset S of {1, . . . , P} with |S| = K. This corresponds to selecting keys randomly and without replacement from the key pool.

Distinct nodes i, j = 1, . . . , n are said to be adjacent if they share at least one key in their key rings, namely

\[ K_i(θ) \cap K_j(θ) \neq \emptyset, \]

in which case an undirected edge is assigned between nodes i and j. The adjacency constraints define an undirected random graph on the vertex set {1, . . . , n}, hereafter denoted G(n; θ). We refer to this random graph as the random key graph.
It is easy to check that
\[ P[K_i(\theta) \cap K_j(\theta) = \emptyset] = q(\theta) \] (3)
with
\[ q(\theta) = \begin{cases} 0 & \text{if } P < 2K \\ \frac{(P-K)}{K} & \text{if } 2K \leq P. \end{cases} \] (4)
The probability \( p(\theta) \) of edge occurrence between any two
nodes is therefore given by
\[ p(\theta) = 1 - q(\theta). \] (5)
If \( P < 2K \) there exists an edge between any pair of nodes, and \( \mathbb{K}(n; \theta) \) coincides with the complete graph on the vertex
set \( \{1, \ldots, n\} \). While it is always the case that \( 0 \leq q(\theta) < 1 \), it is plain from (3) that \( q(\theta) > 0 \) if and only if \( 2K \leq P \).
The expression (4) is a consequence of the general fact
\[ P[S \cap K_i(\theta) = \emptyset] = \frac{(P-S)}{K}, \quad i = 1, \ldots, n \] (6)
valid for any subset \( S \) of \( \{1, \ldots, P\} \) with \( |S| \leq P - K \).
We close by introducing the events
\[ E_{ij}(\theta) = [K_i(\theta) \cap K_j(\theta) \neq \emptyset], \quad i, j = 1, \ldots, n \]
whose indicator functions
\[ \xi_{ij}(\theta) = 1[K_i(\theta) \cap K_j(\theta) \neq \emptyset], \quad i, j = 1, \ldots, n \]
are the edge rvs defining the random key graph \( \mathbb{K}(n; \theta) \). For each \( i = 1, \ldots, n \), it is a simple matter to check with the help of (6) that the events \( \{E_{ij}(\theta), j \neq i, j = 1, \ldots, n\} \)
are mutually independent, or equivalently, that the rvs \( \{\xi_{ij}(\theta), j \neq i, j = 1, \ldots, n\} \)
form a collection of i.i.d. rvs.

### 2.2 Clustering coefficient

Many networks encountered in practice exhibit high clustering (or transitivity) in that the neighbors of a node are likely to be neighbors to each other [25] — Your friends are likely to be friends! Clustering properties are known to have a significant impact on the dynamics of many interesting processes that take place on a network, e.g., the diffusion of information and epidemic diseases [10, 20, 21, 33], the propagation of influence [13, 39], and cascading failures [13]. With this in mind we shall investigate clustering in random key graphs under various parameter regimes.

A formal definition of clustering is given next. Consider an undirected graph \( G \) with no self-loops on the vertex set \( V \). For each \( i \) in \( V \), let \( T_i(G) \) denote the number of distinct triangles in \( G \) that contain vertex \( i \). The local clustering coefficient of node \( i \) is given by
\[ C_i(G) = \begin{cases} \frac{T_i(G)}{2d_i(d_i-1)} & \text{if } d_i \geq 2 \\ 0 & \text{otherwise} \end{cases} \] (7)
where \( d_i \) is the degree of node \( i \) in \( G \).

There are, however, several possible definitions for a
graph-wide notion of clustering [22]. Inspired by (7), it is
natural to consider the average of the local clustering coefficient \( C_{\text{Avg}}(G) \) over the graph \( G \), i.e.,
\[ C_{\text{Avg}}(G) = \frac{1}{|V'|} \sum_{i \in V'} C_i(G) \] (8)
where \( V' = \{i \in V : d_i \geq 2\} \). This last quantity, while natural, is often replaced by the global clustering coefficient defined as the “fraction of transitive triples” over the whole graph \( G \), namely,
\[ C^*(G) = \frac{\sum_{i \in V} T_i(G)}{\frac{1}{2} \sum_{i \in V} d_i(d_i-1)} \] (9)
provided \( \sum_{i \in V} d_i(d_i-1) > 0 \). It is convenient to set \( C^*(G) = 0 \) otherwise.

In the context of random graphs, related (but simpler) definitions are possible when the edge assignment rvs are exchangeable (as is the case for the random graphs of interest here). Recall that an undirected random graph \( G \) defined over the set of nodes \( \{1, \ldots, n\} \) is characterized by the \{0, 1\}-valued edge rvs \( \{\xi_{ij}, i, j = 1, \ldots, n\} \) with
the interpretation that \( \xi_{ij} = 1 \) (resp. \( \xi_{ij} = 0 \)) if there is an edge (resp. no edge) between nodes \( i \) and \( j \). As we consider graphs which are undirected with no self-loops, we impose the conditions
\[ \xi_{ij} = \xi_{ji} \quad \text{and} \quad \xi_{ii} = 0, \quad i, j = 1, \ldots, n. \]

A case of great interest arises when the rvs \( \{\xi_{ij}, 1 \leq i < j \leq n\} \) form a family of exchangeable rvs [11]. In that setting, a popular approach (e.g., see [26]) is to define the clustering coefficient of the random graph \( G \) as the conditional probability
\[ C(G) = P[E_{12} | E_{13} \cap E_{23}] \] (10)
where we have used the notation
\[ E_{ij} = [\xi_{ij} = 1], \quad i, j = 1, \ldots, n. \]

For the random graphs considered here, we show that the quantity (10) provides a good approximation to the global clustering coefficient defined at (8), when \( n \) is large; see Theorem 5.4 and Theorem 4.1. It is for this reason that we use the simpler definition (10) for studying clustering in the remainder of this paper.

### 2.3 Counting triangles

Pick positive integers \( K \) and \( P \) such that \( K \leq P \), and fix \( n = 3, 4, \ldots \) For distinct \( i, j, k = 1, \ldots, n \), we define the indicator function
\[ \chi_{ijk}(\theta) = 1 \left[ \text{Nodes } i, j, k \text{ form a triangle in } \mathbb{K}(n; \theta) \right]. \] (11)
The number of distinct triangles in \( \mathbb{K}(n; \theta) \) is then simply given by
\[ T_n(\theta) = \sum_{1 \leq i < j < k \leq n} \chi_{ijk}(\theta). \] (12)
Of particular interest is the event that there exists at least one
triangle in \( \mathbb{K}(n; \theta) \), namely \( [T_n(\theta) > 0] = [T_n(\theta) = 0]^c \).
One of our main results is a zero-one law for the existence of triangles in random key graphs. These results will
be established by the method of first and second moments.
applied to the count variables \( \{12\} \), e.g., see [4, p. 2], [15, p. 55]. They are stated in terms of the quantity

\[
\tau(\theta) = \frac{K^3}{P^2} + \left( \frac{K^2}{P} \right)^3, \quad \theta = (K, P), \quad K, P = 1, 2, \ldots \tag{13}
\]

As we shall see soon in Proposition 3.2, this quantity gives the asymptotic probability of a triangle in random key graphs, when the parameters \( K \) and \( P \) are suitably scaled.

Key to much of the discussion carried out in this paper are the first two moments of the count variables \( \{12\} \). The first moment, computed next, will be conveniently expressed with the help of the quantity \( \beta(\theta) \) defined by

\[
\beta(\theta) = (1 - q(\theta))^3 + q(\theta)^3 - q(\theta)r(\theta) \tag{14}
\]

with \( r(\theta) \) defined by

\[
r(\theta) = \begin{cases} 0 & \text{if } P < 3K \\ \frac{(P - 2K)}{(2)} & \text{if } 3K \leq P. \end{cases} \tag{15}
\]

Note that \( r(\theta) \) corresponds to the probability \( \{6\} \) when \( |S| = 2K \).

**Proposition 2.1.** Fix \( n = 3, 4, \ldots \). For positive integers \( K \) and \( P \) such that \( K \leq P \), we have

\[
\mathbb{E}[\chi_{123}(\theta)] = \beta(\theta) \tag{16}
\]

with \( \beta(\theta) \) defined at \( \{14\} \), so that

\[
\mathbb{E}[T_n(\theta)] = n \cdot \frac{3}{3} \cdot \beta(\theta). \tag{17}
\]

A proof of Proposition 2.1 is given in Section 9.1. We see from \( \{16\} \) that the quantity \( \beta(\theta) \) gives the probability that three distinct vertices form a triangle in \( \mathbb{K}(n; \theta) \). For future reference, we note that

\[
r(\theta) \leq q(\theta)^2 \tag{18}
\]

by direct inspection, whence

\[
\beta(\theta) \geq (1 - q(\theta))^3 > 0. \tag{19}
\]

The second moment of the count variables \( \{12\} \) is computed next; it will play a crucial role in the proofs of both Theorem 3.3 and Theorem 3.7 that are forthcoming.

**Proposition 2.2.** For positive integers \( K \) and \( P \) such that \( K \leq P \), we have

\[
\mathbb{E}[T_n(\theta)^2] = \mathbb{E}[T_n(\theta)] + \left( \frac{n-3}{3} \right) + 3(\frac{(n-3)}{(3)})^2 \mathbb{E}[T_n(\theta)]^2 \\
+ 3(n-3) \cdot \frac{n}{3} \cdot \mathbb{E}[\chi_{123}(\theta)\chi_{124}(\theta)] \tag{20}
\]

for all \( n = 3, 4, \ldots \).

The proof of Proposition 2.2 is available in Section 9.2.

**3.1 Two asymptotic equivalences**

The two asymptotic equivalence results (under such scalings) presented next will prove useful in a number of places. They provide easy asymptotic expressions for the edge probability and for the probability of a triangle, respectively, in large random key graphs. The first one, already obtained in \( \{33\} \), is given here for easy reference.

**Lemma 3.1.** For any scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \), we have

\[
limit_{n \to \infty} q(\theta_n) = 1 \quad \text{if and only if} \quad \lim_{n \to \infty} \frac{K^2}{P^2} = 0, \tag{21}
\]

and under either condition at \( \{21\} \), the asymptotic equivalence

\[
1 - q(\theta_n) \sim \frac{K^2}{P_n} \tag{22}
\]

holds.

The next result shows that under certain conditions the quantity \( \{12\} \) behaves asymptotically like \( \{14\} \) (which gives the probability that three nodes form a triangle in random key graphs).

