CHAPTER 2

LITERATURE SURVEY

2.1 WIRELESS SENSOR NETWORKS

This chapter provides a survey of the relevant literature in security issues of wireless sensor networks and it is divided into eight sections. The first section pertains to security issues of sensor networks with a review of existing research on security requirements and challenges for WSN. The second is on challenges of sensor networks and includes information on attacks against WSN and their countermeasures. Section three investigates about the jamming attack defense techniques in WSN. Fourth section discusses the literature review on Denial of Sleep attacks. The fifth section provides a survey on tampering attack. Sixth section deals with various defense techniques for WSN and section seven elaborates various swarm intelligence algorithm used in wireless sensor networks. Deduced from the literature review of first seven sections, the final section presents a discussion focusing particularly on the lack of research studies on security for wireless sensor networks.

Wireless sensor networks provide efficient and reliable observation of some features of physical phenomena which are otherwise very difficult to observe and also the initiation of right actions based on collective information from sensor nodes. This feature of WSN has a significant impact on several military and civil applications such as target tracking, disaster management, field surveillance, environmental and habitat monitoring, health care application, home automation and traffic control has been pointed out by Kuorilehto et al (2005).
2.2 SECURITY FOR WIRELESS SENSOR NETWORK

As the application areas of wireless sensor networks continue to grow, security becomes important. Since sensor networks perhaps interact with sensitive data or operate in hostile unattended environments like battlefield, the protection of sensor data from adversaries is an inevitable need. Similarly, for commercial applications of WSN, the protection of privacy such as personal and psychological information is equally important. Other wireless sensor network applications include ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring and many military applications.

A major benefit of these systems is that they perform in-network processing to reduce large streams of raw data into useful aggregated information. The protecting process is critical because sensor networks pose unique challenges; traditional security techniques used in traditional networks are quite different which cannot be applied directly. Therefore, there are lots of open research issues waiting to be solved in WSN security. First to make sensor networks economically viable, sensor devices are limited in their energy, computation and communication capabilities. Secondly, unlike traditional networks, sensor nodes are often deployed in nearby areas, presenting the added risk of physical attack. And thirdly, sensor networks interact closely with their physical environments and with people, posing new security problems. Consequently, existing security mechanisms are inadequate and new ideas are required. Fortunately, the new problems also instigate new research and represent an opportunity to properly address sensor network security from the start. Perrig et al (2004) gave an outline of security issues in these networks, discussed the state of the art in sensor network security and suggested future directions for research. The several important security challenges, including key establishment, secrecy, authentication, privacy, robustness to denial-of-service attacks, secure routing, and node capture have been discussed.
The fundamental security requirements for typical data networks are confidentiality, integrity and availability which are also known as CIA triad. These are accompanied by other requirements such as authentication, non repudiation, accountability etc. Sensor networks share most of these requirements but also pose unique requirements of their own. These security requirements for sensor networks are data confidentiality, data integrity, data freshness, authentication and availability as given in the literature by Kavitha & Sridharan (2010). The security constraints of wireless sensor network are divided into two broad categories namely node constraints and network constraints. These constraints are the result of limitations regarding the sensor nodes’ memory, energy, and transmission and processing power as summarized in Chaudhari & Kadam (2011).

Devesh Jinwala et al (2008) have proposed a novel design of link layer security architecture for WSNs. The principal characteristic of the design is the flexible and configurable architecture, with respect to the actual security attributes demanded by the application. Their design is based on the premise that when the link layer architecture is implemented in software, the flexibility and seamless integration of the application code become the prime advantages. They also emphasize that the storage and bandwidth resources of the sensor nodes with the increasing computations.

2.3 SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS

In conventional communication networks, the security mechanisms utilized to support the CIA triad are well known and have been in use for years. For instance, symmetric key encryption algorithms such as DES, 3DES, AES, RC4, etc. and public key encryption algorithms such as RSA, Elliptic Curve, Knapsack, etc; are in use to provide confidentiality. Message integrity codes, digital signatures, one-way hash functions etc are utilized in
order to provide authentication and integrity. However, due to the unique challenges posed by sensor networks, traditional security techniques cannot be directly applied to WSN. Challenges in WSN security design can be classified into four broad categories namely resource constraints, unattended operation, in-network processing and unreliable communication. These WSN security challenges are briefly explained by Walters et al. (2006).

- **Resource constraints:** All security approaches require a certain amount of resources to be implemented such as memory, computational power and energy. However in order to develop to be compact, sensor nodes are very limited in terms of storage capacity, processing capability and energy sources. For instance, a common sensor type has a 8-bit 4MHz processor with a total of 8K memory and disk space. With such a limitation, the size of the security software developed for a sensor should also be quite small. Besides, it is not feasible to perform computationally complex security algorithms like public key cryptography using very incapable processors of sensor nodes. In a similar way, the limited power capacity of sensors and the inability to replace and recharge batteries once depleted puts strict limitations on the use of energy. Therefore, energy impacts of proposed security schemes for WSN should also be taken into account. Because cryptographic methods cause extra power consumption due to processing functions such as encryption, decryption, verification etc; and also due to transmission of cryptographic overhead like digital signatures, energy efficient security algorithms should be designed for sensor networks.

- **Unattended operation:** Though it depends on the function of the particular sensor network, sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes:

  **Exposure to physical attacks:** Sensors may be deployed in an environment open to adversaries, harsh physical conditions, bad weather and so on.
The possibility of a sensor to suffer a physical attack in such an environment is much higher than a typical network computer, which is located in a secure place and mainly faces attacks from a network. Therefore, attackers may capture sensor nodes, extract cryptographic keys, modify programming codes or even replace them with malicious nodes under attacker’s control. As a result, the challenge is to build secure networks which can operate correctly even when many nodes have been compromised and behave in a malicious way.

**Maintenance difficulties:** Since sensor networks usually operate in areas which are far from the control point, it is almost impossible to detect physical tampering (i.e., through tamper-proof seals) and deal with physical maintenance issues (e.g., battery replacement). An example of such a case is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed. Thus, security mechanisms used for WSN should not require any maintenance.

**Lack of central management:** A sensor network is a distributed network without a central management point. Although it increases the vitality of the sensor network, it requires distributed security schemes for WSN security.

**In-network processing:** Mostly, the dominant traffic pattern in sensor networks is many-to-one, with many sensor nodes communicating sensor readings or network events back to a central base station. In-network processing such as aggregation, duplicate elimination or data compression is used to make this communication pattern in an energy efficient manner. Since in-network processing requires intermediate nodes to access, modify and possibly suppress the contents of messages, it is highly unlikely that end-to-end security mechanisms between a sensor node and a base station can be used to guarantee integrity, authenticity, and confidentiality of such messages.
Instead, link layer security mechanisms can be used. However, in this case, the intermediate nodes can have access to any messages routed through it and tamper with those messages. Therefore, WSN security schemes should protect also against malicious insiders.

