1
Introduction

Nature is the physical world around us and life in general. It has immense things to explore, analyze and investigate. For instance, plants perform photosynthesis, bees search for nectar, birds fly in a synchronized way, sun rises and sets in a specific way. On observing nature keenly, it can be inferred that it is perfect, divine and mannered. It is because of the intrinsic appealing characteristics of biological systems that now-a-days, many researchers are engaged in producing novel design paradigms to address the challenges in current network systems based on biological systems. Biologically inspired approaches seem promising when high level of robustness and adaptability is aimed for.

Bio-inspired systems are those systems where biology plays a vital constituent to solve problems in another domain. Some of the inherent characteristics of biological systems are listed below [Dressler and Akan, 2010]:

(1) Biological systems are flexible by nature and capable of adapting to dynamics of environmental conditions. They are able to resist the varied surroundings and atmosphere.
(2) They have a proven capacity to heal, remain strong, and be flexible to the failures caused by many natural and man-made factors.
(3) They are able to perform and accomplish very intricate tasks using a limited set of basic rules and fundamentals.
(4) When presented with novel situations, they are simple, convenient and efficient in learning, resolving and regenerating them.
(5) They have effective expert management of accountable resources and coordination among the various components of their system in such a way that they can be called global intelligent systems.
(6) Since different components coordinate with each other, these systems can be called as a stable system having an efficient equilibrium.
(7) They are self-organized by nature and renewable in context.
(8) They can survive under extreme harsh conditions and adversities because of their inherent resistance even after having moderate resources.

One of the incredibly diverse characteristics of the biological system is that they are robust. They may exhibit inferior performance compared to optimized systems but have higher resilience towards critical errors as shown in Figure 1.1 [Leibnitz, 2007].

Bio-inspired networking refers to the fields where biology has inspired computer networks. An excellent survey of bio-inspired networks has been done by Meisel and others, 2010 and Dressler and Akan, 2010. They cover topics such as firefly synchronization, activator and inhibitor systems, swarm intelligence, artificial immune systems, epidemic spreading and cellular signaling networks. These topics are covered in the following subsection.

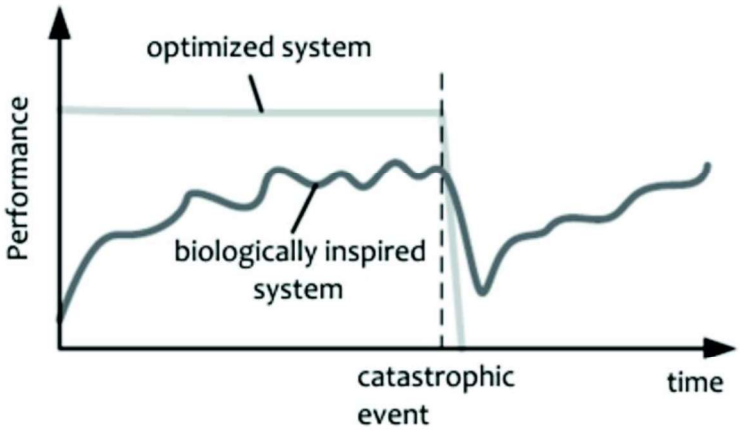

Figure 1.1: Performance level: Optimized system vs Biologically Inspired System (Source: Leibnitz, 2007)

1.1 BIOLOGICALLY INSPIRED SYSTEMS

The study of bio-inspired network systems explores the opportunities from biological systems by mimicking the laws and dynamics governing them and exhibiting a parallelism between the two fields of biology and networks. There are numerous topics in computer networks that can be studied from biological perspective as shown in Figures 1.2 and 1.3. Figure 1.2 illustrates network research inspired by biology for some of the topics, organized by the area of inspiration. Similarly, Figure 1.3 deals with an alternative view of network research inspired by biology, organized by the area of application.