**Proposition 3.2.** For any scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \) satisfying \( \{21\} \), we have the asymptotic equivalence

\[
\beta(\theta_n) \sim \tau(\theta_n). \tag{23}
\]

A proof of Proposition 3.2 is given in Section 9.3. In words, this result shows that under \( \{21\} \) the probability of three vertices forming a triangle in random key graphs is asymptotically equivalent to

\[
\tau(\theta_n) = \frac{K^3}{P_n^2} + \left( \frac{K^2}{P_n} \right)^3. \tag{24}
\]

**3.2 Zero-one laws for the existence of triangles**

The zero-law, which is given first, is established in Section 10.1.

**Theorem 3.3.** For any scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \), the zero-law

\[
\lim_{n \to \infty} \mathbb{P}[T_n(\theta_n) > 0] = 0
\]

holds under the condition

\[
\lim_{n \to \infty} n^3 \tau(\theta_n) = 0. \tag{24}
\]

The one-law given next assumes a more involved form; its proof is given in Section 10.2.

**Theorem 3.4.** For any scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \) for which the limit \( \lim_{n \to \infty} q(\theta_n) = q^* \) exists, the one-law

\[
\lim_{n \to \infty} \mathbb{P}[T_n(\theta_n) > 0] = 1
\]

holds if either \( 0 \leq q^* < 1 \), or if \( q^* = 1 \) and the additional condition

\[
\lim_{n \to \infty} n^3 \tau(\theta_n) = \infty \tag{25}
\]

holds.

To facilitate an upcoming comparison with analogous results in ER graphs, we combine Theorem 3.3 and Theorem 3.4 into a single symmetric statement.
Theorem 3.5. For any scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \) for which \( \lim_{n \to \infty} q(\theta_n) \) exists, we have

\[
\lim_{n \to \infty} P[T_n(\theta_n) > 0] = \begin{cases} 
0 & \text{if } \lim_{n \to \infty} n^3 \tau(\theta_n) = 0 \\
1 & \text{if } \lim_{n \to \infty} n^3 \tau(\theta_n) = \infty.
\end{cases}
\]

By Lemma 5.1 the condition \( \lim_{n \to \infty} n^3 \tau(\theta_n) = 0 \) implies \( \lim_{n \to \infty} q(\theta_n) = 1 \), hence he limit \( \lim_{n \to \infty} q(\theta_n) \) necessarily exists with \( q^* = 1 \).

3.3 Clustering in random key graphs

In accordance with definition (19), the clustering coefficient of the random key graph \( \mathbb{K}(n; \theta) \) is defined by

\[
C_K(\theta) = \mathbb{P}[E_{12}(\theta) | E_{13}(\theta) \cap E_{23}(\theta)].
\]

A closed form expression for this quantity is given next.

Proposition 3.6. For positive integers \( K, P \) such that \( K \leq P \), we have

\[
C_K(\theta) = \frac{\beta(\theta)}{(1 - q(\theta))^2}
\]

with \( \beta(\theta) \) given by (14).

Proof. The definitions of \( C_K(\theta) \) and \( \chi_{123}(\theta) \) yield

\[
C_K(\theta) = \frac{\mathbb{P}[E_{12}(\theta) \cap E_{13}(\theta) \cap E_{23}(\theta)]}{\mathbb{P}[E_{13}(\theta) \cap E_{23}(\theta)]} = \frac{\mathbb{E}[\chi_{123}(\theta)]}{(1 - q(\theta))^2}
\]

since the events \( E_{13}(\theta) \) and \( E_{23}(\theta) \) are independent, with

\[
\mathbb{P}[E_{13}(\theta) \cap E_{23}(\theta)] = \mathbb{P}[K_1(\theta) \cap K_3(\theta) \neq \emptyset, K_2(\theta) \cap K_3(\theta) \neq \emptyset]
\]

\[
= (1 - q(\theta))^2
\]

by virtue of (9) (and comments following it). The conclusion (27) is immediate upon substituting (16) into (28). \( \square \)

For random key graphs there is strong consistency between the definitions (19) and (25) of clustering coefficient.

Theorem 3.7. For positive integers \( K, P \) such that \( K \leq P \), we have

\[
\lim_{n \to \infty} C^*(\mathbb{K}(n; \theta)) = C_K(\theta) \quad \text{a.s.}
\]

A proof of Theorem 3.7 is given in Section 10.3. To the best of our knowledge, Theorem 3.7 is the first rigorous result in the literature that shows that the conditional probability definition (19) of clustering coefficient converges asymptotically almost surely to the empirical clustering coefficient measure of (9). For instance, Deijfen and Kets indicated (2), for another class of random graphs, that the two definitions should be closely related, but that a rigorous proof would need significant additional work.

Simulation results given in Table 1 illustrate the convergence (30) for several realistic parameter values. The numerical values of \( C_K(\theta) \) are obtained directly from the expressions (25). The quantity \( C^*_n(\theta) \) stands for the clustering coefficient of \( \mathbb{K}(n; \theta) \), calculated through (9) and averaged over 1000 realizations; the number of nodes is set to \( n = 1000 \) in all simulations. The data support the validity of (30), and confirm the claim that for large networks the quantity (9) captures essentially the same structural information as (25).

### Table 1: Clustering coefficients with fixed \( \theta \) for random key graphs

| \( K \) | \( P \) | \( 1 - q(\theta) \) | \( C_K(\theta) \) | \( C^*_n(\theta) \) |
|---|---|---|---|---|
| 4  | 10^2 | 0.0159 | 0.2590 | 0.2587 |
| 8  | 5 \times 10^3 | 0.0127 | 0.1348 | 0.1349 |
| 16 | 2 \times 10^4 | 0.0127 | 0.0737 | 0.0736 |
| 20 | 4 \times 10^4 | 0.0100 | 0.0590 | 0.0590 |
| 24 | 10^5 | 0.0057 | 0.0469 | 0.0468 |
| 32 | 10^5 | 0.0102 | 0.0408 | 0.0408 |
| 40 | 5 \times 10^5 | 0.0032 | 0.0280 | 0.0280 |
| 64 | 10^6 | 0.0041 | 0.0196 | 0.0196 |

4 Facts concerning Erdős-Rényi graphs

A little later in this paper, we shall compare random key graphs to related Erdős-Rényi (ER) graphs (8), but first some notation: For each \( n = 2, 3, \ldots \) and each \( p \) in \( [0, 1] \), let \( G(n; p) \) denote the ER graph on the vertex set \( \{1, \ldots, n\} \) with edge probability \( p \). The ER graph \( G(n; p) \) is characterized by the fact that the \( \binom{n(n-1)}{2} \) possible undirected edges between the \( n \) nodes are independently assigned with probability \( p \). Thus, if in analogy with earlier notation, with distinct \( i, j, 1, \ldots, n \), we denote by \( E_{ij}(p) \) the event that there is an (undirected) edge between nodes \( i \) and \( j \) in \( G(n; p) \), then the events \( E_{ij}(p) \) are mutually independent, each of probability \( p \). For ease of exposition it will always be understood that \( E_{ij}(p) = E_{ji}(p) \) for distinct \( i, j, 1, \ldots, n \).

Random key graphs are not stochastically equivalent to ER graphs even when their edge probabilities are matched exactly: As graph-valued rvs, the random graphs \( G(n; p) \) and \( \mathbb{K}(n; \theta) \) have different distributions even under the exact matching condition

\[
p = 1 - q(\theta) = p(\theta).
\]

See (29) for a discussion of (dis)similarities. Under (31) the random graphs \( G(n; p) \) and \( \mathbb{K}(n; \theta) \) are said to be exactly matched.

In analogy with (12) let \( T_n(p) \) denote the number of distinct triangles in \( G(n; p) \). Under the enforced independence, we note that

\[
E[T_n(p)] = \binom{n}{3} \tau^*(p), \quad n = 3, 4, \ldots
\]

with

\[
\tau^*(p) = p^3, \quad 0 \leq p \leq 1.
\]

The edge assignment rvs being exchangeable in ER graphs, we can again define the clustering coefficient in \( G(n; p) \) according to (10) by setting

\[
C_{ER}(p) = \mathbb{P}[E_{12}(p) | E_{13}(p) \cap E_{23}(p)].
\]

By mutual independence of the edge rvs it follows that

\[
C_{ER}(p) = \frac{\mathbb{P}[E_{12}(p) \cap E_{13}(p) \cap E_{23}(p)]}{\mathbb{P}[E_{13}(p) \cap E_{23}(p)]} = p.
\]

Here as well, strong consistency holds between the two notions of clustering (9) and (25).

Theorem 4.1. For every \( p \) in \( (0, 1) \), we have

\[
\lim_{n \to \infty} C^*(G(n; p)) = C_{ER}(p) \quad \text{a.s.}
\]
This result can be established by arguments similar to the ones provided in the proof of Proposition 4.4, see Appendix A for details. Table II expands on Table I given earlier in that we now compare the clustering coefficients of exactly matched random key graphs and ER graphs for the parameter values used in Table I. The quantities for random key graphs are as before. The numerical values of \( C_{ER}(p) \) are obtained directly from the expressions (33). Here \( C_{n}^{\star} (p) \) stands for the clustering coefficient of \( G(n; p) \). It is calculated through (9) and averaged over 1000 realizations. The number of nodes is still set to \( n = 1000 \) in all simulations. Again the data support the claim that for large networks the definition (9) captures essentially the same information as the quantity (33).

Any mapping \( p : N_{0} \rightarrow [0, 1] \) will be called a scaling for ER graphs. In order to meaningfully compare the asymptotic regime of random key graphs with that of ER graphs under their respective scalings, we shall say that the scaling \( p : N_{0} \rightarrow [0, 1] \) (for ER graphs) is asymptotically matched to the scaling \( P, K : N_{0} \rightarrow N_{0} \) (for random key graphs) if
\[
p_n \sim p(\theta_n) = 1 - q(\theta_n).
\]

(36)

Sometimes, when (36) holds, we shall also say that the random graphs \( G(n; p_n) \) and \( G(n; \theta_n) \) are asymptotically matched. Under condition (31), by Lemma (34), the asymptotic matching condition (36) amounts to
\[
p_n \sim \frac{K^2}{P_n}.
\]

(37)

Condition (31) (resp. (36)) is equivalent to requiring that the expected degrees in \( G(n; \theta_n) \) and \( G(n; \theta_n) \) and \( G(n; p_n) \) (resp. \( G(n; \theta_n) \) and \( G(n; p_n) \)) coincide (resp. are asymptotically equivalent).

