Connectivity results for random key graphs

Osman Yağan and Armand M. Makowski
Department of Electrical and Computer Engineering
and the Institute for Systems Research
University of Maryland at College Park
College Park, Maryland 20742
oyagan@umd.edu, armand@isr.umd.edu

Abstract—The random key graph is a random graph induced by the random key predistribution scheme of Eschenauer and Gligor under the assumption of full visibility. We report on recent results concerning a conjectured zero-one law for graph connectivity, and provide an outline for its proof.

Keywords: Wireless sensor networks, Key predistribution, Random key graph, Connectivity, Zero-one laws.

I. INTRODUCTION

Eschenauer and Gligor [5] have recently proposed the following random key predistribution scheme for wireless sensor networks: Before network deployment, each sensor is independently assigned $K$ distinct cryptographic keys which are selected at random from a pool of $P$ keys. These $K$ keys constitute the key ring of the node and are inserted into its memory. Two sensor nodes can then establish a secure link between them if they are within transmission range of each other and if their key rings have at least one key in common; see [5] for implementation details.

Under the assumption of full visibility, namely that nodes are all within communication range of each other, two nodes can communicate securely if their key rings share at least one key. This notion of adjacency induces the random key graph $\mathbb{K}(n; (K, P))$ on the vertex set $\{1, \ldots, n\}$ where $n$ is the number of sensor nodes; see Section II for precise definitions.

It is natural to seek conditions on $n$, $K$ and $P$ under which $\mathbb{K}(n; (K, P))$ is a connected graph with high probability – The availability of such conditions provides an encouraging indication as to the feasibility of this distribution scheme in the context of wireless sensor networks. As explained in [7] this search has lead to the following conjecture which appeared independently in [1, 6]: As we scale the parameters $K$ and $P$ with $n$ according to

$$\frac{K^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots$$

for some sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$, we conjecture that

$$\lim_{n \to \infty} \mathbb{P}[\mathbb{K}(n; (K_n, P_n)) \text{ is connected}] = \begin{cases} 0 & \text{if } \lim_{n \to \infty} \alpha_n = -\infty \\ 1 & \text{if } \lim_{n \to \infty} \alpha_n = +\infty. \end{cases}$$

(2)

This zero-one law for graph connectivity in $\mathbb{K}(n; (K, P))$ mimics a similar one for Erdős-Rényi graphs [2], and can be motivated from it by matching the link assignment probabilities in these two classes of random graphs.

In this short conference paper we report on recent progress made on the conjectured zero-one law (1)-(2). In Section II we formally introduce the class of random key graphs. Section III is devoted to a brief review of recent results, followed in Section IV by a presentation of the main contributions, summarized as Theorem 4.1. Its proof is long and technically involved, and is therefore omitted given the page limitations; it can be found in [7]. Instead, most of the discussion is devoted to an outline of the arguments: A basic roadmap of the proof is provided in Section V where we identify the terms that need to become vanishingly small as $n$ grows large. The needed bounding arguments to do so are developed in Section VI, and the final steps of the proof are then outlined in Section VII. In the concluding Section VIII we contrast our approach against that used by other authors [1], [4].

A word on notation: All statements involving limits, including asymptotic equivalences, are understood with $n$ going to infinity. The cardinality of any discrete set $S$ is denoted by $|S|$.

II. RANDOM KEY GRAPHS

The model is parametrized by the number $n$ of nodes, the size $P$ of the key pool and the size $K$ of each key ring with $K < P$. To lighten the notation we often group the integers $P$ and $K$ into the ordered pair $\theta = (P, K)$.

For each node $i = 1, \ldots, n$, let $K_i(\theta)$ denote the random set of $K$ distinct keys assigned to node $i$. We can think of $K_i(\theta)$ as an $\mathcal{P}_K$-valued rv where $\mathcal{P}_K$ denotes the collection of all subsets of $\{1, \ldots, P\}$ which contain exactly $K$ elements – Obviously, we have $|\mathcal{P}_K| = \binom{P}{K}$. The rvs $K_1(\theta), \ldots, K_n(\theta)$ are assumed to be i.i.d. rvs which are uniformly distributed over $\mathcal{P}_K$ with

$$\mathbb{P}[K_i(\theta) = S] = \binom{P}{K}^{-1}, \quad S \in \mathcal{P}_K$$

(3)

for all $i = 1, \ldots, n$. This corresponds to selecting keys randomly and without replacement from the key pool.