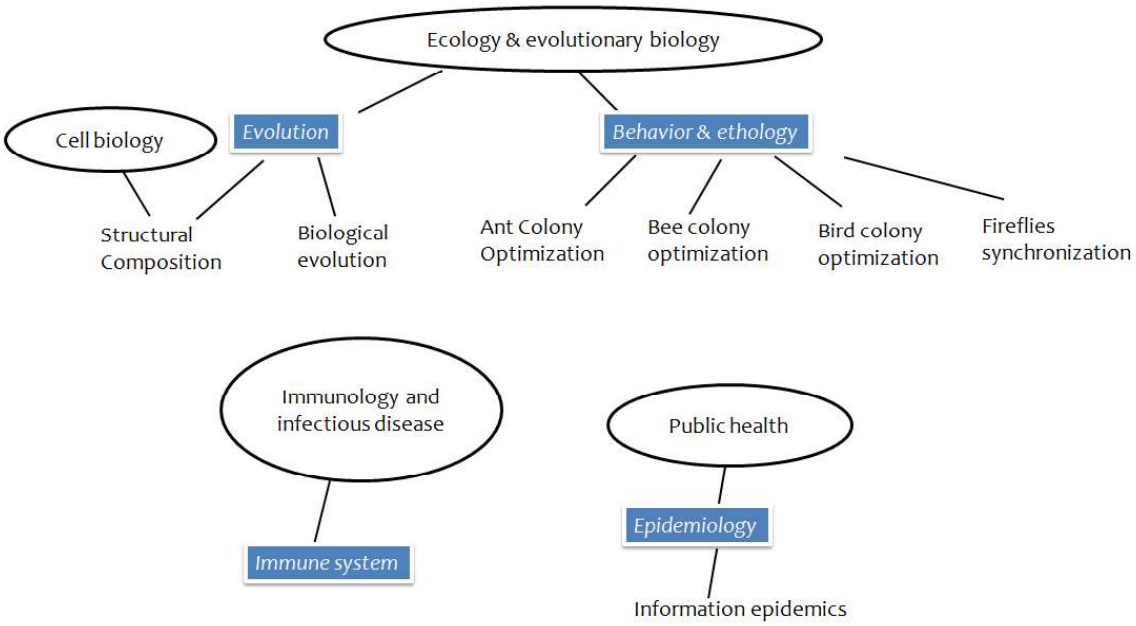

Figure 1.2: Domains of Biology Inspired the Research in Networks

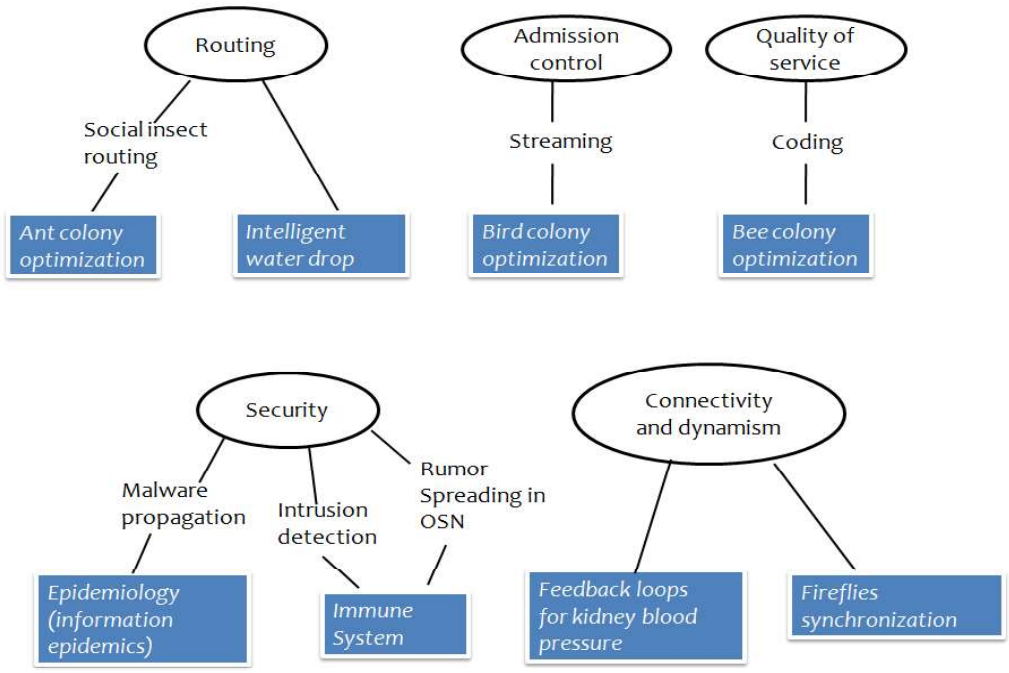

Figure 1.3: Alternative View: Domains of Research in Networks Inspired from Biology

In the early stages, the Highly Optimized Tolerance (HOT) Model was formulated which stated that a complicated and strictly organized internal structure is necessary for any system to exhibit robust external behavior [Carlson and Doyle, 1999]. For instance, the human body has many different organs and physiological systems; each serving a specific purpose. Like, kidney maintains acid base balance to regulate blood pressure, a functionality which cannot be served by the lung. On a similar note, Internet contains a number of specialized devices with specific functionality. At its core, are high speed routers, which forward the data in a highly optimized manner. At its edges, are computers, each having its own functionality and cannot take over the functionality of routers.

Structurally, network domains can be compared to organs, sub-networks to tissues and network nodes to cells. Furthermore, cells communicate with each other in a manner similar to how nodes communicate with each other [Dressler, 2005]. Also, human skin is toughened by collagen and a set of bacteria to provide protection against pathogenic bacteria. This can be compared to the function of firewall in networks [Elsadig and Abdullah, 2008]. Additionally, angiotensin based regulation process for blood pressure was studied. In a sensor network, control of activities requires exchange