### 5. Comparing the Number of Triangles in Random Key Graphs and ER Graphs

Fix \( p \) in \((0, 1)\), and positive integers \( K \) and \( P \) such that \( K \leq P \). From (17) and (32) it is plain that
\[
\frac{\mathbb{E}[T_n(\theta)]}{\mathbb{E}[T_n(p)]} = \frac{\beta(\theta)}{\tau^\star(p)} = n = 3, 4, \ldots
\]

(38)

Under the exact matching condition (31), with \( p(\theta) \) given by (5), this last expression yields
\[
\frac{\mathbb{E}[T_n(\theta)]}{\mathbb{E}[T_n(p(\theta))]} = \frac{\beta(\theta)}{\tau^\star(p(\theta))} = 1 + \frac{q(\theta)^2 - 1}{1 - q(\theta)} \cdot q(\theta)
\]

for each \( n = 3, 4, \ldots \), whence
\[
\mathbb{E}[T_n(p(\theta))] \leq \mathbb{E}[T_n(\theta)], \quad n = 3, 4, \ldots
\]

by virtue of (18). Consequently, the expected number of triangles in a random key graph is always at least as large as the corresponding quantity in an ER graph exactly matched to it. This was already suggested by Di Pietro et al. [27] with the help of limited simulations.

An analogous result is available when the scalings are only asymptotically matched.

**Corollary 5.1.** Consider a scaling \( K, P : N_0 \rightarrow N_0 \) satisfying (21), and a scaling \( p : N_0 \rightarrow [0, 1] \). Under the asymptotic matching condition (35), we have the equivalence
\[
\frac{\mathbb{E}[T_n(\theta_n)]}{\mathbb{E}[T_n(p_n)]} \sim 1 + \frac{P_n}{K^3_n}
\]

(39)

In other words, for large \( n \) the expected number of triangles in random key graphs is always at least as large as the corresponding quantity in asymptotically matched ER graphs – In fact, if the ratio \( P_n/K^3_n \) is large, the number of triangles in random key graphs can be several orders of magnitude larger than that of ER graphs. In Sections 7 and 8 this issue is explored in the context of wireless sensor networks and social networks, respectively.

**Proof.** Replacing \( \theta \) by \( \theta_n \) and \( p \) by \( p_n \), according to the given scalings in the expression (38), we get
\[
\frac{\mathbb{E}[T_n(\theta_n)]}{\mathbb{E}[T_n(p_n)]} = \frac{\beta(\theta_n)}{\tau^\star(p_n)} = n = 3, 4, \ldots
\]

Under (21), Proposition (5.2) yields
\[
\frac{\mathbb{E}[T_n(\theta_n)]}{\mathbb{E}[T_n(p_n)]} \sim \frac{\tau(\theta_n)}{\tau^\star(p_n)}
\]

(40)

with
\[
\frac{\tau(\theta_n)}{\tau^\star(p_n)} = \frac{1}{p_n^3} \left( \frac{K^3_n}{P_n^2} \right) + \frac{1}{p_n^3} \left( \frac{K^3_n}{P_n} \right)^3, \quad n = 3, 4, \ldots
\]

With the help of (37), we conclude
\[
\frac{\tau(\theta_n)}{\tau^\star(p_n)} \sim 1 + \frac{P_n}{K^3_n}
\]

(41)

and the equivalence (39) follows from (40).

From (41) it follows that under the asymptotic matching condition (35) (together with (21)), triangles will start appearing earlier in the evolution of a random key graph as compared to an ER graph (asymptotically) matched to it. It should also be clear from (41) that the larger the quantity \( P_n/K^3_n \), the more pronounced will such difference be.

We close this section by comparing Theorem (3.3) with its analog for ER graphs. Fix \( n = 3, 4, \ldots \) and \( p \) in \([0, 1]\). Consider the event that there exists at least one triangle in \( G(n; p) \), i.e., \( T_n(p) > 0 \). The following zero-one law for triangle containment in ER graphs is well known [3] Chap. 4, [15] Thm. 3.4, p. 56.

**Theorem 5.2.** For any scaling \( p : N_0 \rightarrow [0, 1] \), we have
\[
\lim_{n \to \infty} \mathbb{P}[T_n(p) > 0] = \begin{cases} 
0 & \text{if } \lim_{n \to \infty} n^3 \tau^\star(p_n) = 0 \\
1 & \text{if } \lim_{n \to \infty} n^3 \tau^\star(p_n) = \infty.
\end{cases}
\]
This result, which is also established by the method of first and second moments, is easily understood once we recall (32). As we compare Theorem 3.3 with Theorem 3.2, we note a direct analogy since the terms \( \tau (\theta_n) \) and \( \tau^* (p_n) \) correspond to the (asymptotic) probability that three arbitrary nodes form a triangle in random key graphs and ER graphs, respectively.

6. Comparing the Clustering Coefficients of Random Key Graphs and ER Graphs

Fix \( p \in (0, 1) \) and positive integers \( K \) and \( P \) such that \( K \leq P \). Combining (27) and (34) we get

\[
C_K (\theta) = \frac{\beta (\theta)}{\theta (1 - \theta)^2},
\]

Under the exact matching condition (31) we find

\[
\frac{C_K (\theta)}{C_{\text{ER}} (p(\theta))} = \frac{\beta (\theta)}{(1 - q(\theta))^2} \cdot q(\theta) \tag{42}
\]

and we recall (32). As we compare Theorem 3.5 with Theorem 3.2, we note a direct analogy since the terms \( \tau (\theta_n) \) and \( \tau^* (p_n) \) correspond to the (asymptotic) probability that three arbitrary nodes form a triangle in random key graphs and ER graphs, respectively.

Several conclusions can be extracted from these expressions: Equality in (44) holds only when \( P < 2K \), i.e., from (4) we get

\[
\frac{C_K (\theta)}{C_{\text{ER}} (p(\theta))} = 1 \quad \text{if} \quad K \leq P < 2K
\]

since then \( q(\theta) = r(\theta) = 0 \). If \( 2K \leq P < 3K \), then \( 0 < q(\theta) < 1 \) but \( r(\theta) = 0 \), whence

\[
\frac{C_K (\theta)}{C_{\text{ER}} (p(\theta))} = 1 + \left( \frac{q(\theta)}{1 - q(\theta)} \right)^3 > 1.
\]

Understanding the case \( 3K \leq P \) is more challenging due to a lack of simple expressions. Therefore, before dealing with the case of an arbitrary positive integer \( K \), we first consider a couple of special cases as a way to explore the relative ranges possibly exhibited by the clustering coefficients. For \( K = 1 \) it is a simple matter to check from (43) that

\[
\frac{C_K (1, P)}{C_{\text{ER}} (p(\theta))} = P
\]

for each \( P = 2, 3, \ldots \). For \( K = 2 \) uninteresting calculations show that

\[
\frac{C_K (2, P)}{C_{\text{ER}} (p(\theta))} = \frac{P}{2} \cdot \frac{2P^3 - 4P^2 - P + 3}{(2P - 3)^3}
\]

for each \( P = 6, 7, \ldots \), whence

\[
\frac{P}{8} < \frac{C_K (2, P)}{C_{\text{ER}} (p(\theta))} < P \tag{46}
\]

on that range. This upper bound is seen to hold by noting that

\[
4(2P^3 - 4P^2 - P + 3) = (2P - 3)^3 + (P - 1)(20P - 38) + 1 > (2P - 3)^3 \quad \text{for all} \quad P = 2, 3, \ldots
\]

The lower bound follows from the easily checked fact that

\[
2P^3 - 4P^2 - P + 3 < 2(2P - 3)^3 \quad \text{for all} \quad P = 2, 3, \ldots
\]

The cases \( K = 1 \) and \( K = 2 \) may not be interesting from the perspective of envisioned modeling applications of random key graphs. However, the discussion already shows that the parameters of the corresponding random key graph can be selected (e.g., by taking \( P \) very large in these two cases) so that it has a much larger clustering coefficient than the ER graph exactly matched to it. Additional limited numerical evidence along these lines is also available in Table II discussed earlier. In fact, for any given \( K \) we see that the linear behavior found in (45) and (46) holds asymptotically for large \( P \).

**Corollary 6.1.** For each positive integer \( K \), it holds that

\[
\frac{C_K (\theta)}{C_{\text{ER}} (p(\theta))} \sim 1 + \frac{P}{K^3} \quad (P \to \infty). \tag{47}
\]

Thus, exactly matched random key graphs and ER graphs will have vastly different clustering coefficients when \( P \) is large. This will be especially so for WSNs where the size of the key pool \( P \) in the Eschenauer-Gligor scheme is expected to be in the range \( 2^{17} - 2^{20} \) (with \( K \) much smaller).

**Proof.** Fix positive integers \( K \) and \( P \) such that \( 2K \leq P \). We can rewrite (43) as

\[
\frac{C_K (\theta)}{C_{\text{ER}} (p(\theta))} = 1 + \left( \frac{q(\theta)}{1 - q(\theta)} \right)^3 \left( 1 - \frac{r(\theta)}{q(\theta)^2} \right). \tag{48}
\]

With \( K \) fixed and \( P \) getting large, we see from Lemma 3.1 that \( 1 - q(\theta) \sim \frac{K^2}{P^2} \) and \( q(\theta) \sim 1 (P \to \infty) \), so that

\[
\left( \frac{q(\theta)}{1 - q(\theta)} \right)^3 \sim \left( \frac{P}{K^2} \right)^3 \quad (P \to \infty).
\]

The arguments given in the proof of Proposition 3.2 to establish (49) can also be used to establish

\[
1 - \frac{r(\theta)}{q(\theta)^2} \sim \frac{K^3}{P^2} \quad (P \to \infty). \tag{49}
\]

Collecting we conclude to the validity of (47).

Next we compare the clustering coefficients of asymptotically matched random key graphs and ER graphs when the parameters \( \theta \) and \( p \) are scaled with \( n \).

**Corollary 6.2.** Consider a scaling \( K, P : \mathbb{N}_0 \to \mathbb{N}_0 \) satisfying (27) and a scaling \( p : \mathbb{N}_0 \to [0, 1] \). Under the asymptotic matching condition (50), we have the equivalence

\[
\frac{C_K (\theta_n)}{C_{\text{ER}} (p_n)} \sim 1 + \frac{P_n}{K_n^3}, \tag{50}
\]

**Proof.** As we replace \( \theta \) by \( \theta_n \) and \( p \) by \( p_n \) according to these scalings in the expression (42), we get

\[
\frac{C_K (\theta_n)}{C_{\text{ER}} (p_n)} = \frac{\beta (\theta_n)}{p_n (1 - q(\theta_n))^2}, \quad n = 3, 4, \ldots \tag{51}
\]

Note that

\[
\frac{C_K (\theta_n)}{C_{\text{ER}} (p_n)} \sim \frac{\beta (\theta_n)}{(1 - q(\theta_n))^3} \sim \frac{\tau (\theta_n)}{(1 - q(\theta_n))^3}. \tag{52}
\]
The first equivalence is a consequence of (56) while the second equivalence follows by Proposition 5.2 under (21). With (57) being still valid here, we easily conclude (58) by the same arguments as the ones used to obtain (39). 

