CHAPTER 3

KEY MANAGEMENT

3.1 INTRODUCTION

Security in Wireless Sensor Networks is a significant issue of investigation among the research community for the past few decades. The predominant issue to be addressed in the domain of secure WSNs is key management. Key management includes key generation, distribution, rekeying and revocation. This provision is made in a cryptographic system design that is related to generation, exchange, storage, safeguarding, use, and replacement of keys. WSNs dynamic structure, easy node compromise and self organization property increase the difficulty of key management and bring down broad research issues.

The fundamental security services such as confidentiality, integrity and authentication, also depend on the concept of key management. The main goal of key management scheme is to ensure the confidentiality of information. Keys can be useful in authenticating legitimate nodes. If keys are used for authentication purposes, the adversary may try to act as a legitimate node and try to extract confidential information from other nodes. While trying to crack a secret key, adversaries try to learn messages patterns and guess the secret key. In order to prevent the adversaries from guessing the secret key, periodic refreshment of keys is needed.
The massive usage of public key algorithms such as RSA and Diffie-Hellman, is not computationally feasible for a resource constrained environment such as WSN. Also in symmetric key algorithms, establishment of key management is not a trivial task as security protocols always need additional overhead incurred on physical memory, computation and energy resources. Traditional key exchange and distribution protocols are not useful as they are based on trusting third parties. A widely accepted solution to key management for a network with limited resources is the Key Pre-distribution techniques. These schemes can broadly be classified as Probabilistic or Random Key Pre-distribution (RKP) and Deterministic Key Pre-distribution (DKP) schemes. The Random key pre-distribution schemes are taken into consideration which satisfies the important requirements of key management scheme. They are:

1) It should have highly effective sensor node authentication mechanisms;

2) It should also have effective mechanism to deal with sensor node compromise.

In this chapter, the secure connectivity and resilience of wireless sensor networks are investigated under the various Random Key Pre-distribution schemes – Escheauer and Gligor (EG), Q-composite, Pair-wise Schemes and the good understandability of the properties is carried out using Random Graph model. The model parameters of the network such as no isolated nodes and securely connected are prioritized in the analysis. Resilience means robustness under adverse conditions of node capture. Accurate calculating of resilience is also evaluated & compared for the three Random Key Pre-distribution Schemes.
Out of the various harmful activities, one can either try to jam wireless signals of sensor networks or can carry out denial-of-service attacks, targeting the physical layer of WSNs which cannot be addressed by the key management scheme.

3.2 MODELING EG SCHEME

The methodical execution of EG scheme can be carried out in three phases namely, Initialization phase, Key setup phase, Path key identification phase. Consider a collection of ‘n’ sensor nodes equipped with wireless transceiver, and assume a large set of cryptographic keys $K_P$ collectively framing a key pool.

3.2.1 Initialization Phase

Before Network deployment, each node randomly selects a set of $K$ distinct keys from the pool. These $K$ keys from the key ring ($K_R$) are inserted into the memory module of the node. The memory load of each sensor node consists of a key ring ($K_R$) with $K$ distinct keys randomly chosen from the key pool ($K_P$). Key rings are selected independently from the available $n$ number of nodes. This feature creates the inevitability of using the random graph theory for strengthening the key distribution with a critical number of keys in the key ring.

3.2.2 Key Setup Phase

After deployment, neighbourhood discovery is the primary activity of the key setup phase. When a node finds a wireless neighbour with whom it shares a key they mutually authenticate the key to verify that the other party actually owns it. At the end of this phase, wireless neighbours who have keys in common can only communicate with each other in one hop securely.
3.2.3 Path-Key Identification Phase

The key rings being randomly selected, there is a possibility that some pairs of wireless neighbours may not share a key. The two nodes with no common key, can establish a direct link by requesting an unused common key from the respective key ring.