- **Unreliable communication:** The poor quality of wireless channel causes high transmission error rates and more packet loss in sensor networks. If the communication protocol used lacks in appropriate error handling, the critical security packets like cryptographic keys can be lost. Even if the channel is sufficiently reliable, collisions may occur due to the broadcast nature of wireless sensor networks causing critical packet losses. In addition, multi-hop routing, network congestion and processing at nodes may lead to latency in the network and it may be difficult to achieve synchronization among nodes. This synchronization problem can be critical to sensor network security where security mechanism relies on key distribution.

Security architecture for sensor networks must integrate a number of security measures and techniques in order to protect the network and satisfy the desirable requirements, outlined. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security must pervade every aspect of the underlying system design. The most important components that are currently under research in this type of distributed networking are described below. Some of these research issues are similar to those faced in traditional networks, only with some additional constraints; others are unique to sensor networks.

- **Self-Organization.** A WSN is a typical ad hoc network, which requires every sensor node to be independent and flexible enough to use self-organizing and self-healing properties according to the application demands. There is no fixed infrastructure available for the purpose of network
management in a sensor network. In the same way that the nodes can organize their routes for supporting multi-hop communication, they must also self-organize to conduct key management and build trust relations among sensors has been proposed by Chan et al (2003) and Liu et al (2005). If self-organization is lacking, the damage resulting from an attack or from the surrounding hostile environment can be raised.

Key Establishment. When setting up a sensor network, one of the first requirements is to establish cryptographic keys for later use. Researchers have proposed a variety of protocols over several decades for this well-studied problem. Why can't the same key-establishment protocols be used in sensor networks? The inherent properties of sensor networks render previous protocols impractical. Many current sensor devices have limited computational power, making public-key cryptographic primitives too expensive in terms of system overhead. Key-establishment techniques need to scale the networks with hundreds or thousands of nodes. Moreover, having each node which shares a separate key with every other node in the network is not possible due to memory constraints.

Time Synchronization: Most sensor network applications rely on some form of time synchronization between communicating nodes as given by Ganeriwal et al (2005): (i) energy conservation by turning on and off their radio in predefined time slots, and (ii) computation of a packet's end-to-end delay. Explicit defenses against attacks assume a loose synchronization between cooperating nodes such as TESLA discussed by Perrig et al (2002). However, secure time synchronization is considered to be a very important but challenging task that has not yet been addressed effectively.

Secure Localization: Some of the most important utilities of sensor networks, e.g. tracking, rely on their ability to accurately locate each node in the network. For example, a protocol designed to locate faults will need
accurate location information in order to pinpoint the location of a fault. A number of attempts have been made towards this direction given by Lazos & Poovendran (2005) and Capkun & Hubaux (2006). Unfortunately, an attacker can easily manipulate unsecured location information by reporting false signal strengths, replaying signals, etc.

- **Secure Data Aggregation:** WSNs continue to grow in size and so does the amount of data that nodes are capable of sensing. Because of this, a query made by the base station is likely to return a great deal of traffic, much of which is not of interest to intermediate individuals that act as routers. Therefore, it is advantageous to have aggregators for collecting primitive data from a subset of nodes and then process them into more useful sets before actually transmitting them. Secure information aggregation techniques are needed because, as it is noted earlier, not all nodes can be considered trustworthy; aggregators can easily alter the received content (Dimitriou 2005). A number of attempts have been made towards this direction by Alzaid et al (2008) but much more investigation is needed.

- **Secure Routing:** Routing and data forwarding are essential services for enabling communication in sensor networks. Current routing protocols suffer from many security vulnerabilities as discussed by Karlof & Wagner (2003). For example, an attacker might launch denial-of-service attacks on the routing protocol, preventing communication. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard against injection attacks, but some routing protocols are susceptible to replay by the attacker of legitimate routing messages. Securing such protocols is very important, since even a single compromised node could completely paralyze communication in the network.
The major issues and challenges for employing any efficient security scheme in wireless sensor networks has been pointed out in Al-Sakib Khan pathan et al (2006) are created by size of sensors, consequently the processing power and type of tasks expected from the sensors. The critical security issues in WSN about cryptography, steganography and various types of attacks like Denial of service, Sybil attack, Black hole/sinkhole attack, Hello flood attack and wormhole attack against wireless sensor network are discussed in detail.

A number of the security architectures employed in wireless sensor network are proposed in David Boyle & Thomas Newe (2008). The various characteristics of each protocol presented are easily identifiable as potential network designers, allowing a more informed decision to be made while implementing a security protocol for their intended application. Authentication is the primary focus, as the most malicious attacks on a network are the work of imposters, such as DOS attacks, packet insertion etc. Authentication can be defined as a security mechanism, whereby the identity of a node in the network can be identified as a valid node of the network. Subsequently, data authenticity can be achieved; once the integrity of the message sender/receiver has been established. From a design perspective, scalability of security architectures is a desirable feature. Not all applications of WSNs will require the same security, and even in applications that do, different types of messages will require different degrees of security. This is a feature of the IEEE 802.15.4/ZigBee security architecture, and is a salient feature of ECC based architectures. What is certain is that security is going to play a pivotal role in the eventual ubiquity of wireless sensor networks, and therefore leaves a way in this research area for the near future.

2.3.1 Various Attacks and Countermeasures in Wireless Sensor Networks

Since sensor nodes are deployed usually in unprotected areas where several security threats exist, the sensor networks are vulnerable to several
kinds of attacks. These attacks can be performed in a variety of ways ranging from Denial of Service attacks to physical attacks. Some of the attacks launched in wireless sensor network are discussed.

A DoS attack is “any event that diminishes or eliminates a network’s capacity to perform its expected function”. Wood & Stankovic (2002) addressed about various DoS attacks on sensor networks range from simple jamming of sensor’s communication channel to more complicated attacks violating 802.11 MAC protocol or any other layer of the protocol stack. DoS attacks are very dangerous when sensor networks are used in highly critical and sensitive applications. For this reason, researchers have spent lots of time to identify various types of DoS attacks against WSN.

A very common Denial-of-Service attack specific to sensor networks is battery power exhaustion. Battery life is the critical parameter for the nodes in a sensor network and many techniques are used to maximize it. In one technique, for example, nodes try to spend most of the time in a sleep mode in which they only turn on the radio receiver, or even the processor, once in a while. In this environment, energy exhaustion attacks are a real threat. Without sufficient security, a malicious node could prohibit another node to go back to sleep causing the battery to be drained. Although there are several solutions to mitigate DoS for traditional networks, sensor networks cannot afford the computation overhead needed in implementing those methods. New strategies are being developed for WSN to weaken such attacks.