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

$$K_i(\theta) \cap K_j(\theta) \neq \emptyset,$$

(4)

in which case an undirected link is assigned between nodes $i$ and $j$. The resulting random graph defines the random
key graph on the vertex set \( \{1, \ldots, n\} \), hereafter denoted by \( \mathbb{K}(n; \theta) \). Random key graphs, which form a subclass in the family of random intersection graphs, are also called uniform intersection graphs by some authors [1] (and references therein).

For distinct \( i, j = 1, \ldots, n \), it is a simple matter to check that

\[
P[K_i(\theta) \cap K_j(\theta) = \emptyset] = q(\theta)
\]

with

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

The case \( P < 2K \) is clearly not interesting: It corresponds to an edge existing between every pair of nodes, so that \( \mathbb{K}(n; \theta) \) coincides with the completely regular graph \( K_{n,n} \).

With \( n = 2, 3, \ldots \) and positive integers \( K \) and \( P \) such that \( K \leq P \), let \( P(n; \theta) \) denote the probability that the random key graph \( \mathbb{K}(n; \theta) \) is connected, namely

\[
P(n; \theta) := P[\mathbb{K}(n; \theta) \text{ is connected}], \quad \theta = (K, P).
\]

III. RELATED WORK

To set the stage we survey recent results concerning the conjectured zero-one law (1)-(2).

Di Pietro et al. have shown [4, Thm. 4.6] that for large \( n \), the random key graph will be connected with very high probability if \( P_n \) and \( K_n \) are selected such that

\[
K_n \geq 5, \quad P_n \geq n \quad \text{and} \quad \frac{K_n^2}{P_n} \sim \frac{\log n}{n}
\]

for some \( c \geq 16 \).\(^1\) They also observe that for large \( n \), the random key graph will be disconnected with very high probability if the scaling satisfies

\[
\frac{K_n^2}{P_n} = o\left(\frac{\log n}{n}\right).
\]

In [1] Blackburn and Gerke recently generalized these results by Di Pietro et al.. Under the conditions

\[
K_n \geq 2 \quad \text{and} \quad n \leq P_n, \quad n = 1, 2, \ldots
\]

they showed [1, Thm. 5] that

\[
\lim_{n \to \infty} P(n; \theta_n) = 0 \quad \text{if} \quad \limsup_{n \to \infty} \frac{K_n^2 n}{P_n \log n} < 1 \quad (9)
\]

and

\[
\lim_{n \to \infty} P(n; \theta_n) = 1 \quad \text{if} \quad \liminf_{n \to \infty} \frac{K_n^2 n}{P_n \log n} > 1. \quad (10)
\]

In the process of establishing (9)-(10), they also showed [1, Thm. 3] that the conjectured zero-one law (1)-(2) holds when \( K_n = 2 \) without any constraint on the size of the key pool. From this last result it then follows that (1)-(2) holds when \( P_n = o\left(\frac{n}{\log n}\right) \) with \( 2 \leq K_n \leq P_n \).

\(^1\)In the conference version of this work [3, Thm. 4.6] the result is claimed to hold for \( c > 8 \).

IV. THE MAIN RESULT

Next we present results concerning the zero-one law (1)-(2) which we have recently obtained [7]. To fix the terminology, any pair of functions \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \) is called a scaling, and we can always associate with it a sequence \( \alpha : \mathbb{N}_0 \to \mathbb{R} \) through the relation

\[
\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots
\]

We refer to this sequence \( \alpha : \mathbb{N}_0 \to \mathbb{R} \) as the deviation function associated with the scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \). A scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \) is said be admissible if

\[
K_n \leq P_n, \quad n = 1, 2, \ldots
\]

and

\[
2 \leq K_n
\]

for all \( n = 1, 2, \ldots \) sufficiently large.

Our main result is given next; its proof can be found in [7].