The random graph model is used with the natural induction of EG scheme and scaling laws are developed corresponding to desirable network properties. For example, absence of isolated secure nodes and secure connectivity is made possible. This is executed with the aim of deriving guidelines to dimension the schemes, to adjust its parameters so that these properties occur with high probability as the number of nodes becomes large. The basic requirement of secure communication for WSN is achieved by providing prime prioritization to connectivity properties.

Till date many efforts have been carried out under the assumption of full visibility according to which sensor nodes are all within the communication range of each other. Under this assumption, the EG scheme gives rise to a class of random graphs known as random key graphs. To be sure, the full visibility assumption does away with the wireless nature of communication medium supporting WSNs. In practice, nodes with impaired links are very few. As a result, the achievement of desired connectivity properties is not possible, if dimensioning is done with respect to results derived under full visibility. So here simple communication model is assumed where unreliable wireless links are represented as ON/OFF channel.

3.3 RANDOM KEY GRAPHS

Random key graphs are parameterized by the n number of nodes, $K_p$ the size of the key pool, and K the size of each key ring $K_R$ with $K \leq K_p$. 
To lighten the notation, integers \( P \) and \( K \) are grouped into the ordered pair \( \varphi \equiv (K, P) \). For each node \( i = 1 \ldots n \), let \( K_i(\varphi) \) denote the random set of \( K \) distinct Keys of \( K_R \) assigned to node \( i \). The \( K_i(\varphi) \) is a \( P_K \)-valued Random Variable (RV), where \( P_K \) denotes the collection of all subsets of \( \{1, \ldots, P\} \) which contains exactly \( K \) elements. The RVs \( K_1(\varphi), \ldots, K_n(\varphi) \) are assumed to be identically independent random variables. Each and every random variable is equally distributed over \( P_K \) with \( P[K_i(\varphi) = T] = \binom{K_P}{T}^{-1} \) for all \( i = 1 \ldots n \). This corresponds to selecting the key randomly and without replacement from the key pool.

Distinct nodes \( i, j = 1 \ldots n \) are said to be \( K \)-adjacent written \( i \sim_K j \) if they share at least one key in their key rings iff \( [K_i(\varphi) \cap K_j(\varphi) \neq \emptyset] \).

For distinct \( i, j = 1 \ldots n \), it is easy to find the disconnected nodes \( P[K_i(\varphi) \cap K_j(\varphi) = \emptyset] = q(\varphi) \) with

\[
q(\varphi) = \begin{cases} 
0 & \text{if } K_P < 2K \\
\binom{K_P - K}{K} & \text{if } 2K \leq K_P 
\end{cases}
\]  

For \( 1 \leq i \leq j \leq n \), let \( B_{ij}(\beta) \) denote i.i.d \( \{0, 1\} \)-valued RVs with success probability \( \beta \). The channel between nodes \( i \) and \( j \) is available with probability \( \beta \) and unavailable with the complementary probability \( 1 - \beta \). Distinct nodes \( i \) and \( j \) are said to be \( B \)-adjacent, written \( i \sim_B j \) if \( B_{ij}(\beta) = 1 \). The notation of \( B \)-adjacency defines the standard Erdos and Renyi (ER) graph \( G(n; \beta) \) on the vertex set \( \{1 \ldots n\} \). Obviously
\[
P[\{i \sim B(j)\}_B = \beta \text{ the random graph model studied here is obtained by intersecting the random key graph } k(n; \beta) \text{ with Erods-renyi (ER) graph } G(n; \beta) \text{ more precisely, the distinct nodes } i \text{ and } j \text{ are said to be adjacent } i \sim j \text{ iff } K_i(\varphi) \cap K_j(\varphi) \neq \emptyset \text{ and } B_{i,j}(\beta) = 1.\]

The resulting undirected random graph defined on the vertex set \{1,...,n\} through this notation of adjacency is denoted as \( k \cap G(n; \varphi, \beta) \). Throughout the collections of RVs \( \{K_1(\varphi),...,K_n(\varphi)\} \) and \( \{B_{i,j}(\beta), 1 \leq i \leq j \leq n\} \) are assumed to be independent. The edge occurrence probability in \( k \cap G(n; \varphi, \beta) \) is given by

\[
P[i \sim j] = \beta, \quad P[i \sim K_j] = \beta \left(1 - q(\beta)\right) \quad (3.2)
\]