of information between multiple nodes. It is similar to kidneys' arterial low blood pressure in terms of sequential activity which occurs when there is a decrease in blood pressure [Dressler et al, 2005]. Internet evolution can also be mimicked from biological evolution which has similarities on the grounds of genetic heritage, variation and natural selection [Dovrolis, 2008]. Furthermore, a fiddling example of linking the two fields is the hourglass model of Internet Protocol (IP). In biology, there is an hourglass model similar to IP hourglass model. Here, the animal morphology tends to be conserved during the embryonic phylotypic period which is the period of maximal similarity between the species within each animal phylum [Leigh, 2007]. As shown in Figure 1.4, it leads to the proposition that embryogenesis diverges more extensively early and late than in the middle. The IP hourglass model, on similar note is a diverse and rapidly changing set of applications which runs on top of smaller set of transport protocols, which in turn run on a single Internet protocol [Akhshabi and Dovrolis, 2011; Csete and Doyle, 2011].

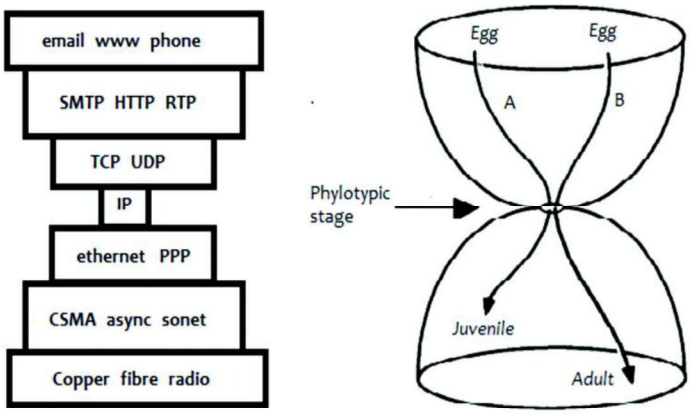

Figure 1.4: Hourglass Model of Network and Biology

There are many issues in networks such as routing, admission control and quality of service which can be looked upon from the biological perspective. Few bio-inspired systems, namely firefly synchronization, activator and inhibitor systems, swarm intelligence, artificial immune systems, epidemic spreading, and cellular signalling networks, are described below.