**Theorem 4.1:** Consider an admissible scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \) with deviation function \( \alpha : \mathbb{N}_0 \to \mathbb{R} \) determined through (11). We have

\[
\lim_{n \to \infty} P(n; \theta_n) = 0 \quad \text{if} \quad \liminf_{n \to \infty} \alpha_n = -\infty. \quad (14)
\]

On the other hand, if there exists some \( \sigma > 0 \) such that

\[
\sigma n \leq P_n
\]

for all \( n = 1, 2, \ldots \) sufficiently large, then we have

\[
\lim_{n \to \infty} P(n; \theta_n) = 1 \quad \text{if} \quad \limsup_{n \to \infty} \alpha_n = \infty. \quad (16)
\]

The condition (15) is sometimes expressed as \( P_n = \Omega(n) \) and is weaker than the growth condition at (8) used by Blackburn and Gerke [1]. It is also easy to check that Theorem 4.1 implies the zero-one law (9)-(10). The remainder of the paper is devoted to a discussion of the proof of Theorem 4.1; only an outline of the arguments will be provided due to space limitations. Also, a careful inspection of the detailed arguments given in [7] points to the validity of the following version of the “double-exponential” result in random key graphs: Under (15) we have

\[
\lim_{n \to \infty} P(n; \theta_n) = e^{-e^{-c}} \quad \text{if} \quad \liminf_{n \to \infty} \alpha_n = c
\]

for some \( c \in \mathbb{R} \). Work on this issue will be reported elsewhere.

V. A ROADMAP FOR THE PROOF OF THEOREM 4.1

Fix \( n = 2, 3, \ldots \) and consider positive integers \( K \) and \( P \) such that \( 2 \leq K \leq P \). We define the events

\[
C_n(\theta) := [\mathbb{K}_n(\theta) \text{ is connected}]
\]

and

\[
I_n(\theta) := [\mathbb{K}_n(\theta) \text{ contains no isolated nodes}].
\]
If the random key graph \( K(n; \theta) \) is connected, then it does not contain isolated nodes, whence \( C_n(\theta) \) is a subset of \( I_n(\theta) \), and we conclude to

\[
P [C_n(\theta)] \leq P [I_n(\theta)]
\]

and

\[
P [C_n(\theta)^c] = P [C_n(\theta)^c \cap I_n(\theta)] + P [I_n(\theta)^c].
\]

In [6], we established the following zero-one law for the absence of isolated nodes by the method of first and second moments applied to the number of isolated nodes in the random key graph. This result was also obtained independently by Blackburn and Gerke [1].

**Theorem 5.1:** For any admissible scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \), it holds that

\[
\lim_{n \to \infty} P [I_n(\theta_n)] = \begin{cases} 
0 & \text{if } \lim_{n \to \infty} \alpha_n = -\infty \\
1 & \text{if } \lim_{n \to \infty} \alpha_n = +\infty
\end{cases}
\]

where the function \( \alpha : \mathbb{N}_0 \to \mathbb{R} \) is determined through (11).

Pick an admissible scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \) whose deviation function \( \alpha : \mathbb{N}_0 \to \mathbb{R} \) is determined through (11). If \( \lim_{n \to \infty} \alpha_n = -\infty \), then \( \lim_{n \to \infty} P [I_n(\theta_n)] = 0 \) by the zero-law for the absence of isolated nodes, whence \( \lim_{n \to \infty} P [C_n(\theta_n)] = 0 \) with the help of (18). If \( \lim_{n \to \infty} \alpha_n = +\infty \), then \( \lim_{n \to \infty} P [I_n(\theta_n)] = 1 \) by the one-law for the absence of isolated nodes and the desired conclusion \( \lim_{n \to \infty} P [C_n(\theta_n)] = 1 \) will follow via (19) if we can show that

\[
\lim_{n \to \infty} P [C_n(\theta_n)^c \cap I_n(\theta_n)] = 0
\]

under appropriate conditions on the scaling.

As we embark on establishing (21), we find it convenient to refer to an admissible scaling \( P, K : \mathbb{N}_0 \to \mathbb{N}_0 \) as being **strongly admissible** scaling if its deviation function \( \alpha : \mathbb{N}_0 \to \mathbb{R} \) satisfies the additional growth condition

\[
\alpha_n = o(n).
\]

Strong admissibility has implications which turn out to be technically helpful in some of the proofs: Under (22) it is always the case from (11) that

\[
\lim_{n \to \infty} \frac{K_n^2}{P_n} = 0.
\]

Since \( 1 \leq K_n \leq K_n^2 \) for all \( n = 1, 2, \ldots \), this last convergence implies

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

As a result,

\[
\lim_{n \to \infty} \frac{P_n}{K_n} = \infty
\]

so that \( 2K_n \leq P_n \) for all \( n = 1, 2, \ldots \) sufficiently large. In other words, the random key graph does not degenerate into a completely regular graph under strongly admissible scalings. Finally, it is easy to check [7] that (23) implies

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

The relevance of the notion of strong admissibility flows from the following facts.