### 3.4 EG SCHEME - THEOREM

#### 3.4.1 Absence of Isolated Nodes

Consider the scaling \( K, K_P: N_0 \rightarrow N_0 \) and a scaling \( \beta : N_0 \rightarrow (0,1) \) so that \( \beta_n \left(1 - q(\varphi)\right) \sim h_n \log n, \quad n = 1, 2,... \) for some \( h > 0 \). If

\[
\lim_{n \to \infty} \beta_n \log n = \beta^* \text{ exists the equation expressed as}
\]

\[
\lim_{n \to \infty} \mathbb{P}[K \cap G(n; K, K_P, \beta) \text{ contains no isolated node}] = \begin{cases} 0, & \text{if } h < 1 \\ 1, & \text{if } h > 1 \end{cases}
\quad (3.3)
\]

The condition \( \beta_n \left(1 - q(\varphi)\right) \sim h_n \log n \) on the scaling’s will often be used in the equivalent form \( \beta_n \left(1 - q(\varphi)\right) = h_n \log n, \quad n = 1, 2,... \) with the sequence \( h: N_0 \rightarrow \mathbb{R} \), satisfying \( \lim_{n \to \infty} h_n = h \).
3.4.2 Connectivity

Absence of isolated nodes also holds the property of graph connectivity. Consider an admissible scaling \( K, P : N_0 \to (0,1) \) so that
\[
\beta_n (1 - q(\varphi)) \sim h \frac{\log n}{n}, n = 1, 2, \ldots
\]
e exists than the equation expressed as
\[
\lim_{n \to \infty} P[\mathbb{K} \cap \mathbb{G}(n ; K, K_P, \beta) \text{is connected}] = 0, \text{if } h < 1 \quad (3.4)
\]

On the other hand, if there exists some \( \rho > 0 \) such that \( \rho n \leq K_{P_0} \) for all \( n = 1, 2, \ldots \) adequately large, than the equation expressed as
\[
\lim_{n \to \infty} P[\mathbb{K} \cap \mathbb{G}(n ; K, K_P, \beta) \text{is connected}] = 1, \text{if } h > 1
\]

3.4.3 Resilience

The ratio of node-node connections is ‘wrecked’ (the key or keys securing a particular link are known to the adversary) due to compromised \( S \) nodes is the common measure of resilience called failure, which is defined to be the probability that a randomly-chosen link between a pair of uncompromised nodes is broken after the adversary has compromised \( S \) nodes.

\[
\text{failure}_s = 1 - \left( 1 - \frac{k}{K_P} \right)^S
\]

\[
\text{failure}_s = 1 - \left( 1 - \frac{k}{K_P} \right)^S
\]

For all \( n = 1, 2, \ldots \) adequately large, the equation expressed as
\[
\lim_{n \to \infty} P[\mathbb{K} \cap \mathbb{G}(n ; K, K_P, \beta) \text{is connected}] = 1, \text{if } h > 1
\]

\[ k \rightarrow \text{key storage in each node}, \quad K_P \rightarrow \text{key pool size}, \quad S \rightarrow \text{number of compromised nodes.} \]

Proof:
Initially assume that an adversary has compromised only one node (i.e) \( S = 1 \). Let the key pool be represented by \( K_P = \{K_1, K_2, \ldots, K_P\} \) and \( Y \) be a random uniform subset of \( K_P \) which represent the keys known to adversary after compromising a single node. Then \( failure_1 = \Pr[K_i \in Y] \) is the probability that the key \( K_i \) is known to the adversary.

\[
failure_1 = 1 - \Pr[K_i \notin Y] \\
= 1 - \left(1 - \frac{k}{K_P}\right)
\]