Under (21) and (56), we conclude that
\[ \lim_{n \to \infty} \frac{C_K(\theta_n)}{C_{\text{ER}}(p_n)} = 1 \quad \text{if} \quad \lim_{n \to \infty} \frac{K^3}{P_n} = \infty, \quad (53) \]
and
\[ \lim_{n \to \infty} \frac{C_K(\theta_n)}{C_{\text{ER}}(p_n)} = \infty \quad \text{if} \quad \lim_{n \to \infty} \frac{K^3}{P_n} = 0. \quad (54) \]

Thus, asymptotically matched random key graphs and ER graphs can in principle have vastly different clustering coefficients. We explore this possibility in the next two sections where the implications of the main results are discussed in the context of wireless sensor networks and of social networks based on common interest relationships.

7 Wireless Sensor Networks

Random key graphs were originally introduced to model the random key pre-distribution scheme proposed by Eschenauer and Gligor [2] in the context of WSNs. When the WSN comprises \( n \) nodes, it is natural to select the parameters \( K_n \) and \( P_n \) in order for the induced random key graph to be connected. However, there is a tradeoff between connectivity and security [2], requiring that \( \frac{n}{K_n} \) be kept as close as possible to the critical scaling \( \frac{\log n}{c} \) for connectivity (but above it); see the papers [3, 7, 24, 28, 33]. The desired regime near the boundary can be achieved by taking
\[ \frac{K_n^2}{P_n} \sim c \cdot \frac{\log n}{n} \quad (55) \]
with \( c > 1 \) but close to one.

Now, consider the situation where the random key graph \( K(n; \theta_n) \) is matched asymptotically to the ER random graph \( G(n; p_n) \) under the asymptotic matching condition (56). It follows from (59) that
\[ \frac{\mathbb{E}[T_n(\theta_n)]}{\mathbb{E}[T_n(p_n)]} \sim 1 \quad \text{if and only if} \quad \frac{P_n}{K_n^3} = o(1) \quad (56) \]
under the condition (21). This last condition obviously occurs when (55) holds, in which case the condition at (56) amounts to taking
\[ \frac{1}{K_n} = o(1) \left( \frac{c}{\log n} \right). \]
Thus, under the connectivity condition (55) it holds that
\[ \frac{\mathbb{E}[T_n(\theta_n)]}{\mathbb{E}[T_n(p_n)]} \sim 1 \quad \text{if and only if} \quad \lim_{n \to \infty} \frac{K_n}{n/\log n} = \infty. \quad (57) \]
The expected number of triangles in random key graphs is then of the same order as the corresponding quantity in asymptotically matched ER graphs with \( \frac{\mathbb{E}[T_n(\theta_n)]}{\mathbb{E}[T_n(p_n)]} \sim \frac{\log n}{c} \). This is a direct consequence of (52), (57) and (55). This conclusion holds regardless of the value of \( c \) in (55).

However, given the limited memory and computational power of the sensor nodes, key ring sizes satisfying (57) are not practical since requiring \( K_n \gg \frac{n}{\log n} \). Furthermore, they will also result in high node degrees, and this in turn will decrease network resiliency against node capture attacks. It was proposed by Di Pietro et al. [7] Thm. 5.3 that resiliency in large WSNs against node capture attacks can be ensured by selecting \( K_n \) and \( P_n \) such that \( \frac{K_n}{P_n} \sim \frac{1}{n} \). Under (55) this additional requirement then leads to \( K_n \sim c \cdot \log n \), whence \( P_n \sim c \cdot n \log n \), and (59) now implies
\[ \frac{K_n^2}{P_n} \sim c \cdot \frac{\log n}{n} \quad (59) \]

Therefore, for such realistic WSN implementations the expected number of triangles in the induced random key graphs will be orders of magnitude larger than in ER graphs.

Concerning the clustering coefficients, we see that under the condition (55), (53) can hold only if the key ring size \( K \) is much larger than \( n/\log n \). As already discussed, this condition can not be satisfied in a practical WSN scenario due to storage limitations at the sensor nodes and security constraints. In fact, we see from (39) and (58) that, in a realistic WSN, the condition (54) is always in effect and the clustering coefficient of the random key graph is much larger than that of the asymptotically matched ER graph.

8 Social Networks — Can Random Key Graphs Be Small Worlds?

With an obvious change in terminology, random key graphs can be used to model certain types of social networks, e.g., see [2, 57]; Instead of viewing \( \{1, \ldots, P\} \) as a collection of cryptographic keys randomly assigned to the nodes of a WSN according to the Eschenauer-Gligor scheme, we can think of it as a list of “interests,” e.g., hobbies, books, movies, sports, etc., which are pursued by the members of a social group. In that reformulation, the i.i.d. random sets \( K_1(\theta), \ldots, K_n(\theta) \) appearing in the definition of the random key graph \( \mathbb{K}(n; \theta) \) can now be interpreted as the interests assigned to the individual members of that group. The random key graph \( \mathbb{K}(n; \theta) \) then naturally describes a common-interest relationship between community members since two individuals are now adjacent in \( \mathbb{K}(n; \theta) \) when they have at least one interest in common.

In parallel to the discussion given in Section 7 for WSNs, we explore the parameter ranges likely to appear in practice for random key graphs modeling social networks. We do so with an eye towards understanding the behavior of the expression appearing at (39).

We begin with the observation that most real-world social networks are known to be sparse in the sense that the expected number of edges per node appears to remain (nearly) constant as the size of the network increases. In the case of random key graphs, the expected degree of a node is given by \( (n - 1)(1 - q(\theta_n)) \) and sparsity amounts to \( 1 - q(\theta_n) \sim \frac{1}{n} \) for some \( c > 0 \), or equivalently, to
\[ \frac{K_n^2}{P_n} \sim c \cdot \frac{\log n}{n} \quad (59) \]

1. Here we assume that each individual has exactly \( K \) interests drawn from the list \( \{1, \ldots, P\} \). More realistic models can be obtained through more complex randomization mechanisms as in the work of Godehardt et al. on general random intersection graphs [11, 12] and as in the work of Yağan on inhomogeneous random key graphs [35].
by virtue of Lemma \[3.4\] whence
\[
P_n \sim \frac{n}{cK_n}.
\]

In view of Corollary 5.1 and Corollary 5.2 in the sparse regime, random key graphs will have many more triangles and will be much more clustered (by orders of magnitude) than the asymptotically matched ER graphs unless
\[
\limsup_{n \to \infty} \frac{n}{K_n} < \infty.
\]
This condition is equivalent to
\[
K_n = \Omega(n),
\]
and is even more stringent than the corresponding condition \[57\] derived for WSN applications. More importantly, under the condition \[59\] we have \(P_n \sim c^{-1} nK_n\), requiring
\[
P_n = \Omega(n^3)
\]
if \[62\] is also enforced. Thus, under \[59\] and \[62\] generating the random key graph will require each of the \(n\) nodes to choose \(K_n = \Omega(n)\) objects from a universe of size \(P_n = \Omega(n^3)\). The computational complexity of this task quickly becomes prohibitively high as the number of individuals in the social network becomes large. Yet, we would expect the realistic values for the number \(K_n\) of interests of a single individual to be much smaller than the network size \(n\), in sharp contrast with \[62\]. In other words, the condition \[62\] is naturally eliminated in realistic applications of random key graphs to such social networks – The resulting random key graphs will naturally have very high clustering and contain very large number of triangles when used for social network modeling.

Since random key graphs can be highly clustered, a natural question arises as to their suitability for modeling the small world effect. This notion is linked to a well-known series of experiments conducted by Milgram \[19\] in the late sixties. The results, commonly known as six degrees of separation, suggest that the social network of people in the United States is small in the sense that path lengths between pairs of individuals are short. As a way to capture Milgram’s experiments, Watts and Strogatz \[27\] introduced small world network models that are highly clustered and yet have a small average path length. More precisely, a random graph is considered to be a small world if its average path length is of the same order as that of an ER graph with the same expected average degree, but with a much larger clustering coefficient.

The results of this paper already show that random key graphs can satisfy the high clustering coefficient requirement of a small world. Under \[55\], Rybaczky \[23\] has shown that
\[
diam[K(n; \theta_n)] \sim \frac{\log n}{\log \log n}
\]
with high probability where \(K(n; \theta_n)\) is the largest connected component of \(K(n; \theta_n)\). This suggests that the diameter, hence the average path length, in random key graphs is small as was the case with ER graphs \[5\]. We also note \[31\] Corollary 5.2 that random key graphs have very small (e.g., \(\leq 2\)) diameter under certain parameter ranges (e.g., with \(P_n = O(n^\delta)\) with \(0 < \delta < \frac{1}{2}\)). Thus, random key graphs may indeed be considered good candidate models for small worlds!

9 \enspace PROOFS OF THE PRELIMINARY RESULTS

In Sections 9.1 and 9.2 we fix positive integers \(K\) and \(P\) such that \(K \leq P\), and \(n = 3, 4, \ldots\).