Du & Chen (2008) have recognized that one of the categorizations like inside and outside attacks. The inside attacks are much powerful than outside attacks. Because the insiders are considered more trustworthy, they are difficult to be detected and defended against than the outside attackers. Attackers have also been categorized by many researchers according to the
OSI layer levels. They have found it to be taking place mainly at the physical, data link, network and transport and application layers. Main types of attack that can be launched against wireless sensor networks are covered in this subsection. A survey of intrusions and their explored remedies for wireless sensor networks are discussed by Shivangi Raman et al (2010).

In a Sybil attack, a single node presents multiple identities to other nodes in the network has been dealt by David Boyle & Thomas Newe (2008); Mona Sharifnejad et al (2007). The Sybil attack can significantly decrease the effectiveness of fault-tolerant schemes such as distributed storage, multipath routing and topology maintenance. Replicas, storage partitions, or routes believed to be using disjoint nodes could actually be using a single malicious node presenting multiple identities. Sybil attacks also pose an important threat to geographic routing protocols which require nodes to exchange location information with their neighbors. It is reasonable to expect a node to accept only a single set of coordinates from each of its neighbors, but by using the Sybil attack, a malicious node can pretend to be in more than one place at simultaneously. Maximum solutions to the attacks in WSN have been found to be based upon cryptographic grounds.

In the wormhole attack (Hu et al 2006) a malicious node tunnels the packets received in one part of the network over a low latency link and replays them in a different part. Wormhole attacks usually involve two distant malicious nodes collaborating to understate distance between them by relaying packets along an out-of-band channel. An adversary located close to a base station can totally disrupt routing by creating a well-placed wormhole. The adversary can fool nodes who are normally multiple hops from a base station that they are only one or two hops away via the wormhole. This creates a sinkhole. Since the malicious node on the other side of the wormhole can artificially provide a high quality route to the base station, all
traffic in the surrounding area will be drawn through it if alternative routes are less attractive. This will most likely be the case when the endpoint of the wormhole is relatively far from a base station.

The low-cost, unattended nature and the capability of self-organizing of sensors yield the use of wireless sensor networks very popular today. Unfortunately, the unshielded nature of sensors, their deployment in remote open (hostile) areas, and the use of wireless transmission medium make them subject to several kinds of threats and attacks like eavesdropping, intrusion, Denial of Services (DoS) attacks and nodes compromising. While most of threats and attacks can be prevented using cryptographic materials (i.e. shared pair wise secret keys, certificates, etc.) provided by key management protocols, some other threats, like nodes replication attacks, can still go undetectable. Node replication attacks are harmful attacks, where an attacker compromising a node, uses its secret cryptographic key materials to successfully populate the network with several clones of it, in-order to gain the control over the network or disturb the normal operation of the network.

Chakib Bekara & Maryline (2007) proposed a new protocol for securing and preventing against node replication attacks on static WSN, where any deployed cloned node can be detected once if it attempts to establish pair-wise keys with legitimate neighbor nodes of the network, thus protecting legitimate nodes from communicating with it or relaying its packets, and protecting our network from being penetrated. The protocol does not rely on node’s locations for achieving detection of replication attacks since the nodes are assumed to be static and base station is trusted.

Malicious Node Detection in wireless sensor network through detection of message transmission in a network is provided in Waldir Riberiro Pires et al (2004). A message transmission is considered suspicious if its
signal strength is incompatible with its originators geographical position. A protocol for detecting suspicious transmissions and consequent identification of malicious nodes is proposed. The two ray model used does not model signal power loss due to obstacles, weather conditions, interference etc. Determination of malicious node’s locations needs coordination with its neighbors. Idris M. Atakli et al (2008) proposed a novel scheme based on weighted–trust evaluation to detect malicious nodes. A light weight algorithm which incurs little overhead and hierarchical network architecture is adopted. In this approach, the base station is assumed to be trusted. In fact, if the adversary gains control over the base station, the possibility of attack is more.

Khalil Issa et al (2008) has presented a countermeasure for the wormhole attack, called MOBIWORP, which alleviates the drawbacks of the previous work and efficiently mitigates the wormhole attack in mobile networks. MOBIWORP uses a secure Central Authority (CA) for global tracking of node positions. Local monitoring is used to detect and isolate malicious nodes locally. Additionally, when sufficient suspicion builds up at the CA, it enforces a global isolation of the malicious node from the whole network. MOBIWORP provides a technique that isolates the malicious nodes from the network thereby removing their ability to cause future damage. The isolation is achieved in two phases, locally and globally that neutralize the capability of the malicious nodes from launching further attacks after detection, whether at the current location or at a new location. In this protocol, guard nodes are assumed to be minimum and choosing them based on their location which eliminates the causes of loss in detection coverage has not been discussed.

A specification based intruder detection system to detect black hole and selective forwarding attack in WSN has been proposed by Mukesh Tiwari et al (2009). In this Nodes, their neighborhood and collaborate with cluster
head is to monitor malicious behavior. Watch dog nodes closely watch the behavior of nodes in the network and report their feedback to cluster head for decision making. The probability of attacking watch dog nodes in the network is more thus disturbing the communication between cluster head and watch dog nodes.

WSN has least energy resources for carrying the process such as environment sensing, information processing and communication. A fuzzy based approach for detecting Node-Exhaustion attack has been proposed by Zubair A. Baig & Salman A. Khan (2010) to achieve a tradeoff between attack detection and energy utilization. This scheme has been proposed with the limitation in number of cluster heads and inter-node distances for attack detecting process.

Mohammad Sadegh et al (2012) described briefly some of the different types of attacks on wireless sensor networks and also security analysis of some major routing protocols in wireless sensor network in term of design and security goals. A secure routing protocol should possess preventive measures against known attacks. Secure sensor network routing protocol provides better security against all known attacks. On detection of any suspicious activity of a malicious node, the recovery mechanisms should be triggered. Some secure routing protocols were explained and on implementing these protocols in particular operating system environment, it has been observed that the performance overhead is within acceptable limits compared to the level of security.

Sensor networks usually operate in hostile outdoor environments. In such settings, the minimalism of the sensors, coupled with the unattended and distributed nature of their deployment makes them highly susceptible to physical attacks. Unlike many other attacks mentioned above, physical attacks may destroy sensors permanently and the losses can be irreversible.
For example, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker. If an adversary compromises a sensor node, then the code inside the physical node may be modified. Therefore, as stated previously, the security schemes for sensor networks should be resilient to node capture. One of the major physical layer attacks are jamming attack and tampering attack. Detailed surveys on these attacks are discussed in the following subsections.