**Lemma 5.2:** Consider an admissible scaling \( K, P : \mathbb{N}_0 \to \mathbb{N}_0 \) whose deviation sequence \( \alpha : \mathbb{N}_0 \to \mathbb{R} \) satisfies \( \lim_{n \to \infty} \alpha_n = \infty \). Assume that (15) holds for all \( n = 1, 2, \ldots \) sufficiently large. Then, there always exists a strongly admissible scaling \( K, P : \mathbb{N}_0 \to \mathbb{N}_0 \) with

\[
K_n \leq K_n \quad \text{and} \quad P_n = P_n, \quad n = 1, 2, \ldots
\]

whose deviation function \( \tilde{\alpha} : \mathbb{N}_0 \to \mathbb{R} \) satisfies both conditions \( \lim_{n \to \infty} \tilde{\alpha}_n = \infty \) and \( \tilde{\alpha}_n = o(n) \).

An easy coupling argument based on (27) implies

\[
P(n; \theta_n) \leq P(n; \theta_n), \quad n = 2, 3, \ldots
\]

Thus, we need only show (16) under (15) for strongly admissible scalings, and this leads to taking the following useful reduction step.

**Proposition 5.3:** Consider any strongly admissible scaling \( K, P : \mathbb{N}_0 \to \mathbb{N}_0 \) whose deviation function \( \alpha : \mathbb{N}_0 \to \mathbb{R} \) satisfies \( \lim_{n \to \infty} \alpha_n = \infty \). Under the condition (15), we have

\[
\lim_{n \to \infty} P [C_n(\theta_n)^c \cap I_n(\theta_n)] = 0.
\]

**VI. Bounding arguments (Outline)**

We shall establish (28) by finding a sufficiently tight upper bound on the probability appearing there, and then showing that it goes to zero as well. The additional condition (15) and strong admissibility of the scaling will play a crucial role in carrying out this argument. We outline the approach with most of the lengthy technical details available in [7].

Throughout the discussion, let \( K \) and \( P \) denote given positive integers such that \( 2 \leq K \leq P \), and fix \( n = 2, 3, \ldots \).

For any non-empty subset \( S \) of nodes, i.e., \( S \subseteq \{1, \ldots, n\} \), consider the graph \( K(n; \theta)(S) \) (with vertex set \( S \)) defined as the subgraph of \( K(n; \theta) \) restricted to the nodes in \( S \). The set \( S \) is said to be isolated in \( K(n; \theta) \) if there are no edges (in \( K(n; \theta) \)) between the nodes in \( S \) and the nodes in the complement \( S^c = \{1, \ldots, n\} \setminus S \). Let \( C_n(\theta; S) \) denote the event that the subgraph \( K(n; \theta)(S) \) is itself connected. We also introduce the event \( B_n(\theta; S) \) that \( S \) is isolated in \( K(n; \theta) \), i.e.,

\[
B_n(\theta; S) := [K_n(\theta) \cap K_j(\theta) = \emptyset, \ i \in S, \ j \in S^c].
\]

Finally, we set

\[
A_n(\theta; S) := C_n(\theta; S) \cap B_n(\theta; S).
\]

The following basic observation has been used in the context of Erdős-Rényi graphs [2], and underpins the arguments in both [1] and [3]: If \( K(n; \theta) \) is not connected and yet contains no isolated nodes, then there must exist a non-empty subset
On the event $C_n^c \cap I_n(\theta) \subseteq \cup_{S \in N_r} A_n(\theta; S)$ and a standard union bound argument immediately gives

$$
\mathbb{P}[C_n^c \cap I_n(\theta)] \leq \sum_{r=2}^{\lfloor \frac{|S|}{2} \rfloor} \left( \sum_{S \in N_r} \mathbb{P}[A_n(\theta; S)] \right)
$$

where for each $r = 1, \ldots, n$, $N_r$ denotes the collection of all subsets of $\{1, \ldots, n\}$ with exactly $r$ elements.

Now, for each $r = 1, \ldots, n$, we simplify the notation by writing $A_{n,r}(\theta) := A_n(\theta; \{1, \ldots, r\})$, $B_{n,r}(\theta) := B_n(\theta; \{1, \ldots, r\})$ and $C_{r}(\theta) := C_n(\theta; \{1, \ldots, r\})$. This notation is consistent with $C_n(\theta)$ as earlier defined in Section V. Under the enforced assumptions, it is a simple matter to check that

$$
\mathbb{P}[A_n(\theta; S)] = \mathbb{P}[A_{n,r}(\theta)], \quad S \in N_r
$$

and we obtain the bound

$$
\mathbb{P}[C_n^c \cap I_n(\theta)] \leq \sum_{r=2}^{\lfloor \frac{|S|}{2} \rfloor} \binom{n}{r} \mathbb{P}[A_{n,r}(\theta)]
$$

(30)

upon noting that $|N_r| = \binom{n}{r}$.