9.1 A proof of Proposition 2.1

As exchangeability yields \[17\], we need only show the validity of \[16\]. We make repeated use of the fact that for any pair of events \(E\) and \(F\) in \(\mathcal{F}\), we have
\[
\mathbb{P}[E \cap F] = \mathbb{P}[E] - \mathbb{P}[E \cap F^c].
\]
Thus, by repeated application of \[55\] we find
\[
\mathbb{E}[\chi_{123}(\theta)] = \mathbb{P}\left[ K_1(\theta) \cap K_2(\theta) \neq \emptyset, K_1(\theta) \cap K_3(\theta) \neq \emptyset, K_2(\theta) \cap K_3(\theta) \neq \emptyset \right] = \mathbb{P}[K_1(\theta) \cap K_2(\theta) \neq \emptyset] - \mathbb{P}[K_1(\theta) \cap K_3(\theta) \neq \emptyset] + \mathbb{P}[K_2(\theta) \cap K_3(\theta) \neq \emptyset] - \mathbb{P}[K_1(\theta) \cap K_2(\theta) \neq \emptyset, K_1(\theta) \cap K_3(\theta) \neq \emptyset, K_2(\theta) \cap K_3(\theta) \neq \emptyset].
\]

By independence, with the help of \[5\], we readily obtain the expressions
\[
\mathbb{P}[K_1(\theta) \cap K_2(\theta) \neq \emptyset, K_1(\theta) \cap K_3(\theta) \neq \emptyset] = (1 - q(\theta))^2
\]
and
\[
\mathbb{P}[K_1(\theta) \cap K_2(\theta) \neq \emptyset, K_2(\theta) \cap K_3(\theta) = \emptyset] = (1 - q(\theta)) q(\theta).
\]

Next, as we use \[63\] one more time, we get
\[
\mathbb{P}\left[ K_1(\theta) \cap K_2(\theta) \neq \emptyset, K_1(\theta) \cap K_3(\theta) = \emptyset, K_2(\theta) \cap K_3(\theta) = \emptyset \right] = \mathbb{P}[K_1(\theta) \cap K_2(\theta) \neq \emptyset] - \mathbb{P}[K_1(\theta) \cap K_2(\theta) \neq \emptyset, K_1(\theta) \cap K_3(\theta) = \emptyset] + \mathbb{P}[K_2(\theta) \cap K_3(\theta) = \emptyset].
\]

Again, by independence, with the help of \[5\] we conclude that
\[
\mathbb{P}[K_1(\theta) \cap K_3(\theta) = \emptyset, K_2(\theta) \cap K_3(\theta) = \emptyset] = q(\theta)^2
\]
and
\[
\mathbb{P}\left[ K_1(\theta) \cap K_2(\theta) = \emptyset, K_1(\theta) \cap K_3(\theta) = \emptyset, K_2(\theta) \cap K_3(\theta) = \emptyset \right] = \mathbb{P}[K_1(\theta) \cap K_2(\theta) = \emptyset] - \mathbb{P}[K_1(\theta) \cap K_2(\theta) = \emptyset, K_1(\theta) \cap K_3(\theta) = \emptyset] + \mathbb{P}[K_2(\theta) \cap K_3(\theta) = \emptyset].
\]

since \(|K_1(\theta) \cup K_2(\theta)| = 2K\) when \(K_1(\theta) \cap K_2(\theta) = \emptyset\).

Collecting these facts we find
\[
\mathbb{E}[\chi_{123}(\theta)] = (1 - q(\theta))^2 - (1 - q(\theta)) q(\theta) + q(\theta)^2 - q(\theta) r(\theta)
\]
and the conclusion \[16\] follows by elementary algebra.
9.2 A proof of Proposition 2.2

By exchangeability and the binary nature of the rvs involved we readily obtain

\[
\mathbb{E} [T_n(\theta)^2] = \mathbb{E} [T_n(\theta)] + \binom{n}{3} \binom{n-3}{2} \binom{n-3}{1} \mathbb{E} [\chi_{123}(\theta)\chi_{124}(\theta)] + \binom{n}{3} \binom{n-3}{2} \binom{n-3}{1} \mathbb{E} [\chi_{123}(\theta)\chi_{145}(\theta)] + \binom{n}{3} \binom{n-3}{2} \binom{n-3}{1} \mathbb{E} [\chi_{123}(\theta)\chi_{456}(\theta)]. \quad (64)
\]

Under the enforced independence assumptions the rvs \( \chi_{123}(\theta) \) and \( \chi_{456}(\theta) \) are independent and identically distributed. As a result,

\[
\mathbb{E} [\chi_{123}(\theta)\chi_{456}(\theta)] = \mathbb{E} [\chi_{123}(\theta)] \mathbb{E} [\chi_{456}(\theta)] = \beta(\theta)^2,
\]

and using the relation \( (12) \) yields

\[
\binom{n}{3} \binom{n-3}{2} \binom{n-3}{1} \mathbb{E} [\chi_{123}(\theta)\chi_{456}(\theta)] = \binom{n-3}{3} \left( \mathbb{E} [T_n(\theta)] \right)^2. \quad (65)
\]

On the other hand, with the help of \( (5) \) we readily check that the indicator rvs \( \chi_{123}(\theta) \) and \( \chi_{145}(\theta) \) are independent and identically distributed conditioned on \( K_1(\theta) \) with

\[
\mathbb{P} [\chi_{123}(\theta) = 1 | K_1(\theta)] = \mathbb{P} [\chi_{123}(\theta) = 1] = \beta(\theta). \quad (66)
\]

As a similar statement applies to \( \chi_{145}(\theta) \), we conclude that the rvs \( \chi_{123}(\theta) \) and \( \chi_{145}(\theta) \) are (unconditionally) independent and identically distributed with

\[
\mathbb{E} [\chi_{123}(\theta)\chi_{145}(\theta)] = \mathbb{E} [\chi_{123}(\theta)] \mathbb{E} [\chi_{145}(\theta)] = \beta(\theta)^2.
\]

Again by virtue of \( (17) \), this last observation yields

\[
\binom{n}{3} \binom{n-3}{2} \binom{n-3}{1} \mathbb{E} [\chi_{123}(\theta)\chi_{145}(\theta)] = 3 \binom{n-3}{2} \left( \mathbb{E} [T_n(\theta)] \right)^2. \quad (67)
\]

Substituting \( (65) \) and \( (67) \) into \( (64) \) establishes Proposition 2.2.

9.3 A proof of Proposition 3.2

Since \( 1 \leq K_n \leq K_n^2 \) for all \( n = 1, 2, \ldots \), the condition \( (21) \) implies both

\[
\lim_{n \to \infty} \frac{1}{P_n} = 0 \quad \text{and} \quad \lim_{n \to \infty} \frac{K_n}{P_n} = 0. \quad (68)
\]

Therefore, \( \lim_{n \to \infty} P_n = \infty \), and for any \( c > 0 \), we have \( cK_n < P_n \) for all \( n \) sufficiently large in \( \mathbb{N}_0 \) (dependent on \( c \)). Thus, we have \( 3K_n < P_n \) for all \( n \) sufficiently large in \( \mathbb{N}_0 \). On that range we can use the expression \( (14) \) to write

\[
\beta(\theta_n) = (1 - q(\theta_n))^3 + q(\theta_n)^3 \left( 1 - \frac{r(\theta_n)}{q(\theta_n)} \right)^2.
\]

As Lemma \( 3.1 \) already implies \( q(\theta_n)^3 \sim 1 \) and \((1 - q(\theta_n))^3 \sim \left( \frac{K_n}{P_n} \right)^3 \), the asymptotic equivalence \( \beta(\theta_n) \sim \tau(\theta_n) \) will be established if we show that

\[
1 - \frac{r(\theta_n)}{q(\theta_n)^2} \sim \frac{K_n^3}{P_n^3}. \quad (69)
\]

This is an easy consequence of the fact that all terms involved are non-negative.

To establish \( (69) \) we proceed as follows: With positive integers \( K, P \) such that \( 3K \leq P \), we note that

\[
\frac{r(\theta)}{q(\theta)^2} = \left( \frac{(P - 2K)!}{(P - K)!} \right)^2 \left( \frac{(P - 3K)!}{(P - 2K)!} \right)^3 \mathbb{P} \left[ \chi_{123}(\theta) = 1 | K_1(\theta) \right] \mathbb{P} \left[ \chi_{145}(\theta) = 1 | K_1(\theta) \right]
\]

\[
= \left( \frac{(P - 2K)!}{(P - K)!} \right)^2 \left( \frac{(P - 3K)!}{(P - 2K)!} \right)^3 \mathbb{P} \left[ \chi_{123}(\theta) = 1 | K_1(\theta) \right] \mathbb{P} \left[ \chi_{145}(\theta) = 1 | K_1(\theta) \right]
\]

\[
= \prod_{\ell = 0}^{K-1} \left( 1 - \frac{K}{P - K} \right) \prod_{\ell = 0}^{K-1} \left( 1 + \frac{K}{P - K} \right)
\]

Upon grouping factors appropriately, Elementary bounding arguments now yield the two bounds

\[
1 - \left( 1 - \left( \frac{K}{P - K} \right)^2 \right)^K \leq 1 - \frac{r(\theta)}{q(\theta)^2}
\]

and

\[
1 - \frac{r(\theta)}{q(\theta)^2} \leq 1 - \left( 1 - \left( \frac{K}{P - 2K} \right)^2 \right)^K.
\]

Pick a scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \) satisfying the equivalent conditions \( (21) \) and consider \( n \) sufficiently large in \( \mathbb{N}_0 \) so that \( 3K_n < P_n \). On that range, we replace \( \theta \) by \( \theta_n \) in the last chain of inequalities according to this scaling. A standard sandwich argument will yield the desired equivalence \( (69) \) if we show that

\[
1 - \left( 1 - \left( \frac{K_n}{P_n - cK_n} \right)^2 \right)^K \sim \frac{K_n^3}{P_n^3}, \quad c = 1, 2. \quad (70)
\]

To do so we proceed as follows: Fix \( c = 1, 2 \). With

\[
A_n(c) = \left( \frac{K_n}{P_n - cK_n} \right), \quad n = 1, 2, \ldots
\]

standard calculus yields

\[
1 - \left( 1 - \left( \frac{K_n}{P_n - cK_n} \right)^2 \right)^K = 1 - \left( 1 - A_n(c)^2 \right)^K
\]

\[
= K_n A_n(c)^2 \int_0^1 (1 - A_n(c)^2 t)^{K_n - 1} dt \quad (71)
\]

on the appropriate range. The asymptotic equivalences

\[
A_n(c)^2 \sim \left( \frac{K_n}{P_n} \right)^2 \quad (72)
\]
and
\[ K_n A_n(c)^2 \sim \frac{K_n^3}{P_n^2} \tag{73} \]
follow from (69), so that (70) will hold if we show that
\[ \lim_{n \to \infty} \int_0^1 (1 - A_n(c)^2 t) K_n^{-1} dt = 1. \tag{74} \]
In view of (72) we conclude from (68) that for all \( n \) sufficiently large in \( \mathbb{N}_0 \) we have \( \sup_{0 \leq t \leq 1} |1 - A_n(c)^2 t| \leq 1. \) Therefore, the Bounded Convergence Theorem will yield (74) as soon as we establish
\[ \lim_{n \to \infty} (1 - A_n(c)^2 t) K_n^{-1} = 1, \quad 0 \leq t \leq 1. \tag{75} \]
To that end, recall the decomposition
\[ \log(1 - x) = -\int_0^x \frac{1}{1 - t} dt = -x - \Psi(x) \tag{76} \]
where
\[ \Psi(x) = \int_0^x \frac{t}{1 - t} dt, \quad 0 \leq x < 1. \]
It is easy to check that
\[ \lim_{x \to 0} \frac{\Psi(x)}{x} = 0. \tag{77} \]
Fix \( n \) sufficiently large in \( \mathbb{N}_0 \) as required above. For each \( t \) in the interval \( [0, 1] \), with the help of (75) we can write
\[
(1 - A_n(c)^2 t) K_n^{-1} = e^{-(K_n-1)\log(1-A_n(c)^2 t)}
= e^{-(K_n-1)A_n(c)^2 t - (K_n-1)\psi(A_n(c)^2 t)}.
\tag{78}
\]
Returning to (75), we use (21) and (68) to find
\[
\lim_{n \to \infty} K_n A_n(c)^2 = \lim_{n \to \infty} \left( \frac{K_n^3}{P_n^2} \cdot \frac{K_n}{P_n} \right) = 0.
\]
It is then plain that \( \lim_{n \to \infty} (K_n - 1) A_n(c)^2 = 0 \), whence
\[
\lim_{n \to \infty} (K_n - 1) \psi(A_n(c)^2 t) = \lim_{n \to \infty} (K_n - 1) A_n(c)^2 t \cdot \frac{\psi(A_n(c)^2 t)}{A_n(c)^2 t} = 0
\]
with the help of (77) in the last step. Finally, letting \( n \) go to infinity in (78), we readily get (75) as desired.

