Chapter 1

Introduction

IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LRWPANs). It is maintained by the IEEE 802.15 working group, which has defined it in 2003. It is the basis for the ZigBee, ISA100.11a, WirelessHART (W-HART), and MiWi specifications, each of which further extends the standard by developing the upper layers which are not defined in IEEE 802.15.4[1]. Alternatively, it can be used with 6LoWPAN [2] and standard Internet protocols to build a wireless embedded Internet. IEEE standard 802.15.4 intends to offer device level wireless connectivity, which focuses on low-cost, low-speed ubiquitous communication between devices (in contrast with other, more end-user oriented approaches, such as Wi-Fi), low power consumption and self-organization features. The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more.

The basic framework conceives 10 meter to 80 meter communications range with a transfer rate of 250 kbps to 1mbps. The low rate WPANs(IEEE 802.15.4/LRWPAN) is intended to serve a set of industrial, residential and medical applications with very low power consumption and cost requirement not
considered by the above WPANs and with relaxed needs for data rate and QoS. The low data rate enables the LRWPAN to consume very little power.

The main identifying feature of IEEE 802.15.4 among WPANs is the importance of achieving extremely low manufacturing and operation costs and technological simplicity, without sacrificing flexibility or generality.

Important features include real-time suitability by reservation of guaranteed time slots, collision avoidance through CSMA/CA and integrated support for secure communications. Devices also include power management functions such as link quality and energy detection.

1.1 ZigBee and IEEE 802.15.4

ZigBee technology is a low data rate, low power consumption, low cost, wireless networking protocol targeted towards automation and remote control applications. IEEE 802.15.4 committee started working on a low data rate standard a short while later. Then the ZigBee Alliance and the IEEE decided to join forces and ZigBee is the commercial name for this technology. ZigBee is expected to provide low cost and low power connectivity for equipment that needs battery life as long as several months to several years but does not require data transfer rates as high as those enabled by Bluetooth. In addition, ZigBee can be implemented in mesh networks larger than is possible with Bluetooth. ZigBee compliant wireless devices are expected to transmit 10-75 meters, depending on the RF environment and the power output consumption required for a given application, and will
operate in the unlicensed RF worldwide (2.4GHz global, 915MHz Americas or 868 MHz Europe). The data rate is 250kbps at 2.4GHz, 40kbps at 915MHz and 20kbps at 868MHz. IEEE and ZigBee Alliance have been working closely to specify the entire protocol stack. IEEE802.15.4 focuses on the specification of the lower two layers of the protocol (physical and data link layer). On the other hand, ZigBee Alliance aims to provide the upper layers of the protocol stack (from network to the application layer) for interoperable data networking, security services and a range of wireless home and building control solutions, provide interoperability compliance testing, marketing of the standard, advanced engineering for the evolution of the standard. This will assure consumers to buy products from different manufacturers with confidence that the products will work together.

IEEE 802.15.4 is now detailing the specification of PHY and MAC by offering building blocks for different types of networking known as “star, mesh, and cluster tree”. Network routing schemes are designed to ensure power conservation, and low latency through guaranteed time slots. A unique feature of ZigBee network layer is communication redundancy eliminating single point of failure in mesh networks. Key features of PHY include energy and link quality detection, clear channel assessment for improved coexistence with other wireless networks.
1.2 Components of LRWPAN

LRWPAN system consists of several components. The most basic is the device. A device can be a full-function device (FFD) or reduced-function device (RFD). A network shall include at least one FFD, operating as the PAN coordinator. The FFD can operate in three modes: a personal area network (PAN) coordinator, a coordinator or a device. An RFD is intended for applications that are extremely simple and do not need to send large amounts of data. An FFD can talk to RFDs or FFDs while an RFD can only talk to an FFD.

1.3 Network Topologies

Figure 1.1 shows 3 types of topologies that LRWPAN supports: star topology, mesh topology and cluster tree.

1.3.1 Star Topology

In the star topology, the communication is established between devices and a single central controller, called the PAN coordinator. The PAN coordinator should be mains powered whereas the devices are required to be battery powered. Applications that benefit from this topology include home automation, personal computer peripherals, toys and games. After an FFD is activated for the first time, it may establish its own network and become the PAN coordinator. Each start network chooses a PAN identifier, which is not currently used by any other
network within the radio sphere of influence. This allows each star network to operate independently.

1.3.2 Mesh Topology

In contrast to star topology, any device can communicate with any other device as long as they are in range of one another. A peer-to-peer network can be ad hoc, self-organizing and self-healing. Applications such as industrial control and monitoring, wireless sensor networks, asset and inventory tracking would benefit from such a topology. It also allows multiple hops to route messages from any device to any other device in the network. It can provide reliability by multipath routing.