For each $r = 2, \ldots, n-1$, define the event $C_r^c(\theta) := C_r(\theta) \cap [U_r(\theta) \leq P - K]$ where

$$
U_r(\theta) := |\cup_{i=1}^r K_i(\theta)|.
$$

(31)

The rv $U_r(\theta)$ counts the number of distinct keys assigned to the nodes $\{1, \ldots, r\}$.

The event $C_r(\theta)$ is determined by the rv $K_1(\theta), \ldots, K_r(\theta)$, and conditioning upon them, we get

$$
\mathbb{P}[A_{n,r}(\theta)] = \mathbb{P}[C_r^c(\theta) \cap B_{n,r}(\theta)] = E \left[ \mathbb{1}[C_r^c(\theta)] \cdot \left( \frac{P - U_r(\theta)}{K_r} \right)^{n-r} \right] \leq E \left[ \mathbb{1}[C_r^c(\theta)] \cdot e^{-(n-r)\frac{\theta}{P}} U_r(\theta) \right].
$$

(32)

In this last step we made use of the easy bound

$$
\left( \frac{P - K}{K_r} \right) \leq e^{-\frac{\theta}{P} L}
$$

valid for positive integers $K, L$ and $P$ such that $K + L \leq P$; see [7] for details.

Next, for each positive integer $x$, define the event $E_r(\theta; x)$ by

$$
E_r(\theta; x) := [U_r(\theta) \leq x].
$$

On the event $C_r^c(\theta) \cap E_r(\theta; x)$, it is always the case that $U_r(\theta) \geq K$, while on the event $C_r^c(\theta) \cap E_r(\theta; x^c)$ we get $U_r(\theta) \geq x + 1$. Reporting these facts into (32) we get the following bound.

**Lemma 6.1:** For $r = 1, \ldots, n$, we have

$$
\mathbb{P}[A_{n,r}(\theta)] \leq \mathbb{P}[E_r(\theta; x)] e^{-(n-r)\frac{\theta}{P}} + \mathbb{P}[C_r^c(\theta)] e^{-(n-r)\frac{\theta}{P} (x+1)}
$$

(33)

$$
\leq \mathbb{P}[E_r(\theta; x)] e^{-(n-r)\frac{\theta}{P}} + \mathbb{P}[C_r(\theta)] e^{-(n-r)\frac{\theta}{P} (x+1)}
$$

for each positive integer $x$.

The constraints $K \leq U_r(\theta) \leq \min(rK, P)$ automatically imply $U_r(\theta) \leq P - K$ whenever $rK \leq P - K$, i.e., $(r + 1)K \leq P$. Thus, $C_r^c(\theta) = C_r(\theta)$ for all $r = 1, \ldots, n,r(\theta)$ where we have set

$$
r_n(\theta) := \min \left( r(\theta), \frac{n}{2} \right) \quad \text{with} \quad r(\theta) := \left\lfloor \frac{P}{K} \right\rfloor - 1.
$$

The next two results provide clues as to how we could bound the terms in (33). The first result shows that the probability of $C_r(\theta)$ can indeed be bounded in terms of known quantities.

**Lemma 6.2:** For each $r = 2, \ldots, n$, we have

$$
\mathbb{P}[C_r(\theta)] \leq r^{r-2} (1 - q(\theta))^{r-1}.
$$

(34)

The basic idea behind this bound is as in Erdős-Rényi graphs [2] where the analog of (34) holds with $1 - q(\theta)$ playing the role of probability of link assignment.

**Proof.** If $\mathbb{K}(n; \theta)(S)$ (with $S = \{1, \ldots, r\}$) is a connected graph, then it must contain a spanning tree on $S$. As a result, with $T_r$ denoting the collection of all trees on the vertex set $\{1, \ldots, r\}$, we find

$$
\mathbb{P}[C_r(\theta)] \leq \sum_{T \in T_r} \mathbb{P}[T \subseteq \mathbb{K}(n; \theta)(S)]
$$

(35)

by a union bound argument where the notation $T \subseteq \mathbb{K}(n; \theta)(S)$ indicates that the tree $T$ is a subgraph of $\mathbb{K}(n; \theta)(S)$.