2.4 JAMMING ATTACK IN WSN

Jamming is defined as a DoS attack that interferes with the communication between nodes. The objective of the adversary causing a jamming attack is to prevent a legitimate sender or receiver from transmitting or receiving packets. Adversaries can launch jamming attacks at multiple layers of the protocol suite. Xu et al (2004) proposed a channel hopping and physically moving away from a jammer in Mica2 networks focus on determining when jamming is occurring rather than avoiding it altogether. Two strategies are presented that are employed by wireless devices to evade a MAC/PHY-layer jamming-style wireless Denial of Service attack. The first strategy, channel surfing, is a form of spectral evasion that involves legitimate wireless devices changing the channel that they are operating on. The second strategy, spatial retreats, is a form of spatial evasion whereby legitimate mobile devices move away from the locality of the DoS emitter. In these strategies, channel hopping overhead increases and spatial retreats requires node mobility which consumes more energy in sensor networks.

Wenyuan Xu et al (2005) carried out intense study of the jamming attack detection mechanism with experiments using the MICA2 Mote platform. Firstly, they collected data about various percentages of the PSR and PDR (measured at the transmitter end) for constant, deceptive, random,
and reactive jammers for BMAC and 1.1.1 MAC protocols for varying distances between the transmitting-node and the jammer. They considered additional jammer parameters like on-off periods for the random jammer and different packet sizes for the reactive jammer. The results show that although the PSR and the PDR vary for different jammers under different conditions, it is difficult to conclude about jamming and its type by these parameters alone. They then studied the levels of carrier sensing time, energy consumption, and the received signal strength as well as the received signal spectrum under normal and jamming conditions for two application layer protocols namely Constant Bit Rate (CBR) and Maximum Traffic, and tried to identify the jammer type through spectral discrimination using the Higher Order Crossing (HOC) method. They conclude through these experiments that it is not always possible to use simple statistics, such as average signal strength, energy, or carrier sensing time to discriminate jamming condition from the normal traffic, because it is difficult to devise thresholds. They also conclude that the HOC method can distinguish the constant and deceptive jamming from the normal traffic, but cannot distinguish the random and reactive jamming from the normal traffic. Finally, they conclude that if PDR is used with consistency checks like, checking own PDR and signal strength and comparing the same with those of the neighbors, and/or ascertaining own distances from the neighbors, then the combination can very effectively detect and discriminate various forms of jamming. The study is rigorous and the suggested methodology is sound. Its limitations are: (1) the complete process has to be done by the WSN node which is taxing, and (2) that the node may not be able to communicate with its neighbors during jamming to get the required statistics for comparison, as required in the method.

Link layer jamming using MAC layer semantics is a complex type of reactive jamming attacks. A link layer jammer switches between the sleeping and active modes and also adjusts its operation to the MAC layer rules of the participants in the communication. The jammer uses total energy
in an effective manner as discussed in Law et al (2005). S-MAC is analyzed for less number of attackers and the sensor nodes exchange messages that are not encrypted.

Wood et al (2007) have presented DEEJAM, a novel MAC-layer protocol for defeating efficient jamming in networks based on IEEE 802.15.4 compatible hardware. It uses four defensive mechanisms together to defeat or diminish the effectiveness of jamming by attackers in the same capability class as network nodes. Each additional defense addresses different jamming attack mechanisms to hide communication from a jammer, evade its search, and reduce its impact. Four complementary solutions are frame masking, channel hopping, packet fragmentation and redundant encoding that together significantly reduce the probability of a successful jamming attack.

Cagali et al (2007) proposed a wormhole based anti jamming technique for sensor networks. An adversary can easily mask the events that the sensor network detects by stealthily jamming an appropriate subset of the nodes; in this way, it prevents them from reporting what they are sensing to the network operator. Therefore, even if an event is sensed by one or several nodes (and the sensor network is otherwise fully connected), the network operator cannot be informed on time. The sensor nodes exploits channel diversity in order to create wormholes that lead out of the jammed region, through which an alarm is transmitted to the network operator. Three solutions have been proposed based on wired pairs of sensors, frequency hopping and uncoordinated channel hopping. These solutions to detect jamming attack involve more complex computations and overhead.

The two algorithms for detecting a jamming attack have been proposed by Cakiroglu & Ozcerit (2008). The first algorithm is based on threshold values of three detection parameters namely Bad Packet Ratio (BPR), Packet Delivery Ratio (PDR) and Energy Consumption Amount
(ECA). If all three parameters are below the thresholds, or if only the PDR exceeds the threshold, then it is concluded that there is no jamming; otherwise, there is jamming. The second algorithm is an improvement over the first one where the neighboring nodes’ conditions, ascertained through queries to be raised and replies there-to to be received within the threshold time periods, are also taken into account to enhance the jamming detection rate. The results of the simulations are very encouraging, thus establishing the effectiveness of the algorithms. However, the suggested models suffer from fixing of too many thresholds and processing at the node levels, which have their own problems, as discussed earlier. In addition, the PDR, measured at the transmitter end as in the instant case, is not suitable for the resource-constrained WSN because it imposes the avoidable burden of acknowledgements.

Sudip Misra et al (2010) proposed mechanism for jamming attack detection for wireless sensor networks based on fuzzy inference system-based jamming detection method which follows a centralized approach, wherein the jamming detection is done by the base station based on the input values of the jamming detection metrics received by it from the respective nodes. There are three inputs required to be sent by the nodes to the base station: 1) the number of total packets received by it during a specified time period, 2) the number of packets dropped by it during the period, and 3) the received signal strength (RSS). The former two metrics are normally sent to the base as part of the network health monitoring traffic at a pre-decided frequency, as part of most of the existing network management protocols. The third metric, RSS has to be additionally sent to the base station in this scheme. A different approach to the problem of detecting jamming, facilitating other jamming related works such as jammed area mapping, jammer localization and tracking and consequent decision making for different anti-jamming actions for various tactical operations are discussed based on contour mapping, flexibility in extent of jammed area mapping and holistic decision. The algorithm for
confirmation of jamming attack on a node through ‘2-means clustering’ of node neighborhood can be refined for its performance with respect to the edge nodes, especially which are in the corners. An additional step has to undertaken for discriminating edge and corner nodes from the rest and allotting various allowances to them for loss of prospective jammed or un-jammed neighbors.

Mingyan Li et al (2010) has proposed optimal jamming attack strategies and network defense policies in wireless sensor network which discuss about the controllable jamming attacks that are easy to launch but are difficult to detect. The jammer controls the probability of jamming and the transmission range in order to cause maximal damage to the network in terms of corrupted communication links. When it is detected by one or more monitoring nodes and a notification message is transferred out of the jamming region. Following this notification message, drastic actions are presumably taken by the network in order to isolate, penalize, localize and even physically capture the attacker. These actions are not addressed in this work. An optimal solution that dictate optimal jamming attack and network defense strategies are derived. Optimal jamming attack and defense policies as solution to optimization problems are analyzed for constant jamming power with one monitor node, constant jamming power with multiple monitor nodes and finally controllable jamming power with multiple jamming nodes.