Figure 1.1: Network topologies for star, mesh and cluster
1.3.3 Cluster Tree Topology

In the cluster tree topology, each device is capable of communicating with any other device within its radio sphere of influence. One device will be nominated as the PAN coordinator, for instance, by virtue of being the first device to communicate on the channel. Further network structures can be constructed out of the cluster tree topology and may impose topological restrictions on the formation of the network. An example is the cluster tree network, as shown in the figure 1.1, which is a special case of a peer-to-peer network in which most devices are FFDs. An RFD may connect to a cluster tree network as a leave node at the end of a branch, because it may only associate with one FFD at a time. Any of the FFDs may act as a coordinator and provide synchronization services to other devices or other coordinators. Only one of these coordinators can be the overall PAN coordinator, which may have greater computational resources than any other device in the PAN.

1.4 LRWPAN Device Architecture

Figure 1.2 shows an LRWPAN device. The device comprises a PHY, which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and a MAC sublayer that provides access to the physical channel for all types of transfer. The upper layers consists of a network layer, which provides network configuration, manipulation, and message routing, and application layer, which provides the intended function of a device. An IEEE 802.2 logical link
control (LLC) can access the MAC sublayer through the service specific convergence sublayer (SSCS) [3].

Figure 1.2: LRWPAN Device Architecture

1.5 IEEE 802.15.4 Superframe Structure

The IEEE 802.15.4 standard allows the optional use of a superframe structure. The superframe is bounded by network beacons sent by the coordinator and is divided into 16 equally sized slots. All transactions shall be completed by the time of the next network beacon. The beacons are used to synchronize the attached devices, to identify the PAN, and to describe the structure of the superframes. The format of the superframe is defined by the coordinator. The superframe can have an active and an inactive portion, as shown in figure 1.3.
The active portion of each superframe is composed of three parts: a beacon, a contention access period (CAP) and a contention-free period (CFP) [4]. The beacon shall be transmitted, without the use of carrier sense multiple access with collision avoidance (CSMA-CA), at the start of slot 0, and the CAP shall commence immediately after the beacon. Any device wishing to communicate during the CAP between two beacons shall compete with other devices using a slotted CSMA-CA mechanism. The CFP, if present, follows immediately after the CAP and extends to the end of the active portion of the superframe. No transmissions within the CFP shall use a CSMA-CA mechanism to access the channel. For low-latency applications or applications requiring specific data bandwidth, the PAN coordinator may dedicate portions of the active superframe to that application. These portions are called guaranteed time slots (GTSs). Any allocated GTSs shall be located within the CFP. The PAN coordinator may allocate up to 7 of these GTSs, and a GTS may occupy more than one slot period. However, a sufficient portion of the CAP shall remain for contention-based access of other networked devices or new devices wishing to join the network. All contention-based transactions shall be complete before the CFP begins. Also, each
device transmitting in a GTS shall ensure that its transaction is complete before
the time of the next GTS or the end of the CFP. Then, during the following
inactive portion, the coordinator shall not interact with its PAN and may enter a
low-power mode.

1.6 Security Requirements for IEEE 802.15.4

Generally an LRWPAN is organized as a star or peer to peer topology (cluster)
depending on the application. A network topology may considerably affect the
overall power consumption of the system. Thus, it is important to design a star
topology for self-organizing LRWPAN to reduce the power consumption.
Conserving battery power is very significant because battery life is not expected
to increase significantly in the coming years. However, one critical issue of
security exists in wireless networks especially some attacks are medium
dependent and do not exist in the earlier counterpart [5], [6]. Traditionally
distributed denial of service (DDoS) attacks is carried out in MAC layer such as
jamming, exhaustion, and collision. The wireless medium introduces many those
attacks which cannot be easily addressed by the traditional protection methods.
One significant set of such attacks is DDoS which is concerned with satisfying
user or system domain buffers. But in wireless realm, attackers may attain ability
to prevent legitimate nodes from communication by capturing the medium. It is
because wireless networks are constructed via open medium which creates a
trouble-free path for intruders to introduce such attacks [7]. In wireless network
defenses like cryptography, pass-phrase sharing etc can be overrun by a simple DDoS attack that can shutdown the whole network. In order to ensure the smooth and uninterrupted network operation in mission-critical environments, it is essential to protect these networks from attacks that may be launched by the adversary class, with the intent of causing loss or damage to the network.

Security in wireless networks has become an active research area in recent years. Much related research work has been done for both wireless mobile ad hoc networks and wireless sensor networks, including key management [8], [9] authentication [10], [11], [12], secure routing, cooperation and unfairness [13]. With the proliferation of LRWPANs, the availability of security services for those networks will become a key issue. In the following sections, we first present the general security objectives.