(1) *Swarm intelligence*: Collectively social insects can perform various complex tasks such as food gathering, motion paths etc. Swarm intelligence is a technique which takes inspiration from social insects such as ants, bees, birds which performs group activities. The application of swarm intelligence in networks can be seen in the area of ad-hoc routing, video streaming, Huffman coding etc.

1.1 Areas such as social insect routing, epidemic routing and physiological networks provide extensive insights into how routing of information is handled in nature. Ant Colony Optimization (ACO) is a meta-heuristic algorithm to find the shortest path in large graphs. Ants have an inbuilt capability to converge from their nest to the food source in the shortest possible way. This study can serve as a source of inspiration for routing messages between nodes using shortest plausible distance [Blum, 2005]. This information can also be used for tackling social network problems [Ahmad and Srivastava, 2008; Mandala et al, 2013].

1.2 When birds collectively flock together they exhibit a coordinated beautiful pattern. They follow a behavioral model in which each agent/bird follows separation, cohesion and alignment with each other. Bird colonies were used for video streaming for improving Quality of Service [Baguda et al, 2012]. The system performed better under bad channel conditions for its simplicity and fast convergence property.

1.3 Bee colonies perform the forage selection which is the act of looking or searching for food through a beautiful waggle dance. Interestingly, bee colonies were used for the generation of Huffman Codes [Tatar and Holban, 2012]. The algorithm inspired from bees performed better in terms of lookup time, which is significantly better than the traditional structural approach.

(2) *Firefly synchronization*: The phenomenon, where thousands of male fireflies of certain species congregate in trees and flash in synchrony, is observed at night in certain parts of the world. Fireflies can simply be abstracted as oscillators that emit a pulse of light periodically. These types of oscillators are referred to as pulse coupled oscillators and are used to study biological systems such as neurons and earthquakes. Applications in the field of networking include robust and fully distributed clock synchronization [Mirollo and Strogatz, 1990]. Fireflies can also be linked with the data gathering aspect of wireless sensor networks [Taniguchi et al, 2006].

(3) *Activator and inhibitor systems*: These are the ones which relate to reaction and diffusion mechanisms. An activator and inhibitor system consists of two substances that act on each

other. The activator stimulates its own production via auto-catalysis as well as the production of the inhibitor. The inhibitor, in turn, represses the production of the activator. In addition, the inhibitor diffuses more rapidly than the activator such that the patterns of activator and inhibitor concentrations arise. These systems can be used for the self-organization of autonomous systems, distributed coordination, and continuous adaptation of system parameters in highly dynamic environment [Henderson, 2004; Dressler, 2008].

(4) *Artificial immune system*: Intrusion detection and propagation of viruses, i.e., areas related to security, can be studied from immunological perspective [Elsadig and Abdullah, 2008; Boukerche et al, 2007]. Here again, there are interesting natural phenomenon, which can serve as an inspiration. Our human body has an ability to build immunity against many viruses. In addition, it also has an ability to fight back against a new virus. This can be used as inspiration to develop self-healing and self-adapting systems to address the issues in security [Wang et al, 2008; Wang and Suda, 2001].

(5) *Epidemic spreading*: The study of epidemic disease has always been an area of research where biological issues are mixed with social ones. When epidemic disease is talked about, it is about contagious diseases like influenza, measles, and sexually transmitted diseases. Epidemics can either pass explosively through a population [Goffman and Newill, 1964], or persist over a longer time period at low levels. They can experience unexpected flare-ups or even wavelike cyclic patterns of increasing and decreasing prevalence. This field can be directly linked to content distribution in computer networks (e.g. in Delay Tolerant Networks), overlay networks and analysis of worm and virus spreading in the Internet. It can also be used in studying rumor spreading when it comes to online social networks [Doerr et al, 2012, David et al, 2005].

(6) *Cellular signaling networks*: These networks comprises of highly connected modules that can be utilized to manage multiple functions in a context dependent approach. This field directly links with coordination and control in massively distributed systems and programming of network-centric operating sensor and actor networks [Tschudin, 2003; Pawson 1995].