The ability of sensor nodes to enter a sleep mode becomes a serious concern for sensor networks deployed in unattended and hostile environments. An adversary launches security attacks against the sensor network ranging from physical layer to application layer. Two attacks which prevent victim nodes from sleeping are barrage attack and sleep deprivation attack were presented in Matthew pirretti et al (2006). The effect of sleep deprivation attack is analyzed using three separate defense mechanisms to mitigate this attack such as the random vote scheme, the round robin scheme
and the hash based scheme. The ability to mitigate the adversary’s attack and the amount of time required to select cluster head are evaluated. The cluster head is assumed identical to any other in the cluster in terms of capacity and resources. Since the defense schemes increase the overhead of cluster head, the energy consumption increases and the chance of failure of cluster node due to power loss becomes more. It assumes a homogeneous network.

2.5 DENIAL OF SLEEP ATTACK IN WSN

The denial of sleep vulnerabilities for leading wireless sensor network MAC protocols are described in Michael Brownfield et al (2005). The link layer denial of sleep attack exposes the necessity to consider all primary threats to every system component during the design phase to properly integrate security with functionality. The WSN link layer MAC protocol introduced established Gateway MAC (G-MAC), denial of sleep defense by centralizing cluster management. In G-MAC, requests to broadcast traffic must be authenticated by the gateway node before the traffic can be sent to other nodes; therefore, only gateway node suffers power loss due to unauthenticated broadcast. The other security vulnerabilities such as jamming, node/key capture containment and network layer misrouting are not addressed.

David R. Raymond et al (2009) classify sensor network denial of sleep attacks in terms of an attacker’s knowledge of the MAC layer protocol and ability to bypass authentication and encryption protocols. Attacks from each classification are modeled to show the impacts on sensor network MAC protocols namely Sensor MAC (S-MAC), Timeout MAC (T-MAC), Berkley MAC (B-MAC) and Gateway MAC (G-MAC). G-MAC periodically elects a new gateway node to equally distribute the energy requirement among all the sensors which increases the overhead in the network and has a default change over frequency for self recovery. The gateway node will constantly remain
awake during entire collection period any legitimate network traffic in addition to the unauthenticated broadcast packets further reduces the life time.

Based on the analysis to the phenomenon and methods of denial of sleep attacking in WSN, Chen Chen et al (2009) proposed a fake scheduling switch with RSSI measurement aid which defends the collision, exhaustion, broadcast and jamming attacks.

An effective countermeasure based on ARMA prediction model and frequency hopping to react against split network attack was proposed by Chunlai Du et al (2011). A Defense scheme based on frequency hopping and fast network integration to react against split-network attack proposed uses communication frequency of the network escape from attack frequency while fast network integration makes separate subnets reintegrate into a whole network in a new communication frequency. Time series model predicts the future values from the past values. ARMA is a time series model which is used to predict the future traffic. Based on the prediction, frequency hopping is initiated. When the hopping time arrives, each cluster begins frequency adjustment to escape from the attacker. Integration of network needs time synchronization and two different solutions are given which are not feasible if the node receives the communication frequency after a long time. This scheme assumes execution of frequency hopping only once in the simulation parameter.

Ching-Tsung Hsueh et al (2011) proposed a cross layer design of secure scheme integrating the MAC protocol for denial of sleep attacks in wireless sensor networks. Two-Tier Energy Efficient Secure Scheme uses the hash chain to generate the dynamic session key used for mutual authentication and symmetric encryption key. X-MAC protocol is involved as the basic architecture of the proposed security scheme. The proposed scheme uses MD5 as hashing function and RC4 as encryption/ decryption algorithm.
The length of cluster key, secure token, random number and session key is 16 bytes. The energy consumption under various data packet rate and attack scenarios is not investigated. The evaluation of two tier energy efficient secure scheme is done for single node.

A hierarchical framework based on distributed collaborative mechanism for detecting sleep deprivation attack in wireless sensor network was proposed by Tapalina Bhattasali et al (2012). The Energy efficiency and network scalability is improved by clustering and sectoring approach. Two level detection mechanisms detect attack by reducing probability of false detection with increasing the packet transmission overhead. If a leaf node receives fake data request from the unknown nodes (intruder), it cannot detect the attack which leads to energy exhaustion completely and affects the data transmission in the network.

2.6 TAMPERING ATTACK IN WSN

One of the possible physical layer attacks is tampering attack. The term “tampering” is well accepted in the research community to designate attacks on components that involve modification of the internal structure of a single chip. The adversary can gain full control of these components, try to extract sensitive information such as secret key shared between nodes and tamper the received messages thereby altering the information to be forwarded to the destination node. At the destination node, the Cyclic Redundancy Code (CRC) would be computed, where the redundancy check fails and it would result in dropping the packet. Wang xun et al (2005) proposed search-based physical attacks that are defined as those which search for sensors and physically destroy them. The searching process is executed by means of detecting electronic, magnetic, heat signals emitted by the sensors. The model contains both flat and hierarchical sensor networks which uses a weighted random selection based approach to discriminate
multiple target choices. The attacker uses random sweeping in order to destroy sensors which have no searching phase for specific sensors like cluster-heads and data aggregators.

Wenjun et al (2005) proposed a representative search-based physical attack model in which the attacker continuously detects sensors by means of signal detection and physically destroys the detected sensors. A Sacrificial Node-assisted defense protocol has been proposed to defend sensor networks against search-based physical attacks. A sacrificial node is one which detects the attacker to save other sensors from destruction at the risk of being detected and physically destroyed by the attacker. The existence of sacrificial nodes compensates the weakness of the sensors ability to detect the attacker by extending the area in which sensors are aware of the proximity of the attacker. The core principle of our sacrificial node-assisted defense protocol is to trade short term local coverage for long term global coverage through the sacrificial node-assisted attack notification and state switching of sensors.

A 2-hop ACK technique has been proposed by Liu et al (2007) to monitor the nodes’ frequency of dropping packets instead of using the medium overhearing technique. Node A accuses the neighboring node B of dropping a packet if node A does not receive ACK from the 2-hop away node C, but the mechanism completely fails when two neighboring nodes collide to issue fake ACKs.