**Data Confidentiality**: The main goal of data confidentiality is to ensure that sensitive data are not disclosed to any entities other than the intended receivers. Confidentiality is the basic method to prevent passive attacks. A standard approach to protect the confidentiality of sensory data is to encrypt it using a cryptographic key. The resource constrained nature of sensor nodes makes it a challenge to generate, store, and use cryptographic keys of any kind, asymmetric or symmetric.

**Data Authentication**: The authentication of messages exchanged between the sensor nodes is necessary to ensure protection against hoax messages that may be
injected into the network by an adversary. Such an attack may have catastrophic consequences considering the mission critical nature of sensor applications.

**Data Integrity**: Data integrity ensures that the received data is not modified or tampered with on its way from the sender to the receiver. For instance, in a bush fire sensing network, an adversary may attempt to alter sensor readings to trigger an alarm which otherwise would have been initiated only for actual emergency scenarios.

**Data Freshness**: An old set of messages i.e. sensor readings may be replayed by an adversary to mock a potential emergency in a normal situation. Therefore, it is essential to ensure the freshness of all data exchanged within the sensor networks.

**Data Availability**: Sensor nodes deployed in untrusted environments for carrying out critical operations must be able to survive the expected battery lifetimes. Premature exhaustion of the limited battery lives of sensor nodes may have a catastrophic effect on operations of the entire network. An adversary may attempt to launch an attack against valuable resources in the sensor network to exhaust their energy resources, and cause the network to be disabled from continuing to operate and carry out its designated tasks pertaining to environment sensing and detection.

Such an attack leads to denied access for the base station to sensory data, which may be crucial for critical applications. Therefore, these types of attacks are
referred to as Denial of Service (DoS) attacks. The DoS attack may or may not be launched from a single end point of the network, wherein a single compromised node or a node belonging to an adversary, repeatedly sends hoax requests to a legitimate target sensor node with the intent of exhausting its limited energy resources. On the contrary, an intelligent attacker may launch the attack from multiple ends of the network by compromising enough available resources to ensure high success in the attack process. The distributed nature of this attack is called a Distributed Denial of Service (DDoS) attack.

1.7 Background of DDoS in IEEE 802.15.4

DDoS is that lots of clients simultaneously send service requests to certain server on the internet through wireless network such that this server is too busy to provide normal services for others. Attackers using legitimate packets and often changing package information, so that traditional detection methods based on feature descriptions are difficult to detect it, shown in figure 1.4. Distributed denial of service attacks in sensor networks may be defined as attacks which are launched by an adversary triggering multiple zombie or compromised sensor nodes to send hoax requests to a target sensor node in the network at very short time intervals. As a consequence, the target node is overwhelmed with more number of requests than its maximum processing capacity, thus incapacitating it from providing any further service to its clients [14],[15]. Such attacks may also rely on the usage of laptop-class adversaries, i.e. adversaries with a few orders of
magnitude higher computational power than normal sensor nodes, with forged identities of legitimate sensor nodes operating in the network. More specifically, distributed denial of service attacks in a sensor network may lead to exhaustion of the limited energy resources of a target node, owing to the large inflow of requests towards it. Therefore, we also refer to a distributed denial of service attack in a sensor network as a distributed energy-exhaustion attack. It may be noted that distributed energy-exhaustion attacks in sensor networks are analogous to flooding attacks in high-performance networks wherein, an adversary triggers the generation of a flood of requests towards the victim node from several ends of the network with the intent of incapacitating it from providing additional service.

![DDoS Attack Model](image)

**Figure 1.4: DDoS Attack Model**

A.D Wood *et al* classified the denial of service attacks at various layers of operation within a typical sensor network [14]. Sensor network design must incorporate the level of damage an adversary may cause to the functionality of the network, as well as the failure tolerance levels of the network, to ensure a certain
degree of robustness to node or route failure. Moreover, the asymmetry in the resources between the sensor network and the adversary must be considered prior to design of any security scheme. It may happen that a sensor network deployed in enemy territory is subverted or disrupted by an already existing wired network or power grid existing in the field.

Figure 1.5: A High-level illustration of a Distributed Denial of Service Attack in a Wireless Sensor Network

As shown in figure 1.5, a single victim node may be targeted with overwhelming number of incoming requests from multiple ends of the network. The attacker nodes can either be legitimate but compromised nodes operating in the network, or be a laptop-class adversary, i.e. an adversary with higher capabilities, using forged identities to generate a large set of legitimate packets for overwhelming the victim node. It is assumed that no pre-hand information is available to elude
towards critical (potential victims) nodes in the network. Therefore, an adversary must have observation capabilities for a certain period of time to identify on the critical nodes in the network. Intelligent set of adversaries will launch the distributed denial of service attacks from multiple ends of the network so as to avoid being detected by a detection module observing traffic flow from a single point of origin in the network. For example, figure 1.6 indicates the correct sequence of messages being exchanged without an attacker present and the message sequence with an attacker M in the middle. To both A and B the sequence looks the same as extra messages have been jammed.