Generalise the above steps for \( S > 1 \). Let \( Y_1, Y_2, \ldots, Y_S \) be the random uniform subsets of the key pool each of size \( k \) that is independent. Then the resilience when \( S \) nodes are compromised is given by

\[
failure_1 = \Pr[K_i \in Y_1 \cup Y_2 \cup \ldots \cup Y_S] \\
= 1 - \Pr[K_i \notin Y_1 \cup Y_2 \cup \ldots \cup Y_S] \\
= 1 - \left[\Pr[K_i \notin Y_1] \Pr[K_i \notin Y_2] \ldots \Pr[K_i \notin Y_S]\right] \\
= 1 - (\Pr[K_i \notin Y_1])^S \\
= 1 - \left(1 - \frac{k}{K_P}\right)^S
\]

### 3.5 Q-COMPOSITE SCHEME

In the EG scheme, any two neighbouring nodes need to find a single common key from their key rings to establish a secure link in the key-setup phase. In q-composite scheme instead of one key q common keys (\( q > 1 \)) are needed. The resilience of the network against node capture is increased by increasing the amount of key overlap in the key ring of that pair of nodes,
which is required during the key-setup. If the requirement of key is increased, it is difficult for an attacker to break a link with a given set of key. By reducing the size of key pool, the probability between two nodes sharing sufficient key which establish a secure link will be preserved. The interplay of these two opposing factors has to result in an optimal amount of key overlap to pose the greatest obstacle to an attacker with some desired probability of eavesdropping on that link. The q-composite scheme improves a sensor network’s resilience in the face of a node capture attack.

\[
\text{failure}_s = \frac{1}{Pr} \left( \sum_{c=q}^{k} \left[ 1 - \sum_{i=1}^{c} (-1)^{i-1} \left( \frac{K_p-i}{K_p} \right)^{\binom{c}{i}} \right]^{S} p(c) \right)
\]  

(3.7)

k – key storage in each node, \( K_p \) – key pool size, \( S \) - number of compromised nodes. \( Pr \)– connectivity probability

In a q-composite scheme with key pool size \( K_p \) and key storage in each node \( k \), the connectivity probability \( Pr \)

\[
Pr = 1 - \sum_{i=0}^{q-1} p(i) \text{ where } p(i) = \frac{\binom{K_p-k-i}{k}}{\binom{k}{i}} \text{ for } i = 1, 2, .. q \text{ defines the probability that a pair of nodes share exactly ‘q’ keys.}
\]

The q-composite key scheme strengthens the network’s resilience against node capture when the number of nodes captured is low. However, a large fraction of the network communication is disclosed by q-composite key schemes when large numbers of nodes are compromised. By increasing q, it is hard for an adversary to obtain small amounts of initial information from the network via a small number of initial node captures. This comes at the cost of making the network more vulnerable once a large number of nodes have been breached. It is easy to mask an attack on a single node as communications
breakdown due to occlusion or interference; it is much harder to disguise an attack on many nodes as a natural occurrence.

3.6 **RANDOM PAIR-WISE SCHEME**

The Random Pair-wise Key Distribution Scheme has some advantages over the EG Scheme. In this scheme even if some nodes are captured by an adversary, the secrecy of the remaining nodes is perfectly preserved and this scheme also enables node-to-node authentication. In the pair-wise key distribution scheme two positive integer n, K are parameterized, such that K<n. The n nodes are labeled as i = 1… n, with unique Ids Id_1,…,Id_n. A subset of nodes δ_{n,i} [i = 1, ..., n] is also associated with node i and each of the nodes in subset δ_{n,i} is paired to node i. For any subset, the requirement is

P[δ_{n,i} = C] = \begin{cases} \binom{n-1}{K}^{-1} & \text{if } |C| = K \\ 0 & \text{otherwise} \end{cases} \quad (3.8)