Trust and reputation have been recently suggested as an effective security mechanism for open environments such as the internet and considerable research has been done on modeling and managing trust and reputation. Using the trust and reputation management scheme to secure, wireless sensor networks requires paying close attention to the incurred bandwidth, delay and overhead, which so far have been overlooked by most
research work. Boukerch et al (2007) proposed an Agent-based Trust and Reputation Management (ATRM) scheme for wireless sensor networks, where trust and reputation management is carried out locally with minimal overhead in terms of extra messages and time delay. It is based on a clustered WSN with backbone and its core is a mobile agent system. It requires a node's trust and reputation information to be stored respectively in the forms of t-instrument and r-certificate by the node itself. In addition, ATRM requires every node to locally hold a mobile agent that is in charge of administrating the trust and reputation of its hosting node. Based on the collected t-instruments, a mobile agent periodically issues its hosting node updated r-certificates. But since mobile agents are designed to travel over the entire network and run on remote nodes, they must be launched by trusted entities. Therefore, in ATRM, it is assumed that (1) there is a trusted authority that is responsible for generating and launching mobile agents, and (2) mobile agents are resilient against the unauthorized analysis and modification of their computation logic.

A new Randomized, Efficient and Distributed (RED) protocol for detection of node replication attack has been proposed by Mauro Conti et al (2007). When an adversary captures some of nodes, the attacker reprograms it and replicates the node which easily takes control over the network. An adversary eavesdrops on all communication and could capture nodes thereby acquiring all the information stored within the nodes. Since sensor nodes are commonly assumed not to be tamper proof, the information inside the nodes is easily accessible. An adversary replicates the captured sensors and launches variety of inside attacks. A RED protocol detects the node replication attack efficiently with the requirement that the overhead generated by the protocol should be small.
Different trust and/or reputation models have arisen in the last few years. All of them have certain key processes in common such as scoring, ranking, rewarding, punishing or gathering behavioral information. Many scenarios would benefit from the existence of some trust and/or reputation model standardization recommendations such as, P2P networks, multi-agent systems, ad-hoc networks, Wireless Sensor Networks, file-sharing systems, etc, since these scenarios already have standards in many other issues, but not in managing trust and/or reputation between different entities. Gómez Mármol Félix & Gregorio Martinez Perez (2010) presented a pre-standardization approach for trust and/or reputation models in distributed systems. A wide review of them has been carried out, extracting common properties and providing some pre-standardization recommendations. Wireless sensor networks have recently gained a high attention because of their multiple and innovative applications as well as their singular characteristics. They are susceptible to a large number of security threats where some of which might be effectively mitigated with an accurate trust and reputation management. The main goals of reputation and trust-based systems in wireless communication network consist of providing information that allows nodes to distinguish between trustworthy and non-trustworthy nodes, encouraging nodes to be trustworthy and discouraging participation of nodes that are untrustworthy. Additionally, two more goals of a reputation and trust-based system from a wireless communication network perspective can be identified. The first goal is to cope with any kind of observable misbehavior. And the second goal is to minimize the damage caused by insider attacks.

A reputation based scheme proposed detects false data injection in wireless sensor network has been pointed by CHEN Dongling & Wencheng yang (2011). False data injection can be launched by both inside and outside attackers. The defense of false data injection from outside attacker can be
achieved by using message authentication codes schemes. The inside attacker will threaten the network security since the security mechanisms and keys of compromised nodes are more difficult to detect. A reputation evaluation mechanism based on statistic and information theory to defend the false data injection launched by inside attacker distinguish less-trustworthy nodes and choose the high trustworthy nodes to send data to the aggregator, minimizing the influence of false data injection attack launched by the compromised nodes. There is a lack of defend mechanism for attack launched by both inside and outside attacker using reputation based scheme.

Mahmoud & Shen (2011) proposed ESIP, a communication protocol that can be used for a cooperation stimulation mechanism. The protocol uses the public key cryptography and the identity based cryptography to reduce the number of signing and verifying operations. The source and destination nodes generate hash chains and sign their roots. For each message, the source node appends the pre-image of the last sent hash value from its chain and a keyed hash value for each intermediate node to ensure the message integrity at each hop. The destination node replies with ACK packet containing the pre-image of the last sent hash value from its chain. By this way only two signatures can be generated for the whole session, i.e., one signature from the source node and one signature from the destination node.

TRIPO, a novel mechanism that can Thwart the Rational and Irrational Packet dropping attacks by adopting stimulation and punishment strategies has been proposed by Mohamed Elsalih Mahmoud & Xuemin Shen (2011). TRIPO uses credits to stimulate the rational packet droppers to relay packets, and uses reputation system to identify and evict the irrational packet droppers. With TRIPO, uncooperativeness will not be an abuse because the nodes are stimulated and not forced to relay others’ packets
using their own devices as packet relay incurs a cost of energy and other resources, but frequently dropping packets are an obvious abuse due to disrupting the network proper operation. Since a trusted party may not be involved in a communication route, the nodes in the route submit receipts (proofs of packet-relay) to an offline trusted party. For efficient implementation, a novel technique for measuring the nodes’ frequency of dropping packets based on processing the receipts instead of using the traditional medium overhearing technique are proposed. The trusted party processes the receipts to extract financial information to reward the intermediate nodes and to charge the source and destination nodes, and contextual information, such as the broken link, to build up a reputation system to identify the irrational packet droppers. The trusted party placed offline which increases the overhead of submitting and clearing the receipts from the network node and trusted party.

2.7 DEFENSE TECHNIQUES FOR WSN

Hongmei Deng et al (2009) proposed a trust-aware in-network aggregation approach for resilient WSNs, in which the trust evaluation mechanism is applied to identify trustworthiness of sensor nodes, distinguish illegal/misbehaving nodes and filter out bogus data in the aggregation process.

The network model is simplified by assuming ‘n’ sensor nodes for each aggregation point and secures transmission link between sensor nodes. The aggregation node is assumed to be trustworthy which evaluates the trust and identifies the misbehaving nodes.

Proano Alejandro & Loukas Lazos (2012) have addressed the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. They illustrated the advantages of selective
jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. They show that selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, they developed three packet hiding schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. They analyzed the security of their methods and evaluated their computational and communication overhead. These packet hiding schemes address only jamming attacks and they have left a way for minimizing tampering attacks using these hiding schemes.

A light-weight trust based routing protocol has been proposed by Marchang & Datta (2012). Every node in the network independently executes a trust model to estimate the trust it has on other nodes in network. The intrusion detection system IDS used for estimating the trust that one node has for another consumes limited computational resource. IDS takes care of only two kinds of attacks namely black hole attack and grey hole attack. Every node maintains a value for each of its neighbors. This value is a measure of the level of trust it has on its neighbor. The trustworthiness of the route depends on the reliability of all the nodes in the route. Several secure routing protocols presume the existence of a centralized or distributed trusted third party in the network has been pointed out by Pirzada et al (2006). Trust based routing is considered as a viable security solution, in which a trust based scheme is used to protect the routing protocol.