Biologically inspired approaches for resolving computational problems have recently gained importance in computing due to the need for flexible and adaptable ways for solving networking problems. Robotics is one such field which has gained importance and is rapidly growing [Beer et al, 1997; Cruse et al, 1998]. Recently honeybees have also been used as a model for the study of visually guided flight, navigation in robots [Srinivasan, 2011]. Consensus based schemes are also being used to sense the surrounding environment [Yu et al, 2010]. The Nano-network is the technology used to create devices which are as small as the size of a human cell. This technology closely resembles biological cell communication and has recently shown some advances [Akyildiz, 2011]. A review of future prospects of bio-inspired networking is given by Nakano, 2011.

1.1.1 Mapping Biological Systems to Network Systems

In order to develop next generation bio-inspired systems, it is essential to understand nature, which requires close collaboration with biologists. Consequently, the probable biological solutions can be applied to respective field of computer networks and provide close interaction between the two components. The process is a four step model with the following sequence:

(1) *Observe* natural behavior in parallel to desired network behavior.
(2) *Explore* basic biological behavior which includes components, process and model.
(3) *Look* for specific behavior that optimally maps to networks.
(4) *Map* that behavior into a mathematical model for new implementations.

This approach can help in developing novel and intriguing results in the domain of biologically inspired systems. Networking researchers can develop better biologically inspired techniques with the help of system biologists, while improving their understanding of the

biological networks. Nevertheless, such collaborations enhance the knowledge and understanding of complex and dynamic network systems.

1.2 WIRELESS SENSOR NETWORK

A Wireless Sensor Network (WSN) is a group of small, light-weight, portable devices called sensor nodes with a communication infrastructure intended to monitor and record specific parameters such as temperature, humidity, pressure [Akyildiz, 2002]. From the biological perspective, WSN can be visualized to behave as living organisms which are born (configured) in a controlled environment. The nodes of a WSN can be said to imitate cells of a living organism that function and coordinate selflessly towards a common goal. The architectural model contains sensor nodes and gateway nodes/base station where the sensor nodes acquire real world parameters and forwards it to the gateway nodes [Al-Karaki and Kamal, 2004]. Architecture of wireless sensor network can either be a flat configuration or a clustered configuration as shown in Figure 1.5. In flat configuration setup, sensor nodes directly communicate with the gateway nodes and in clustered configuration setup, sensor nodes communicate with a cluster head/relay node which in turn communicates to the gateway node.

Sensor node can be used to monitor environment, alert system or provide information on demand. It has various applications such as:

(1) *Military applications* such as surveillance of battlefields, assessment and analysis of battle damage by weapons of mass destruction.
(2) *Environmental applications* such as detection and surveillance of forest fires, floods and precision agriculture.
(3) *Health applications* such as tracking and monitoring doctors and patients inside a hospital.
(4) *Commercial applications* such as vehicle tracking, detection for decreasing car thefts.

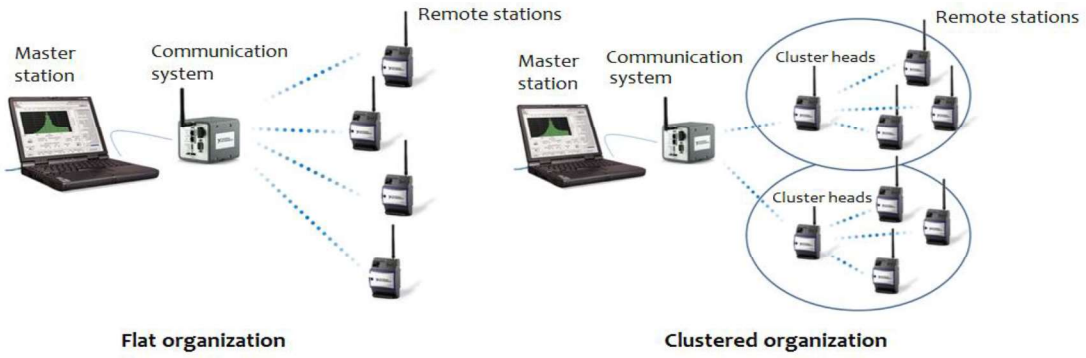

Figure 1.5: Different Architectures of Wireless Sensor Network

There are various factors which influence sensor network design like scalability, cost of production and implementation, environmental factors, hardware limitations, medium for transmitting data, power consumption while sensing, data processing, and communicating. All these factors have to be taken into account while designing a better and efficient sensor network. WSN performance mainly depends on three factors:

(1) *Quality of Service*: Measures how well a network performs a task.
(2) *Fault Tolerance*: Handles node failures without letting QoS fall below certain level.
(3) *Lifetime of entire system*: Time during which network QoS is above certain level.

1.2.1 Security in Wireless Sensor Networks

Sensor nodes precisely have two main functionalities besides processing data, i.e. to sense and communicate data [Momani and Challa, 2007]. Both at the time of sensing as well as communicating data, a node can misbehave/misbehave as shown in Figure 1.6.

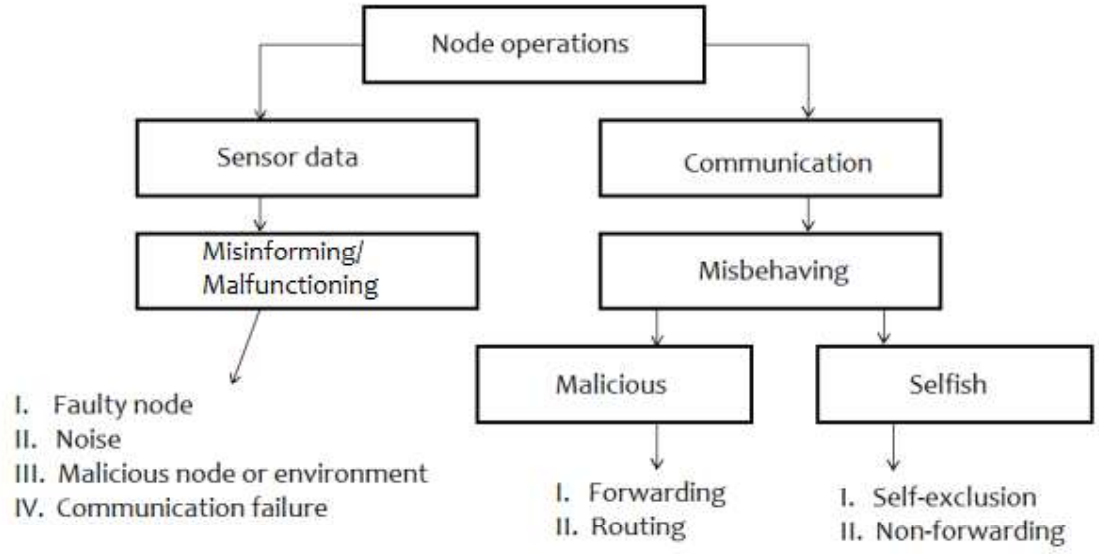

Figure 1.6: Node Misbehavior Classification (Source: Momani and Challa, 2007)

While sensing the data, sensor node can misinform by becoming a faulty node because of noise, environmental harsh conditions, or may be because of interference. While communicating the data, sensor node can become selfish for exhausting the resources of its neighbouring nodes in order to conserve its own. It can even turn into a malicious node even while forwarding or routing packets. Furthermore, it can self-exclude the data by not sending the data to the base station.

1.3 DISCUSSION AND MOTIVATION OF THESIS

In WSN, where nodes besides having inbuilt capability of sensing, processing and communicating data, also possess some risks. These risks expose them to attacks and bring in many security challenges. Therefore, it is imperative to have a secure system where there is perfect confidentiality and correctness to the data being sent from one node to another. Cooperation among the nodes is needed so that they could confidently rely on other nodes and send the data faithfully. However, owing to certain hardware and software faults, nodes can behave fraudulently and send fraudulent information. Nevertheless, since the network is open and any number of nodes can be added, it is prone to various types of attacks which breaches in the security of the system. Therefore, it is required to have correct and accurate secure model for WSN to protect the information and resources from attacks and misbehavior. Many researchers are engaged in developing innovative design paradigms to address such nodes by developing key management protocols, secure routing mechanisms and trust management systems. Key management protocol is used to encrypt and authenticate the data which can limit the attacks of WSN. However, maintaining keys is a challenge when one has large number of nodes. Key management protocols and secure routing cannot themselves provide security to WSNs for some attacks. Trust management system is an innovative solution for maintaining security

between two entities having transactions or interactions within a distributed system. Furthermore, trust models are computationally less expensive.