The random variables δ_{n,1},...,δ_{n,n} are assumed to be mutually independent. The constructions of key rings are done after the offline random pairing. The key rings ε_{n,1}, ..., ε_{n,n}, are constructed one for each node. The collection of nK distinct cryptographic keys is available \{w_{i/l}, i = 1, ..., n; l = 1, ..., K\}. The cryptographic key w_{i/l_{n,i}(j)} is associated with j where each node j in δ_{n,i} is paired with i. The pairwise key w_{n,ij} = [(Id_i | Id_j | w_{i/l_{n,i}(j)})] is constructed and inserted in the memory modules of both nodes i and j. The key ring of node i is the set ε_{n,i} := \{w_{n,ij}, j \in δ_{n,i}\} \cup \{w_{n,ji}, i \in δ_{n,j}\}. The nodes i and j can establish a secure link if at least one of the events i \in δ_{n,j} or j \in δ_{n,i} is taking place within the communication range. The construction of this scheme supports node-to-node authentication.
3.6.1 Full Visibility Model

The Random Pair-wise Distribution Scheme naturally gives rise to the following class of random graphs under the assumption of full visibility. Consider two positive integers $n, K$ where $K < n$. The distinct nodes $i$ and $j$ are $K$-adjacent, if and only if (iff) they share a one key in common in their key rings, $i \sim_K j$ iff $\epsilon_{n,i} \cap \epsilon_{n,j} \neq \emptyset$. The undirected random graph on the vertex set $\{1, \ldots, n\}$ induced by the adjacent notation $i \sim_K j$ iff $\epsilon_{n,i} \cap \epsilon_{n,j} \neq \emptyset$ this corresponds to the modeling the random pair-wise distribution scheme under the assumption of full visibility and it is denoted as $\mathbb{H}(n; K)$. $P[i \sim_K j] = \rho_n(K)$ where $\rho_n(K)$ is the link assignment probability in $\mathbb{H}(n; K)$ is given by

$$
\rho_n(K) = 1 - \left(1 - \frac{K}{n-1}\right)^2
$$

$$
= \frac{2K}{n-1} - \left(\frac{K}{n-1}\right)^2
$$

(3.9)

The assumption of full visibility does away with the wireless nature of the communication medium supporting WSNs. There is also possibility for the communication links between nodes may not be available. In such cases the assumption was done under ON/OFF model.

3.6.2 ON/OFF Model

To find the possibility of communication links between nodes which may not be available, a communication model is assumed which consists of independent channels each of which can be either ON or OFF.

Thus with $\gamma$ in $(0,1)$, let $\{B_{ij}(\gamma), 1 \leq i \leq j \leq n\}$ denote i.i.d $\{0,1\}$ (independently identically distributed) - valued Random Variables with
success probability $\gamma$. The channel between nodes $i$ and $j$ is available with probability $\gamma$ and unavailable with the complementary probability $1 - \gamma$.

Distinct nodes $i$ and $j$ are said to be B-adjacent, written $i \sim_B j$ if $B_{ij}(\gamma) = 1$. The notation of B-adjacency defines the standard Erods and Renyi (ER) graph $G(n; \gamma)$ on the vertex set $\{1, \ldots, n\}$. Clearly $P[i \sim_B j] = \gamma$.

The random graph model studied here is obtained by intersecting the random pair-wise graph $\mathbb{H}(n; K)$ with Erods-renyi (ER) graph $\mathcal{G}(n; K, \gamma)$ more precisely, the distinct nodes $i$ and $j$ are said to be adjacent $i \sim j$ iff $\mathbb{e}_{n,i} \cap \mathbb{e}_{n,j} \neq \emptyset$ and $B_{ij}(\gamma) = 1$. The resulting undirected random graph defined on the vertex set $\{1, \ldots, n\}$ through this notation of adjacency is denoted as $\mathbb{H} \cap \mathcal{G}(n; K, \gamma)$.

Throughout the collections of RVs $\{\delta_{n,1}, \ldots, \delta_{n,n}\}$ and $\{B_{ij}(\gamma), 1 \leq i \leq j \leq n\}$ are assumed to be independent. The edge occurrence probability in $\mathbb{H} \cap \mathcal{G}(n; K, \gamma)$ is given by $P[i \sim j] = \gamma$. $P[i \sim_\kappa j] = \gamma \rho_n(K)$.