In a network, trust helps its elements to decide whether another member of the same network is being uncooperative or malicious. Trust becomes quite important in self-configurable and autonomous systems, such as wireless sensor networks. However, very little effort has been done in the field of trust management in WSN. On the other hand, some efforts have been
made in quite related fields such as Ad-hoc and P2P networks. Carmen Fernández-Gago et al (2007) provided an overview of existing trust management solutions, mainly those developed for Ad-Hoc and P2P networks and, more importantly, investigate their suitability to WSN. Some guidelines to aid the development of trust management systems for WSN according to the nature of these networks have been discussed. One of the biggest constraints regarding trust management for sensor networks is the overhead that the existence of this system may impose over the constrained elements of the network. It is then imperative to balance the overhead of the data collection process, and to make both these processes and the trust and reputation models as lightweight as possible.

Yan Sun et al (2008) described trust evaluation mechanism in distributed networks such as MANET and sensor networks, with a focus on protecting such systems against malicious attacks. In particular, the advantage of integrating trust in distributed networks is demonstrated through a synthesis on the roles of trust. The bad mouthing attack, on-off attack and conflicting behavior attack against trust evaluation are investigated using recommendation trust in malicious node detection which reduces the detection rate. The attack detection mechanisms in sensor networks using trust management are limited to certain attacks.

Momani & Challa (2010) introduced the security and trust concepts in wireless sensor networks. Surveys of trust and reputation systems in various domains were explained in detail for Ad-hoc and sensor networks. The methodologies used to model trust and their references are presented. The factors affecting trust updating are summarized. The survey states that, even though researchers have started to explore the issue of trust in wireless sensor networks, they are still examining the trust associated with routing messages between nodes. This is in contrast to the research, which takes into
consideration not only the communication side but also the continuous sensed data, which is a unique characteristic of sensor networks and has never been addressed by trust researchers in WSNs.

Intruder detection systems which can detect the malicious nodes are very expensive for wireless sensor networks and there is no guarantee in detecting a malicious node. In the current research, a trust-based approach is recommended to minimize the overheads of intruder detection system and detect the abnormal behavior nodes. The model proposed by Yenumula Reddy (2011) uses the repeated games to detect faulty (malicious) nodes through the cooperative effort in the sensor network and judges the trust of successive nodes. The trust models and trust-based approach in sensor networks discussed introduce the role of repeated game in trust models and calculate the average discount payoff verses number of packets dropped. The model identifies that large time slots provide better results than observing the packet dropping in a short period of time. Further, the model for trust relation among the nodes was presented and prediction of a trusted node in the path was discussed using game model. Automatic collaborative filtering approach is useful to transfer the data with minimum overheads. The method limits the discussion for event based and cluster based approaches.

Detection of malicious node in the neighborhood with minimal infrastructure and computations is a requirement in wireless sensor networks. The existing models require more computation, storage, and complex security calculations. These models are inefficient in wireless sensor networks due to their resource limitations. Therefore, an agent-based approach that maintains the node’s current status has been adopted in the literature (Yenumula Reddy 2012). In agent-based detection approach is possible through maintaining the ratings of each node. The ratings of a node are being done through the ratio of packet forwarded by packets received. Further, the ratings can be done using the
E-commerce models. The proposed agent-based framework uses reputation of a node through neighboring nodes as part of trust calculation which increases the overhead in the network. An event based trust models for specific data has not been addressed in this model.

Mehmet Celenk et al (2008) presented a method of anomaly detection based on adaptive Weiner filtering of noise followed by ARMA modeling of network flow data. Noise and traffic signal statistics are dynamically calculated using network-monitoring metrics for traffic features such as average port, high port, server ports and peered port. The port measurements are used to confirm the anomaly prediction as part of the majority voting scheme. The proposed method limits the use of multiple features and additional defense mechanisms for estimating cyber attack which will improve the system accuracy and reliability.

An approach that is based on relatively short-term observations of network features and their respective time averaged entropy values has been proposed by Mehmet Celenk et al (2010) to detect the network anomaly. This approach helps in determining acute and a long-term change in the network feature space and presents system status in a visually compact information graph. A statistical analysis using ARMA and wiener filtering is applied to predict the network traffic flow. First, average entropy for each feature is calculated for every second of observation. Then, the resultant short-term information measurement is subjected to first and second-order time averaging statistics. The process then applies the modified FLD to the underlying time averaged network entropy to identify the exact time of the security incident or attack on the network such as worm outbreaks, bonnet command and control traffic, un-configured network devices, or Denial of Service attacks.
Dingding Zhou et al (2012) have proposed a network traffic prediction based on Auto Regressive Fractionally Integrated Moving Average (ARFIMA) modeling. It is a time series forecasting model, which is an improved ARMA model, a deeply studies on ARFIMA model and adopts ARFIMA model to predict real trace records and net flow sampling flow records. This traffic prediction model adopts three traditional models to forecast the traffic data using Root Mean Square Error (RMSE) and Relative Root Mean Square Error (RRMSE). This model limits its analysis with only traffic prediction which can be extended for further defense mechanisms like network anomaly detection.

2.8 SWARM INTELLIGENCE IN WSN

A number of optimization algorithms, modeled using incorporating swarm behavior, are Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO), Gravitational Search Algorithm (GSA) and Intelligent Water Drops (IWD). Some of the applications of swarm intelligence are discussed below.

Rajani Muraleedharan & Lisa Ann Osadciw (2006) has proposed extension to the security of physical layer of a predictive sensor network model using swarm intelligence and ant system wherein they create an ant agent which proactively uses the WSN node’s information (key performance parameters), as it traverses a route from node to node, to predict or anticipate jamming, and accordingly, to change the route to avoid jamming. They suggest a decision threshold, called probability of selecting a link between nodes i and j, called Pij, to be calculated at node i. They describe that if the calculated Pij is within the acceptable limits then the agent selects the link for its travel; else, it rejects it and selects that link whose Pij is within the acceptable limits. Pij, as suggested by them, is to be calculated using complicated formulae. Although the approach to the problem is novel, where it is obvious that it is not
workable for detecting a jamming attack, especially in an information warfare environment, because: (1) some of the data, e.g., packet delivery ratio and the packet loss on a link, will not be readily available normally, and if they are to be kept readily available, they will be at the cost of memory space of the node, (2) some of the data, like BER, are extremely complicated to be ascertained and involve communicating with other nodes, which may not be possible under jamming, (3) it is computation-intensive and taxes the resource-starved WSN node, (4) it involves of fixing threshold of the decision parameter for each node under different conditions, which is fraught with pitfalls and (5) it is based on evolutionary algorithms whose complexities in terms of time and space is difficult to ascertain, but are important to be minimized for any resource-constrained network, like the WSN. This system has not been tested for large-scale simulated WSNs.