10 Proofs of the Main Results

10.1 A proof of Theorem 3.3
Consider a scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \). For each \( n = 3, 4, \ldots \), the elementary bound \( \mathbb{P} \left[ T_n(\theta_n) > 0 \right] \leq \mathbb{E} \left[ T_n(\theta_n) \right] \) implies
\[ \mathbb{P} \left[ T_n(\theta_n) > 0 \right] \leq \frac{n}{3} \beta(\theta_n) \]
by virtue of Proposition 2.1 Theorem 3.3 thus follows if under (24) we show that \( \lim_{n \to \infty} n^3 \beta(\theta_n) = 0 \). By Proposition 3.2 this convergence is equivalent to the assumed condition \( \lim_{n \to \infty} n^3 \tau(\theta_n) = 0 \), and the proof of Theorem 3.3 is now complete.

10.2 A proof of Theorem 3.4
Assume first that \( q^* \) satisfies \( 0 \leq q^* < 1 \). Fix \( n = 3, 4, \ldots \) and partition the \( n \) nodes into the \( k_n + 1 \) non-overlapping groups \((1, 2, 3), (4, 5, 6), \ldots, (3k_n + 1, 3k_n + 2, 3k_n + 3)\) with \( k_n = \left\lfloor \frac{n - 3}{5} \right\rfloor \). If \( \mathbb{P}(n; \theta_n) \) contains no triangle, then none of \( n \) of these \( k_n + 1 \) groups of nodes forms a triangle. With this in mind we get
\[
\mathbb{P} \left[ T_n(\theta_n) = 0 \right] \leq \mathbb{P} \left[ k_n \prod_{\ell=0}^{k_n-1} \mathbb{P} \left[ 3\ell+1, 3\ell+2, 3\ell+3 \text{ do not form a triangle in } \mathbb{K}(n; \theta_n) \right] \right]
= \mathbb{P} \left[ (1 - \beta(\theta_n))^{k_n+1} \right]
\leq (1 - (1 - q(\theta_n))^3)^{k_n+1}
\leq e^{-((k_n+1)(1-q(\theta_n))^3}}.
\tag{81}
\]
Note that (79) follows from the fact that the events
\[
\text{Nodes } 3\ell + 1, 3\ell + 2, 3\ell + 3 \text{ do not form a triangle in } \mathbb{K}(n; \theta_n), \quad \ell = 0, \ldots, n
\]
are mutually independent due to the non-overlap condition, while the inequality (80) is justified with the help of (19). Let \( n \) go to infinity in the inequality (81). From the constraint \( q^* < 1 \) we conclude that \( \lim_{n \to \infty} \mathbb{P} \left[ T_n(\theta_n) = 0 \right] = 0 \) since \( k_n \approx \frac{n}{5} \) so that \( \lim_{n \to \infty} (k_n + 1)(1 - q(\theta_n))^3 \to \infty \). This establishes the one law in the case \( q^* < 1 \).

To handle the case \( q^* = 1 \), we use a standard bound which forms the basis of the method of second moment [15 Remark 3.1, p. 55]. Here this bound takes the form
\[
\frac{\mathbb{E} \left[ T_n(\theta_n)^2 \right]}{(\mathbb{E} \left[ T_n(\theta_n) \right])^2} \leq \mathbb{P} \left[ T_n(\theta_n) > 0 \right], \quad n = 3, 4, \ldots
\tag{82}
\]
Theorem 3.4 then will be established in the case \( q^* = 1 \) if we show under (21) that the condition (25) implies
\[
\lim_{n \to \infty} \frac{\mathbb{E} \left[ T_n(\theta_n)^2 \right]}{(\mathbb{E} \left[ T_n(\theta_n) \right])^2} = 1.
\tag{83}
\]
As pointed earlier, the conditions (21) imply \( 3K_n < P_n \) for all \( n \) sufficiently large in \( \mathbb{N}_0 \). On that range, with \( \theta_n \) replaced by \( \theta_n \), Proposition 2.2 yields
\[
\frac{\mathbb{E} \left[ T_n(\theta_n)^2 \right]}{(\mathbb{E} \left[ T_n(\theta_n) \right])^2} = \frac{1}{\mathbb{E} \left[ T_n(\theta_n) \right]} + \left( \frac{\binom{n-3}{3}}{(\binom{n}{3})^2} + \frac{\binom{n-3}{3}}{\binom{n}{3}} \right)
+ \frac{3(n-3)}{(\binom{n}{3})^2} \cdot \frac{\mathbb{E} \left[ \chi_{123}(\theta_n) \chi_{124}(\theta_n) \right]}{(\mathbb{E} \left[ \chi_{123}(\theta_n) \right])^2}
\]
as we make use of (17) in the last term.

Let \( n \) go to infinity in the resulting expression: Under condition (25), we have \( \lim_{n \to \infty} n^3 \beta(\theta_n) = \infty \) by Proposition 3.2 whence \( \lim_{n \to \infty} \mathbb{E} \left[ T_n(\theta_n) \right] = \infty \) by virtue of (17). Since
\[
\lim_{n \to \infty} \left( \frac{\binom{n-3}{3}}{(\binom{n}{3})^2} + \frac{\binom{n-3}{3}}{\binom{n}{3}} \right) = 1
\tag{84}
\]
and
\[
\frac{3(n-3)}{(\binom{n}{3})^2} \cdot \frac{\mathbb{E} \left[ \chi_{123}(\theta_n) \chi_{124}(\theta_n) \right]}{(\mathbb{E} \left[ \chi_{123}(\theta_n) \right])^2}
\tag{85}
\]
the convergence \[ \lim_{n \to \infty} \frac{1}{n^2} \mathbb{E} \left[ \frac{\chi_{123}(\theta_n)\chi_{124}(\theta_n)}{\mathbb{E} \left[ \chi_{123}(\theta_n) \right]} \right] = 0 \] (86)
under the foregoing conditions on the scaling.

This is shown as follows: Given positive integers \( K \) and \( P \) such that \( K \leq P \), fix \( n = 3, 4, \ldots \). It is immediate that

\[
\mathbb{E} \left[ \chi_{123}(\theta)\chi_{124}(\theta) \right] \leq \mathbb{E} \left[ \chi_{123}(\theta) \right] \mathbb{E} \left[ \chi_{124}(\theta) \right]
\]

Using (87) together with (16) and

\[
\lim_{n \to \infty} n^2 \beta(\theta_n)^{2/3} = \infty.
\] (90)

As Proposition 5.2 yields \( n^2 \beta(\theta_n)^{2/3} \sim n^2 \tau(\theta_n)^{2/3} \), the desired conclusion (90) follows under the condition (91).

\[ \text{Proof.} \text{ Fix } n = 3, 4, \ldots \text{ and } \varepsilon > 0. \text{ Markov’s inequality already gives}
\]

\[
P \left[ \left| T_n(\theta) - \beta(\theta) \right| > \varepsilon \right] \leq \varepsilon^{-2} \text{Var} \left[ T_n(\theta) \right]
\]

as we recall (17). It is now plain from (20) that

\[ \text{Var} \left[ \frac{T_n(\theta)}{\beta(\theta)} \right] = \mathbb{E} \left[ \left( \frac{T_n(\theta)}{\beta(\theta)} \right)^2 \right] - \left( \mathbb{E} \left[ \frac{T_n(\theta)}{\beta(\theta)} \right] \right)^2
\]

(92)

while

\[
D_{n,i}(\theta) = 3T_n(\theta)
\]

Under the condition

\[
\sum_{i=1}^{n} D_{n,i}(\theta) (D_{n,i}(\theta) - 1) > 0,
\]

the definition of \( C^*(\mathbb{K}(n; \theta)) \) yields

\[
C^*(\mathbb{K}(n; \theta)) = \frac{3T_n(\theta)}{\sum_{i=1}^{n} \frac{T_n(\theta)}{D_{n,i}(\theta)}} = \frac{3T_n(\theta)}{\sum_{i=1}^{n} T_{n,i}(\theta)}
\]

so that

\[
C^*(\mathbb{K}(n; \theta)) = \frac{3T_n(\theta)}{\sum_{i=1}^{n} T_{n,i}(\theta)} 1 \left[ \sum_{i=1}^{n} T_{n,i}(\theta) > 0 \right].
\] (92)

The desired conclusion (90) is now immediate from Lemma 10.1 and Lemma 10.2 established below. They deal with the a.s. convergence of the numerator and denominator (properly normalized) appearing in the ratio (92), respectively.