### 3.7 RANDOM PAIR-WISE SCHEME – THEOREM

The term threshold function is used to express the results. The function $\tau: [0,1] \rightarrow [0,1]$ defined by

$$\tau(\gamma) = \begin{cases} 1 & \text{if } \gamma = 0 \\ \frac{2}{1 - \log(1-\gamma)} & \text{if } 0 < \gamma < 1 \\ 0 & \text{if } \gamma = 1 \end{cases}$$

(3.10)

This threshold function is continuous on its entire domain.
3.7.1 Absence of Isolated Nodes

Consider the scaling \( K: \mathbb{N}_0 \to \mathbb{N}_0 \) and a scaling \( \gamma: \mathbb{N}_0 \to (0,1) \) such that \( \gamma_n \left( 2K_n - \frac{K_n^2}{n-1} \right) \sim h \log n \), \( n = 1, 2, \ldots \) for some \( h > 0 \). If \( \lim_{n \to \infty} \gamma_n = \gamma^* \) exists then the equation expressed as

\[
\lim_{n \to \infty} \mathbb{P}[H \cap \mathbb{G}(n; K_n, \gamma_n) \text{ contains no isolated nodes}] = \begin{cases} 
0 & \text{if } h < \tau(\gamma^*) \\
1 & \text{if } h > \tau(\gamma^*) 
\end{cases}
\]  
(3.11)

The condition \( \gamma_n \left( 2K_n - \frac{K_n^2}{n-1} \right) \sim h \log n \) on the scaling \( \mathbb{N}_0 \to (0, 1) \times \mathbb{N}_0 \) will often be used in the equivalent form \( \gamma_n \left( 2K_n - \frac{K_n^2}{n-1} \right) = h_n \log n \), \( n = 1, 2, \ldots \) with the sequence \( h: \mathbb{N}_0 \to \mathbb{R}_+ \) satisfying \( \lim_{n \to \infty} h_n = h \).

3.7.2 Connectivity

Absence of isolated nodes also holds the property of graph connectivity. Consider an admissible scaling \( K: \mathbb{N}_0 \to \mathbb{N}_0 \) and \( \gamma: \mathbb{N}_0 \to (0,1) \) such that \( \gamma_n \left( 2K_n - \frac{K_n^2}{n-1} \right) \sim h \log n \) holds for some \( h > 0 \). If \( \lim_{n \to \infty} \gamma_n = \gamma^* \) for some \( \gamma^* \in [0, 1] \), than the equation expressed as

\[
\lim_{n \to \infty} \mathbb{P}[H \cap \mathbb{G}(n; K_n, \gamma_n) \text{ is connected}] = \begin{cases} 
0 & \text{if } h < \tau(\gamma^*) \\
1 & \text{if } h > \tau(\gamma^*) 
\end{cases}
\]  
where the threshold \( \tau(\gamma^*) \) is given by

\[
\tau(\gamma) = \begin{cases} 
1 & \text{if } \gamma = 0 \\
\frac{2}{1 - \log(1 - \gamma)} & \text{if } 0 < \gamma < 1 \\
0 & \text{if } \gamma = 1
\end{cases}
\]  
(3.12)
In the particular case, the interest arises when $\gamma^* > 0$ since requiring $\gamma_n\left(2K_n - \frac{K_n^2}{n-1}\right) \sim h \log n$ now amounts to $\left(2K_n - \frac{K_n^2}{n-1}\right) \sim \frac{h}{\gamma} \log n$ for some $h > 0$. Any scaling $K: N_0 \rightarrow N_0$ which behaves like $\left(2K_n - \frac{K_n^2}{n-1}\right) \sim \frac{h}{\gamma} \log n$ must necessarily satisfy $K_n = o(n)$, and it is easy to see that requiring $\gamma_n\left(2K_n - \frac{K_n^2}{n-1}\right) \sim h \log n$ is equivalent to $K_n = d \log n$ for some $d > 0$ with $h$ and $d$ related by $d = \frac{h}{2\gamma}$. With this reparametrization, 3.7.1 & 3.7.2 can be given in a simpler form together as follows.