Although research efforts have been made with regard to various approaches in trust and reputation model, there are still some challenges that need to be addressed. Since, the sensor nodes are characterized by energy constraints, computation capability and memory. The design of the security services should be simple yet effective with regard to fraudulent node detection in WSN.

1.4 OBJECTIVE OF THESIS

(1) Design a resourceful and energy efficient trust and reputation model to detect fraudulent sensor nodes.

- Proposal 1: Machine Learning
- Proposal 2: Sociopsychological Model
- Proposal 3: Extended Sociopsychological Model.

(2) Explore the opportunities in biological systems and translate the solutions to work in distributive manner in a resource constrained wireless sensor networks.

- Proposal 4: Immune Model

1.5 ORGANISATION OF THESIS

The thesis has been structured into six chapters. The following is the outline and focus of each of the chapters in the thesis:

Chapter 1: *Introduction*
The chapter explore analogies that can be derived from biological systems. These findings give the basic framework that can be derived from biological systems and how they can be integrated into network systems.

Chapter 2: *A Review of Security Challenges, Attacks and Trust and Reputation Models in Wireless Sensor Networks*
The chapter begins by explaining the security issues and challenges in WSN. It discusses the goals, threat models and attacks followed by the security measures that can be implemented in the detection of attacks. Here, various types of trust and reputation models are reviewed. The intent of this chapter is to investigate the security related issues and challenges in wireless sensor networks and methodologies used to overcome them.

Chapter 3: *Bio-inspired Machine Learning Model for Wireless Sensor Networks*
The chapter discusses the bio-inspired machine learning based model for detection of fraudulent nodes in the network. Initially, the chapter focuses on explaining machine learning concepts. It explicates the machine learning model for detecting the fraudulent nodes in the network by describing the k-means, Support Vector Machine (SVM) methods. It discusses the results obtained along with the loop-holes of the machine learning model. Once the detection of fraudulent nodes is made, the way to remove its effect is performed by immune model. This chapter focuses in reducing the effect of fraudulent nodes using the immune-inspired model. It gives the basic insight of biological immune systems which have intelligent capabilities of detecting foreign bodies which attack human body. Later, it discusses the methodologies for attaining similar types of perspicacious nature that can be adapted in removal of fraudulent nodes in WSN. The chapter provides results that demonstrate the accuracy and robustness of the proposed model.

Chapter 4: *Sociopsychological Trust Model for Wireless Sensor Networks*
The chapter starts by elucidating the sociopsychological norms in building of trust in society. It unravels the three concepts viz ability, benevolence and integrity. Further, it demonstrates the mapping between WSN and social psychology. The novel method so proposed for security in WSN illustrates its endurance against machine learning model in various performance metrics. The chapter demonstrates the results which substantiate the reliability of the proposed mathematical model. Nevertheless, it also discusses the loop-holes of the machine learning and sociopsychological model.

Chapter 5: *Consensus Aware Sociopsychological Model for Wireless Sensor Networks*
The chapter presents the extended sociopsychological model which uses the consensus approach for building trust in WSN. It discusses the colluding node problem and the solution associated in sociopsychological account. It also discusses the simulations and experimental hardware results that were carried out on various network topologies. It gives the critical appraisal of trust models that was discussed in the thesis.

Chapter 6: *Conclusions and Future Work*
The chapter concludes the work carried out in the thesis and suggests some possible future directions.

The important technical reports, research papers, survey papers and text books that are mentioned in thesis are listed in **References**.

…