Lemma 10.1. For positive integers \( P \) and \( K \) such that \( K \leq P \), we have

\[
\lim_{n \to \infty} \frac{T_n(\theta)}{\beta(\theta)} = \beta(\theta) \text{ a.s.}
\]

(93)

\[ \text{Proof.} \text{ Fix } n = 3, 4, \ldots \text{ and } \varepsilon > 0. \text{ Markov’s inequality already gives}
\]

\[
P \left[ \left| T_n(\theta) - \beta(\theta) \right| > \varepsilon \right] \leq \varepsilon^{-2} \text{Var} \left[ T_n(\theta) \right]
\]

as we recall (17). It is now plain from (20) that

\[ \text{Var} \left[ \frac{T_n(\theta)}{\beta(\theta)} \right] = \mathbb{E} \left[ \left( \frac{T_n(\theta)}{\beta(\theta)} \right)^2 \right] - \left( \mathbb{E} \left[ \frac{T_n(\theta)}{\beta(\theta)} \right] \right)^2
\]

(92)

and

\[
T_{n,i}(\theta) = \sum_{(j,k) \in P_{n,i}} \xi_{ij}(\theta)\xi_{jk}(\theta).
\]

The rv \( T_{n,i}(\theta) \) counts the number of distinct triangles in \( \mathbb{K}(n; \theta) \) which have node i as a vertex, while \( T_{n,i}(\theta) \) counts the number of (unordered) distinct pairs of nodes which are both connected to node i in \( \mathbb{K}(n; \theta) \). The rv \( D_{n,i}(\theta) \) is the degree of node i in \( \mathbb{K}(n; \theta) \) and is given by

\[
D_{n,i}(\theta) = \sum_{k=1}^{n} \xi_{ik}(\theta).
\]

We have

\[
\sum_{i=1}^{n} T_{n,i}(\theta) = 3T_n(\theta)
\]

as we again make use of the expression (17).

With the help of (83) and (85), it is easy to see that

\[
\lim_{n \to \infty} \text{Var} \left[ \frac{T_n(\theta)}{\beta(\theta)} \right] = 0,
\] (95)

a fact which would readily imply a weaker form of (92) with a.s. convergence replaced by convergence in probability.
However, elementary algebra on (94) shows that (95) takes place according to
\[
\lim_{n \to \infty} n^2 \text{Var} \left[ \frac{T_n(\theta)}{n} \right] = C
\]
with
\[
C = 18 \left( \mathbb{E} [\xi_{123}(\theta)\xi_{124}(\theta)] - \beta(\theta)^2 \right) > 0.
\]
As a result, for every \( \varepsilon > 0 \), we have
\[
\sum_{n=3}^{\infty} P \left( T_n(\theta) - \beta(\theta) > \varepsilon \right) \leq \frac{C'}{\varepsilon^2} \sum_{n=3}^{\infty} n^{-2} < \infty
\]
for some \( C' > C \), and the conclusion (95) follows by the Borel-Cantelli Lemma.

**Lemma 10.2.** For positive integers \( P \) and \( K \) such that \( K \leq P \), we have
\[
\lim_{n \to \infty} \sum_{i=1}^{n} T^*_n(i,\theta) = 3p(\theta)^2 \quad \text{a.s.} \quad (96)
\]

**Proof.** Fix \( n = 3, 4, \ldots \) Note that
\[
T^*_{n,1}(\theta) = \sum_{j=2}^{n} \sum_{k=j+1}^{n} \xi_{1j}(\theta)\xi_{1k}(\theta) = \Phi_n(\xi_{12}(\theta), \ldots, \xi_{1n}(\theta))
\]
where the mapping \( \Phi_n : [0,1]^{n-1} \to \mathbb{R}_+ \) is given by
\[
\Phi_n(x_2, \ldots, x_n) = \sum_{\ell=2}^{n-1} \sum_{k=\ell+1}^{n} x_\ell x_k = \sum_{\ell=2}^{n-1} x_\ell \left( \sum_{k=\ell+1}^{n} x_k \right)
\]
with \((x_2, \ldots, x_n)\) arbitrary in \([0,1]^{n-1}\). For each \( j = 2, n \), consider pairs of elements \((x_2, \ldots, x_n)\) and \((y_2, \ldots, y_n)\) in \([0,1]^{n-1}\) which differ only in the \( j^{th} \) component, i.e.,
\[
x_\ell = y_\ell, \quad \ell \neq j, \quad \ell = 2, \ldots, n.
\]
Under such conditions, it is easy to check that
\[
|\Phi_n(x_2, \ldots, x_n) - \Phi_n(y_2, \ldots, y_n)| \\
\leq |x_j - y_j| \cdot \sum_{\ell=2}^{n-1} x_\ell \\
\leq n - 1.
\]
Recall that the \((n-1)\) rvs \( \{\xi_{1j}(\theta), j = 2, \ldots, n\} \) are i.i.d. Bernoulli rvs. In view of the constraints (99) we can now apply McDiarmid’s inequality (17) (with \( c_j = (n-1) \) for all \( j = 2, \ldots, n-1 \)); see also Corollary 2.17 and Remark 2.28 in the monograph [15] p. 38. Thus, for every \( t > 0 \) we find
\[
P \left[ \left| T^*_{n,1}(\theta) - \mathbb{E} \left[ T^*_{n,1}(\theta) \right] \right| > t \right] \leq 2e^{-\frac{t^2}{n-1}}
\]
with
\[
\mathbb{E} \left[ T^*_{n,1}(\theta) \right] = \sum_{j=2}^{n-1} \sum_{k=j+1}^{n} \mathbb{E} \left[ \xi_{1j}(\theta)\xi_{1k}(\theta) \right]
\]
under the independence noted earlier.
With \( \varepsilon > 0 \) we now substitute
\[
t = \frac{(n-1)(n-2)}{2} \varepsilon
\]
into (100). Since
\[
\frac{2\varepsilon^2}{(n-1)^3} = \frac{(n-2)^2}{2(n-1)} \cdot \varepsilon^2 \sim \frac{n}{2} \cdot \varepsilon^2,
\]
we obtain from (100) and (101) that
\[
P \left[ \left| \frac{\sum_{i=1}^{n} T^*_n(i,\theta)}{n(n-1)(n-2)} - p(\theta)^2 \right| > \varepsilon \right] \leq 2e^{-\frac{\varepsilon^2}{(1+o(1))n}}.
\]
Since
\[
\sum_{i=1}^{n} T^*_n(i,\theta) - p(\theta)^2 = \left| \frac{1}{n} \sum_{i=1}^{n} \left( \frac{T^*_n(i,\theta)}{(n-1)(n-2)} - p(\theta)^2 \right) \right|
\]
\[
\leq \frac{1}{n} \sum_{i=1}^{n} \left| \frac{T^*_n(i,\theta)}{(n-1)(n-2)} - p(\theta)^2 \right|
\]
it is plain that
\[
P \left[ \left| \sum_{i=1}^{n} T^*_n(i,\theta) \right| > \varepsilon \right]
\]
\[
\leq P \left[ \left| \sum_{i=1}^{n} \left( \frac{T^*_n(i,\theta)}{(n-1)(n-2)} - p(\theta)^2 \right) \right| \right]
\]
\[
\leq \sum_{i=1}^{n} P \left[ \left| \frac{T^*_n(i,\theta)}{(n-1)(n-2)} - p(\theta)^2 \right| > \varepsilon \right]
\]
\[
= nP \left[ \left| \frac{T^*_n(1,\theta)}{(n-1)(n-2)} - p(\theta)^2 \right| > \varepsilon \right]
\]
where the last inequality follows by a union bound argument and (105) is a consequence of exchangeability.
Invoking (104) (with \( \frac{t}{2} \) instead of \( \varepsilon \)) we get
\[
P \left[ \left| \sum_{i=1}^{n} T^*_n(i,\theta) \right| > 3p(\theta)^2 \right] > \varepsilon \leq 2ne^{-\frac{\varepsilon^2}{(1+o(1))n}}
\]
with
\[
\sum_{n=3}^{\infty} n e^{-\frac{\varepsilon^2}{(1+o(1))n}} < \infty
\]
for every \( \varepsilon > 0 \). The a.s. convergence (96) now follows by the Borel-Cantelli Lemma. □
References

[1] D. J. Aldous, “Exchangeability and related topics,” École d’Été de Probabilités de Saint-Flour XIII 1983, Lecture Notes in Math. 1117, pp. 1198, Springer, Berlin, 1985, doi:10.1007/BFb0099221

[2] F. G. Ball, D. J. Sirl and P. Trapman, “Epidemics on random intersection graphs,” The Annals of Applied Probability 24 (2014), pp. 1081-1128.

[3] S.R. Blackburn and S. Gerke, “Connectivity of the uniform random intersection graph,” Discrete Mathematics 309 (2009), pp. 5130-5140.

[4] B. Bollobás, Random Graphs, Second Edition, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge (UK), 2001.

[5] F. Chung and L. Lu, “The diameter of sparse random graphs,” Advances in Applied Mathematics 26 (2001), pp. 257-279.

[6] M. Deijfen and W. Kets, “Random interaction graphs with tunable degree distribution and clustering,” Probability in the Engineering and Informational Sciences 23 (2009), pp. 661-674.

[7] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, “Redoublet sensor networks,” ACM Transactions on Information Systems Security 11 (2008), pp. 1-22.

[8] P. Erdős and A. Rényi, “On the evolution of random graphs,” Publ. Math. Inst. Hung. Acad. Sci. 5 (1960), pp. 17-61.

[9] L. Eschenauer and V.D. Gligor, “A key-management scheme for distributed sensor networks,” in Proceedings of the ACM Conference on Computer and Communications Security (2002), Washington (DC), November 2002.

[10] J. P. Gleeson, S. Melnik and A. Hackett, A, “How clustering affects the bond percolation threshold in complex networks,” in Proceedings of the 43rd Annual Conference on Information Sciences and Systems (CISS 2011), Kyoto, 2011, pp. 1-5.

[11] O. Yagan and A.M. Makowski, “Designing Securely Connected Wireless Sensor Networks in the Presence of Unreliable Links,” in Proceedings of the IEEE International Conference on Communications (ICC 2011), Kyoto, 2011, pp. 1-5.

[12] O. Yagan and A. M. Makowski, “Zero-one laws for connectivity in random key graphs,” IEEE Transactions on Information Theory IT-58 (2012), pp. 2983-2999.

[13] D. Qian, O. Yagan and Z. Zhang, “Diffusion of real-time information in social-physical networks,” in Proceedings of the IEEE Global Communications Conference (GLOBECOM 2012), Anaheim (CA), 2012, pp. 2072-2077.

[14] O. Yagan, “Zero-one laws for connectivity in inhomogeneous random key graphs,” IEEE Transactions on Information Theory, IT-62 (2016), pp. 4559-4574, August 2016.

[15] J. Zhao, O. Yagan and V. Gligor, “On the strengths of connectivity and robustness in general random intersection graphs,” in Proceedings of the 53rd IEEE Conference on Decision and Control (CDC 2014), Los Angeles (CA), December 2014, pp. 3661-3668.