Rashedi et al (2009) proposed a new optimization algorithm based on the law of gravity and mass interactions. In the proposed algorithm, the searcher agents are a collection of masses which interact with each other based on the Newton gravity and the laws of motion. Agents are considered as objects and their performance is measured by their masses. All these objects attract each other by the gravity force, and this force causes a global movement of all objects towards the objects with heavier masses. Hence, masses cooperate using a direct form of communication, through gravitational force. The gravitational force is a way of transferring information between different masses.

The Intelligent Water Drops (IWD) algorithm is a new swarm-based optimization algorithm inspired from observing natural water drops that flow in rivers proposed in the survey (Shah-Hosseini, 2009). The IWD algorithm which is tested to find solutions of the $n$-queen puzzle with a simple local heuristic. The Travelling Salesman Problem (TSP) is also solved with a
modified IWD algorithm. Hamed shah & Hosseini (2009) has proposed intelligent water drops algorithm based on nature inspired swarm optimization algorithm which to deal with optimization problems in finding solutions with good or optimal path from source to destination. It also demonstrates that the nature is an excellent teacher for designing and inventing new swarm-based optimization algorithms.

Dhurandher et al (2009) presented an Ant Colony Optimization approach for reputation and quality-of-service-based security in WSNs. They specifically proposed a quality-based distance vector protocol known as QDV, where the more reputation a node has, the more reliable it is for communication purposes. QDV is able to protect the network against packet injection by those malicious nodes which have been detected. This protection is made by identifying those nodes that drop the packets forwarded to them. In this model reputation is based on pheromone content of a path for communication. Thus, a path having more deposits of pheromone is considered more secure. Finally, the Quality-of Security, QSec, depends on the two previous parameters and defines the communication and transfers between two nodes. It is the deciding factor as to which node needs to be selected as the next node in the path and is computed as the weighted sum of reputation and QoS.

\[
W_n(t) = w_1q(t) + w_2\hat{q}(t)
\]  

Gómez Mármol Félix & Martinez Perez (2010) proposed, BTRM-WSN a Bio-Inspired Trust and Reputation Model to achieve most trustworthy path leading to the most reputable node. This model helps the node requesting a certain service to the network to find the most trustworthy route. A node is considered untrustworthy either it intentionally provides a fraudulent service or because it provides a wrong one due to hardware failures or performance deterioration. It is assumed that every node will know only its
neighbors wireless range and nothing else about the whole topology of the network. The topology is considered to be relatively dynamic, with many nodes entering or leaving the community. If this frequent switch on and off of nodes in the network is not considered.

Fatih celik et al (2010) proposed a survey on swarm intelligence based routing protocols in wireless sensor networks. Swarm intelligence based routing protocols can remove at least one or several problems in the area such as battery life, scalability, maintainability, survivability, adaptability and so on. A detailed review on various swarm based routing algorithms has been discussed which can be incorporated for various applications.

A survey based on Swarm Intelligence routing protocol for wireless sensor networks and future direction was given by Muhammad Saleem et al (2011). The basic mechanisms at work in biological systems reversed Engineers to design novel algorithms for distributed optimization and control. The analogy between biological systems and routing in networks, and in particular in WSNs, is strict. The ant/bee colony can be seen as a distributed adaptive system of smart control packets. Each of these packets makes little use of computational and energy resources to explore the network/environment. They efficiently cooperate with each other by releasing at the nodes information about the discovered paths and their estimated quality. Due to these similarities between foraging behaviors in insect societies and network routing, in the last decade, a relatively large number of SI based routing protocols have been developed for wired networks, satellite networks, MANETs and more recently, WSNs. This paper is the first attempt to review and critically discuss the most prominent SI-based routing algorithms that have been developed for WSNs. This survey aims at
(i) Making a wide audience aware of the existence and of the usually good performance of a number of SI-inspired WSN routing protocols.

(ii) Highlighting strengths and weaknesses of the proposed algorithms with respect to the central constraints and objectives of routing in WSNs.

(iii) Pointing out a number of methodological flaws common to many work proposing and evaluating WSN routing protocols based on SI.

(iv) Identifying and proposing a scientifically sound experimental methodology and new research directions for this relatively novel research domain.

Qureshi et al (2011) proposed an algorithm to detect malicious beacon nodes based on swarm of intelligent water drops to provide secure localization in wireless sensor networks. IWD algorithm based approach detects the nodes malicious behavior due to security attacks associated with WSN localization. The algorithm detects Sybil Attack, Replay Attack, Wormhole Attack and False node using distances estimation using TOA, TDOA and RSS. More than one malicious node is difficult to detect in the network.

2.9 CONCLUSION

Security is a first and foremost concern in many networking scenarios which replaces the performance rapidly. In this chapter many aspects of wireless sensor network security are described: challenges, requirements, defense techniques and possible attacks. The main aim is to provide a general overview of sensor networking security and highlight the need for efficient defense techniques able to withstand various attacks that
target their confidentiality, functionality and availability. Related literature has been reviewed with a focus on studies proposing solutions for WSN security.

During the literature review, it is observed that research on security considerations for wireless sensor networks have recently begun to get attention of researchers. However, studies on the envisioned WSN applications of near future indicate that applications such as military surveillance or health monitoring have security and privacy requirements. Based on those observations elaborated above, derived from an extensive survey of the pertinent literature, there is a lack of research regarding achievement of security using swarm intelligence for IEEE802.15.4 based wireless sensor networks.

In Chapter 3, a swarm based defense technique to detect the physical layer attack like jamming attack has been proposed. In which the sender and receiver change channels using frequency hopping technique in order to stay away from the jammer. An algorithm based on swarm intelligence collects the channel information from ant agents which verifies the prevalence of the attacker for long time and avoids the particular channel for transmission in order to improve the performance of the network.

Chapters 4 present an algorithm for detecting denial of sleep attack in WSN. Time series S-ARMA (Swarm intelligence Auto Regressive Moving Average) model is proposed to predict the network traffic in future using Swarm intelligence and Auto Regressive Moving Average. This model estimates the difference in actual and predicted traffic. Based on the inaccuracy of traffic, frequency hopping is initiated. Frequency hopping time is calculated and the information about each channel in the network is collected by swarm intelligence technique. S-ARMA model alerts the network to avoid the particular channel which is affected by DoS attack, based on
inaccuracy of network traffic and frequency hopping time in wireless sensor networks.

Chapter 5 introduces Swarm Based Trusted Node model (SBTN-TC) which detects tampering and cheating attack in WSN. This defense technique incorporates trusted node selection scheme which selects the trusted node based on highest trust value using swarm intelligence and cryptographic puzzle hiding scheme to identify the frequently packet dropping node. The sets of algorithms proposed for various attacks will have practical application in real-world deployments and can be considered as a reference point for further investigation of more attractive solutions against various kinds of higher layer attacks.