3.7.3 Absence of Isolated Nodes & Connectivity

Consider the scaling $K: N_0 \rightarrow N_0$ and a scaling $\gamma: N_0 \rightarrow (0, 1)$ such that $\lim_{n \rightarrow \infty} \gamma_n = \gamma^* > 0$. Under the condition $K_n = d \log n$ for some $d > 0$, \begin{align*}
\lim_{n \rightarrow \infty} \mathbb{P}\left[\mathcal{H} \cap \mathcal{G}(n; K_n, \gamma_n) \text{ contains no isolated nodes}\right] = \begin{cases}
0 & \text{if } h < \hat{\gamma}(\gamma^*) \\
1 & \text{if } h > \hat{\gamma}(\gamma^*) \end{cases}
\end{align*}

where $\hat{\gamma}(\gamma) := \frac{\tau(\gamma)}{2\gamma} = \frac{1}{\gamma - \log(1-\gamma)}$. 

0 < \gamma < 1.

3.8 RESULTS AND DISCUSSION

The simulations are carried out with MATLAB using curve fitting tool box running on a 2.4MHz PC. From these simulations, the probability of connectivity and resilience are estimated and the graph is plotted. The validity of the theoretical results is verified from the results shown in Figure 3.1.
3.8.1 EG Scheme

3.8.1.1 Connectivity

The number of sensor nodes $n$ is fixed as $n = 100$ and the key pool size at $K_P = 10,000$ in all the simulations. The channel parameters of connectivity $\beta$ is considered as $\beta = 0.2$, $\beta = 0.4$, $\beta = 0.6$, $\beta = 0.8$ with varying key value $K$ from 1 to 35. For each pair of parameters ($K, \beta$) 200 independent samples are generated and the number of times the obtained results i) have no isolated nodes and ii) are connected counted and the size empirical probability that $K \cap g(n; K, K_P, \beta)$ is connected as a function of key value $K$ is plotted in the graph. For each $\beta$ value, critical threshold of connectivity is considered and minimum integer value of $K$ is selected. For example, if $\beta = 0.2$, key value $K$ should be high for better connectivity and if $\beta = 0.8$ key value $K$ can be less for better connectivity. From this graph, $K$ value can be selected according to the requirement of application.

Figure 3.1 Probability of connectivity (vs) K – key ring
3.8.1.2 Resilience

The proportions of network connections are measured by calculating the failure$_s$. The graph shown in Figure 3.2 is plotted for the failure network connections against the number of compromised nodes.

![Graph showing failure$_s$ vs number of compromised nodes](image)

**Figure 3.2 Failure$_s$ (vs) S – number of compromised nodes**

It is evident from the graph that if the number of compromised nodes increases, failure$_s$ also increases. In EG scheme, keys are drawn from a common key pool and the capture of one sensor node can cause other links to be compromised. So the EG scheme is not perfectly resilient.

3.8.2 Q - Composite Scheme

3.8.2.1 Resilience

The graph is plotted between the number of compromised nodes in the network (s) against the failure rate (failure$_s$) as shown in Figure 3.3. In this graph, failure$_s$ is calculated for the measurement of network connectivity.
In Q-Composite scheme, two sensor nodes must share at least $q$ number of keys so as to establish a link between them. In this way, two linked nodes will have some other keys for communication if one of the keys is compromised. The resilience increases with $q$. It has a better resiliency of the order of $10^{-63}$ to $10^{-61}$ compared to the EG scheme. Thus $q$-composite key scheme strengthens the network’s resilience against node capture when the number of nodes captured is low.