Each tree $T$ in $T_r$ is uniquely determined by $r - 1$ edges. Edge assignments being pairwise independent in $\mathbb{K}(n; \theta)$ [6, 7], we readily conclude (say by an induction argument) that

$$
\mathbb{P}[T \subseteq \mathbb{K}(n; \theta)(S)] = (1 - q(\theta))^{r-1}, \quad T \in T_r.
$$

(36)

By Cayley’s formula there are $r^{r-2}$ trees on $r$ vertices, i.e., $|T_r| = r^{r-2}$, and (34) follows from (35) via (36).

The following rough estimates for the distribution of the rv $U_r(\theta)$ will be adequate to handle the first term in the bound (33).

**Lemma 6.3:** For all $r = 1, 2, \ldots$, we have the bound

$$
\mathbb{P}[U_r(\theta) \leq x] \leq \left( \frac{P}{x} \right)^r K
$$

whenever $x = 1, \ldots, \min(rK, P)$. 
Consider a strongly admissible scaling \( P, K : \mathbb{N}_0 \rightarrow \mathbb{N}_0 \) as in the statement of Proposition 5.3. In view of the discussion leading to (30) we need to show
\[
\lim_{n \to \infty} \sum_{r=2}^{\lfloor R \rfloor} \left( \begin{array}{c} n \\ r \end{array} \right) \mathbb{P} [A_{n,r}(\theta_n)] = 0. \tag{37}
\]

Under (22) we necessarily have \( \lim_{n \to \infty} r_n(\theta_n) = \infty \) (via (25)), and for any given integer \( R \geq 2 \) (to be specified shortly) it is the case that
\[
R < r_n(\theta_n), \quad n \geq n^*(R)
\tag{38}
\]
for some finite integer \( n^*(R) \). On that range we introduce the decomposition
\[
\sum_{r=2}^{\lfloor R \rfloor} \left( \begin{array}{c} n \\ r \end{array} \right) \mathbb{P} [A_{n,r}(\theta_n)] = \sum_{r=2}^{R} \left( \begin{array}{c} n \\ r \end{array} \right) \mathbb{P} [A_{n,r}(\theta_n)]
\tag{39}
\]
\[
+ \sum_{r=R+1}^{r_n(\theta_n)} \left( \begin{array}{c} n \\ r \end{array} \right) \mathbb{P} [A_{n,r}(\theta_n)]
\]
\[
+ \sum_{r=r_n(\theta_n)+1}^{\lfloor R \rfloor} \left( \begin{array}{c} n \\ r \end{array} \right) \mathbb{P} [A_{n,r}(\theta_n)].
\]

Let \( n \) go to infinity: The desired convergence (37) will be established if we show
\[
\lim_{n \to \infty} \sum_{r=2}^{R} \left( \begin{array}{c} n \\ r \end{array} \right) \mathbb{P} [A_{n,r}(\theta_n)] = 0, \tag{40}
\]
\[
\lim_{n \to \infty} \sum_{r=R+1}^{r_n(\theta_n)} \left( \begin{array}{c} n \\ r \end{array} \right) \mathbb{P} [A_{n,r}(\theta_n)] = 0 \tag{41}
\]
and
\[
\lim_{n \to \infty} \sum_{r=r_n(\theta_n)+1}^{\lfloor R \rfloor} \left( \begin{array}{c} n \\ r \end{array} \right) \mathbb{P} [A_{n,r}(\theta_n)] = 0. \tag{42}
\]

We prove the validity of (40), (41) and (42) by a judicious application of Lemma 6.1. In these three cases we make use of the bounds there with
\[
x = \lfloor (1+\varepsilon)KN_\varepsilon \rfloor, \quad \varepsilon \in (0, \frac{1}{2})
\]
\[
x = \lfloor \lambda r K \rfloor, \quad \lambda \in (0, 1)
\]
and
\[
x = \lfloor \mu P_n \rfloor, \quad \mu \in (0, 1),
\]
respectively. The parameters \( \lambda > 0 \) and \( \mu > 0 \) are taken sufficiently small so as to ensure that certain quantities are below various thresholds. Once \( \lambda > 0 \) has been selected, the integer \( R \) appearing at (38) is selected so that \( 0 < \lambda (R+1) \). The arguments leading to (40), (41) and (42) are carried out with the help of the bounds in Lemma 6.2 and Lemma 6.3.