![Diagram showing DATA and ACK exchanges](image)

Figure 1.6: Example for DDoS attack in LRWPAN

1.8 Motivation and Objectives

The DDoS attacks trying to interfere with the physical transmission and reception of wireless communications. Attacks are caused by jamming, exhaustion, collision at MAC layer. At the MAC layer, the jammer can only jam
the receiver by transmitting high power at the network frequency and lowering the signal-to noise ratio below the receiver’s threshold. However, it cannot prevent the transmitter from transmitting, and hence it cannot jam the transmitter and it can jam the receiver by corrupting legitimate packets through protocol violations, also jam the transmitter by preventing it to transmit by capturing the carrier through continuous transmission and the resources that are targeted are battery power, bandwidth, and computational power [16], [17]. In the following section we discuss the objectives of detection and prediction of attacks in IEEE 802.15.4.

Detection of Attacks

The purpose of DDoS attack detection is met in its entirety if the detection rate is close to 100%. It is achieved through fuzzy systems. The attack detection is done by the base station on the input values of detection metrics received by it, from the respective node. There are inputs that required to be sent by the nodes to the base station. They are

1. SNR – No. of packets received by it during period of time.
2. BPR – No. of packets dropped by it during period of time
3. RSS – to be additionally sent to the base station, which computes the power received by the node from the jammer, if any [18].

The base station uses the value of BPR and SNR as input to the Fuzzy systems (Mamdani Fuzzy Inference) to get the level of attack /Jamming Index (JI) as the
output of the system. Based on the outcome of the fuzzy rules, the LOA can be categorized into Normal, Low, Medium and High. Confirmation of attack detection using FCM, which can decide the lower cut-off value of LOA/JI to conclude that all nodes whose LOAs are > lower cut-off values are malicious node, while other are normal node. Power consumption model for LRWPAN, which is self organized to clusters using FCM. The FCM is applied to PAN coordinator selection for each cluster. A self-reconfiguring topology is proposed to manage the mobility. It also recursively update the network topology to minimizing the total energy of the system. While distribution the load evenly to the nodes has a great impact on system lifetime and it will also improve the performance of the network. It helps to reduce the overall energy computation rates incurred by the DDoS attacks detection scheme.

**Prediction of Attacks**

We adopt fuzzy system for prediction of attacks in a cluster-based wireless network in which nodes can be managed locally by cluster heads. Rotating cluster heads makes it possible to select malicious nodes as cluster heads. Adversaries can compromise any node in the network and launch DDoS attacks in IEEE 802.15.4 MAC layer such as jamming, exhaustion, and collision. As malicious nodes require abnormal energy to launch an attack, we focus on malicious nodes energy consumption rate in order to discover the compromised nodes. The two notable features of our scheme are listed as follows:
1. In contrary with the traditional detection methods detect malicious attacks based on behavior or interactions between the nodes within a period of time. A prediction method is introduced to predict the entire nodes energy consumption rate in base station and predict some energy sensitive attacks which require abnormal energy.

2. Fuzzy system for prediction of attacks distinguishes various malicious attacks like jamming, exhaustion, collision according to the energy consumption rate. Energy thresholds are set to classify the malicious attacks, so that we can be aware of the types of attacks.

To our best knowledge, the concept of energy prediction in detection area has never been discussed in any previous research works. These two specific features mentioned above collectively make fuzzy system to predict, a new, lightweight and efficient solution that can predict various attacks applied in any cluster-based wireless networks.

1.9 Thesis Outline

Chapter 2 discusses on works related to DDoS attacks such as jamming, exhaustion, collision and gives a complete comparative analysis of the existing approaches. Chapter 3 explains the various metrics for detection of DDoS attacks proposed by several scholars and explains the selection of metrics suitable for our proposed method. Chapter 4 describes proposed methods for detection of DDoS
attacks, several algorithmic parameters are defined, and optimization criteria are proposed for detection mechanism. Chapter 5 explains the proposed mechanism to predict the type of DDoS attack using fuzzy systems. Chapter 6, we analyze the results and obtain for DDoS attack detection and prediction scheme using NS 2 and perform a comparison of the acquired results with corresponding results. Chapter 7 gives the conclusions of this work and presents the possible future enhancements.