### 3.8.3 Random Pair-wise Scheme

#### 3.8.3.1 Connectivity – full visibility

The critical $K$ value required to achieve secure connectivity at every step of gradual deployment under the assumption of Full Visibility model is shown in Figure 3.4. In this case, the sensor nodes are all within the communication range of each other.
In practice, fewer neighbours whose links may be impaired. As a result, the accurate K value is not known and the desired connectivity may not be achieved if dimensioning is done according to the results derived under full visibility. When compared to ON/OFF model small keys are required for connectivity.
3.8.3.2 Connectivity – ON/OFF

Figure 3.5 Key value (VS) Gamma

The critical Key value K required to achieve secure connectivity at every step of gradual deployment under the assumption of ON/OFF model with $\gamma$ varying from 0 to 1 is shown in Figure 3.5. In this case, a communication model is assumed which consists of independent channels each of which can be either ON or OFF. The probability of connectivity depends on the availability of channel between two nodes. Though the critical value of K derived under ON/OFF model is greater than that of the full visibility model and a higher secure connectivity is achieved.
Figure 3.6 Probability of connectivity (vs) K – key ring

The size Empirical probability that $h \cap g(n; K, \gamma)$ is connected as a function of Key value $K$ for ON/OFF model parameter $\gamma$ varying from $\gamma = 0.2, \gamma = 0.4, \gamma = 0.6, \gamma = 0.8 \& \gamma = 1$ with the number of nodes $n = 500$ is shown in Figure 3.6. For each $\gamma$ value, critical threshold of connectivity is considered and minimum integer value of $K$ is obtained. For example, if $\gamma = 0.2$, key value $K$ should be high for better connectivity and if $\gamma = 1$ key value $K$ can be less for better connectivity. From this graph, $K$ value can be selected according to the requirement of application.
Table 3.1 Comparison of pre-key distribution scheme

<table>
<thead>
<tr>
<th>Parameters \ Pre-Key Distribution Scheme</th>
<th>EG</th>
<th>q-Composite</th>
<th>Random Pair-wise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resilience</td>
<td>Highly depend on compromised nodes</td>
<td>Moderately depend on compromised nodes</td>
<td>100% resilience</td>
</tr>
<tr>
<td>Node authentication</td>
<td>No authentication</td>
<td>No authentication</td>
<td>Good</td>
</tr>
<tr>
<td>Key revocation</td>
<td>No key revocation</td>
<td>No key revocation</td>
<td>Good</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Connected with key size &gt; 10</td>
<td>Connectivity increases with q-Shared Keys</td>
<td>Connected with key size &gt; 5</td>
</tr>
</tbody>
</table>

The main advantage of the EG scheme is its decentralized operation for which no central authority is required for the deployment of the network. The pair-wise scheme requires central authority which maintains the sensor ID’s and key rings. Therefore in WSN, the choice of a Random Key Pre-distribution scheme depends on the application requirement.

Moreover, the Random Pair-wise Scheme has an added advantage of supporting node-to-node authentication so that sensors can identify the neighbours with which they are communicating. This major advantage in terms of network security provides node-to-node authentication which helps to detect the node misbehaviour, and provides resistance against node replication attacks. Also, since keys are unique to a particular communication link, pair-wise scheme has perfect resilience compared to the other schemes. Regarding the key size required to establish secure connectivity it has been evaluated that pair-wise scheme requires the least (K=5) compared to 10 & Q shared keys for EG & Q-Composite Schemes respectively. From Table 3.1 it
has been concluded that the Random Pair-wise Scheme provides the secure connectivity and prefect resilience than the other Random Key-Pre distribution schemes.

3.9 SUMMARY

In this work, the security connectivity and resilience of Wireless Sensor Networks are investigated under the various Random Key Pre-distribution schemes. Random graph model is used for developing the scaling laws and the guidelines are derived to dimension the schemes. If the key ring size and pool size are set according to the guidelines, the network is securely connected with high probability even when the number of nodes becomes large. Resilience is also calculated which is one of the desirable characteristics of Wireless Sensor Networks.