[16] J. Zhao, O. Yagan and V. Gligor, “k-connectivity in random key graphs with unreliable edges,” IEEE Transactions on Information Theory, IT-61 (2015), pp. 3810-3836.

[17] Y. Zhuang and O. Yagan, “Information Propagation in Clustered Multilayer Networks,” in IEEE Transactions on Network Science and Engineering, vol. 3, no. 4, pp. 211-224, Oct.-Dec. 1 2016, doi:10.1109/TNSE.2016.2600059.

[18] Y. Zhuang, A. Arenas, and O. Yagan, “Clustering determines the dynamics of complex contagions in multiplex networks,” to appear in Physical Review E. Available online at arXiv:1608.08237 (2016).

Appendix

A Proof of Theorem 4.1

The pattern of proof is very similar to that given for Theorem 3.7 in Appendix 10.3. Throughout pick \( p \) in \( (0,1) \) and fix \( n = 3, 4, \ldots \). With distinct nodes \( i, j = 1, \ldots, n \), introduce the indicator function

\[ \xi_{ij}(p) = \left[ E_{ij}(p) \right]. \]

As in the proof of Theorem 3.7 for each \( i = 1, \ldots, n \), we define the rvs \( T_{n,i}(p) \) and \( T^*_n,i(p) \) by

\[ T_{n,i}(p) = \sum_{(j,k) \in \mathcal{P}_n,i} \xi_{ij}(p)\xi_{jk}(p) \]

and

\[ T^*_n,i(p) = \sum_{(j,k) \in \mathcal{P}_n,i} \xi_{ij}(p)\xi_{ik}(p) \]

with index set \( \mathcal{P}_n,i \) defined by (91). The rv \( T_{n,i}(p) \) counts the number of distinct triangles in \( G(n;p) \) which have node \( i \) as a vertex, while \( T^*_n,i(p) \) counts the number of (unordered) distinct pairs of nodes which are both connected to node \( i \) in \( G(n;p) \). The degree \( D_{n,i}(p) \) of node \( i \) in \( G(n;p) \) is given by

\[ D_{n,i}(p) = \sum_{k=1, k \neq i}^{n} \xi_{ik}(p). \]
Again we have the relations
\[ \sum_{i=1}^{n} T_{n,i}(p) = 3T_n(p) \]
and
\[ D_{n,i}(p)(D_{n,i}(p) - 1) = 2T_{n,i}^*(p). \]

Under the condition
\[ \sum_{i=1}^{n} D_{n,i}(p)(D_{n,i}(p) - 1) > 0, \]
the definition of \( C^*(\mathcal{G}(n;p)) \) yields
\[ C^*(\mathcal{G}(n;p)) = \frac{\sum_{i=1}^{n} D_{n,i}(p)(D_{n,i}(p) - 1)}{\sum_{i=1}^{n} T_{n,i}(p) - 1} \]
so that
\[ C^*(\mathcal{G}(n;p)) = \frac{3T_n(p)}{\sum_{i=1}^{n} T_{n,i}(p)} - 1 \left( \sum_{i=1}^{n} T_{n,i}^*(p) > 0 \right). \]  \hspace{1cm} (A.1)

The desired conclusion \( (5) \) is now immediate from Lemma \( (13) \) and Lemma \( (12) \) established below. They deal with the a.s. convergence of the numerator and denominator (properly normalized) appearing in the ratio \( (A.1) \), respectively.

**Lemma 1.1.** For every \( p \) in \( (0,1) \), we have
\[ \lim_{n \to \infty} \frac{T_n(p)}{n} = \tau^*(p) \text{ a.s.} \]  \hspace{1cm} (A.2)

**Proof.** Fix \( n = 3,4, \ldots \) and \( \varepsilon > 0 \). Markov’s inequality already gives
\[ P \left[ \left| \frac{T_n(p)}{n} - \tau^*(p) \right| > \varepsilon \right] \leq \varepsilon^{-2} \text{Var} \left[ \frac{T_n(p)}{n} \right] \]
as we recall \( (32) \).

As in the proof of Proposition \( (22) \) we readily obtain
\[ \text{Var} \left[ T_n(p) \right] = \text{Var} \left[ T_n(p) \right] + \frac{n(n-1)}{2} \text{E} \left[ \chi_{123}(p) \chi_{124}(p) \right] \]
\[ + \binom{n}{3} \binom{n-3}{1} \text{E} \left[ \chi_{123}(p) \chi_{145}(p) \right] \]
\[ + \binom{n}{3} \binom{n-3}{2} \text{E} \left[ \chi_{123}(p) \chi_{456}(p) \right]. \]

by the exchangeability and binary nature of the rvs involved. Under the assumed independence, we find
\[ \text{E} \left[ \chi_{123}(p) \chi_{145}(p) \right] = \text{E} \left[ \chi_{123}(p) \right] \text{E} \left[ \chi_{145}(p) \right] = p^6 \]
and
\[ \text{E} \left[ \chi_{123}(p) \chi_{456}(p) \right] = \text{E} \left[ \chi_{123}(p) \right] \text{E} \left[ \chi_{456}(p) \right] = p^6 \]

with \( \text{E} \left[ \chi_{123}(p) \chi_{124}(p) \right] = p^5 \).

Substituting into \( (A.2) \) gives
\[ \text{E} \left[ T_n(p)^2 \right] = \text{E} \left[ T_n(p) \right] + 3(n-3) \binom{n}{3} p^5 \]
\[ + \binom{n}{3} \left( 3 \left( \binom{n-3}{2} + \binom{n-3}{3} \right) \right) p^6. \]

It follows that
\[ \text{Var} \left[ \frac{T_n(p)}{n} \right] = \text{E} \left[ \left( \frac{T_n(p)}{n} \right)^2 \right] - \left( \text{E} \left[ \frac{T_n(p)}{n} \right] \right)^2 \]
\[ = \text{E} \left[ \frac{T_n(p)}{n} \right] + \binom{n-3}{3} + 3 \binom{n-3}{2} - 1 \cdot \left( \text{E} \left[ \frac{T_n(p)}{n} \right] \right)^2 \]
\[ + 3(n-3) \binom{n}{3} \frac{p^5}{n^2} \]  \hspace{1cm} (A.4)
as we again make use of the expression \( (54) \).

With the help of \( (54) \) and \( (55) \) it is easy to see that
\[ \lim_{n \to \infty} \text{Var} \left[ \frac{T_n(p)}{n} \right] = 0. \]  \hspace{1cm} (A.5)

This would readily imply a weaker form of \( (A.2) \) with a.s. convergence replaced by convergence in probability. However, elementary algebra on \( (A.4) \) shows that \( (A.5) \) takes place according to
\[ \lim_{n \to \infty} n^2 \text{Var} \left[ \frac{T_n(p)}{n} \right] = C \]
with \( C = 18p^5/(1-p) \). As a result, for every \( \varepsilon > 0 \), we have
\[ \sum_{n=3}^{\infty} \mathbb{P} \left[ \left| \frac{T_n(p)}{n} - \tau^*(p) \right| > \varepsilon \right] \leq \frac{C^*}{\varepsilon^2} \sum_{n=3}^{\infty} n^{-2} < \infty \]
for some \( C^* > C \), and the conclusion \( (A.2) \) follows by the Borel-Cantelli Lemma.

**Lemma 1.2.** For every \( p \) in \( (0,1) \), we have
\[ \lim_{n \to \infty} \sum_{i=1}^{n} T_{n,i}^*(p) = 3p^2 \text{ a.s.} \]  \hspace{1cm} (A.6)

**Proof.** Fix \( n = 3,4, \ldots \) and \( p \) in \( (0,1) \). Again we have
\[ T_{n,1}^*(p) = \sum_{j=2}^{n} \sum_{k=j+1}^{n} \xi_{ij}(p) \xi_{1k}(p) \]
\[ = \Phi_n(\xi_{12}(p), \ldots, \xi_{1n}(p)) \]  \hspace{1cm} (A.7)

where the mapping \( \Phi_n : [0,1]^{n-1} \rightarrow \mathbb{R}^+ \) is given by \( (28) \).

The \( (n-1) \) rvs \( \{\xi_{ij}(p), j = 2, \ldots, n\} \) are i.i.d. Bernoulli rvs. In view of the constraints \( (99) \) we can now apply McDiarmid’s inequality \( (17) \) (with \( c_j = (n-1) \) for all \( j = 2, \ldots, n-1 \); see also Corollary 2.17 and Remark 2.28 in the monograph \( [13] \) p. 38). Thus, for every \( t > 0 \) we find
\[ \mathbb{P} \left[ \left| T_{n,1}^*(p) - \text{E} \left[ T_{n,1}^*(p) \right] \right| > t \right] \leq 2e^{-\frac{t^2}{(n-1)^2}} \]  \hspace{1cm} (A.8)
with
\[
\mathbb{E} \left[ T_{n,1}^* (p) \right] = \sum_{j=2}^{n-1} \sum_{k=j+1}^{n} \mathbb{E} \left[ \xi_{1j}(p) \xi_{1k}(p) \right]
= \sum_{j=2}^{n-1} (n-j)p^2
= \frac{(n-1)(n-2)}{2} \cdot p^2
\]  
(A.9)

under the assumed independence assumptions.

With \( \varepsilon > 0 \) we now substitute \( t \) given by (102) into (A.8).

Using (103) we obtain from (A.8) and (A.9) that
\[
P \left[ \left| \frac{T_{n,1}^* (p)}{n(n-1)(n-2)/2} - p^2 \right| > \varepsilon \right] \leq 2e^{-\frac{n}{2}(1+o(1))\varepsilon^2}. 
\]  
(A.10)

The arguments leading to (105) also yield
\[
P \left[ \frac{\sum_{i=1}^{n} T_{n,i}^* (p)}{n(n-1)(n-2)/2} - p^2 \right] > \varepsilon \]
\[
\leq nP \left[ \frac{T_{n,1}^* (p)}{n(n-1)(n-2)/2} - p^2 \right] > \varepsilon.
\]

For every \( \varepsilon > 0 \), invoking (A.10) (with \( \frac{\varepsilon}{3} \) instead of \( \varepsilon \)) we get
\[
P \left[ \left| \frac{\sum_{i=1}^{n} T_{n,i}^* (p)}{(n/3)} - 3p^2 \right| > \varepsilon \right] \leq 2ne^{-\frac{n}{18}(1+o(1))\varepsilon^2}
\]

with
\[
\sum_{n=3}^{\infty} ne^{-\frac{n}{18}(1+o(1))\varepsilon^2} < \infty.
\]

The a.s. convergence (A.6) now follows by the Borel-Cantelli Lemma.