University of Cincinnati

Date: 11/23/2016

I, Abhinav Prakash, hereby submit this original work as part of the requirements for the degree of Doctor of Philosophy in Computer Science & Engineering.

It is entitled:

Rendering Secured Connectivity in a Wireless IoT Mesh Network with WPAN's and VANET's

Student's name: **Abhinav Prakash**

This work and its defense approved by:

Committee chair: Dharma Agrawal, D.Sc.

Committee member: Richard Beck, Ph.D.

Committee member: Yizong Cheng, Ph.D.

Committee member: Rashmi Jha, Ph.D.

Committee member: Wen-Ben Jone, Ph.D.

Committee member: Marepalli Rao, Ph.D.

22443

RENDERING SECURED CONNECTIVITY IN A WIRELESS IOT MESH NETWORK WITH WPAN'S AND VANET'S.

A Dissertation submitted to the

Division of Research and Advanced Studies of the University of Cincinnati

In partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in the Department of Electrical Engineering and Computing Systems of the

College of Engineering and Applied Science
University of Cincinnati
November 2016

by

ABHINAV PRAKASH

MS Computer Science

University of Cincinnati

December 2012

Thesis Advisor and Committee Chair: DR. DHARMA P AGRAWAL

DATE: 6TH APRIL 2017

Abstract

A ubiquitous pervasive network incorporates today's Internet of Things/Internet of Everything Paradigm [3–5]: Everything becomes smart with at least one microprocessor and a network interface. All these are under an umbrella of IoT/IoE paradigm where everything is network capable and connected. In most of the cases, these devices have multiple microprocessors and network interfaces at their disposal. In such a scenario, bringing every application to specific network on the same platform is critical, specifically for Sensor Networks, Cloud, WPANs and VANETs. While, enforcing and satisfying the requirements of CIA triad with non-repudiation universally is critical as this can solve multiple existing problems of ISM band exhaustion, leading to excessive collisions and contentions. Cooperative Interoperability also enables universal availability of data across all platforms which can be reliable and fully synchronized. Plug and play universal usability can be delivered. Such a network necessitates robust security and privacy protocols, spanning uniformly across all platforms. Once, reliable data access is made available, it leads to an accurate situation aware decision modeling. Simultaneous multiple channel usage can be exploited to maximize bandwidth otherwise unused. Optimizing Content delivery in hybrid mode which will be the major chunk of network traffic as predicted for near future of IoE.

Now, such a proposed hybrid network does sound very complicated and hard to establish and maintain. However, this is the future of networks with huge leaps of technological advancement and ever dropping prices of hardware coupled with immensely improved capabilities, such a hybrid ubiquitous network can be designed and deployed in a realistic scenario. In this work, we go through not only looking into the issues of the large scale hybrid WMN, but also minutely discovering every possible scenario of direct mesh clients or sub-nets (VANET, Cloud or BAN) associated to it. Further, we propose to design and implement a robust all around security and privacy for each and every possible unit of such a large network. Special focus

is provided to the application of a BAN in medical usage with intricate details is provided in form of our recent endeavor, along with an ongoing work for a wearable device patent, Smart Shoe (Patent Pending). The concepts explained with this example are equally applicable to any such Wireless Personal Area Networks (WPAN's).

Acknowledgments

I would like to thank my mentor and thesis advisor Dr. Dharma Agrawal who helped through academic research in the field of wireless and distributed computing during my graduate studies at University of Cincinnati. I would like to thank and show my gratitude to my parents and my brother who motivated me for this difficult journey of quest for knowledge. I am blessed to be a part of Center of Distributed and Mobile Computing Lab (CDMC). I want to extend my sincere thanks to all the members of the Lab. Special Thanks to the committee members for their critique work and constantly inspiring hard work. Sincere thanks to the lord Almighty for showing me the right path in difficult times and helping me make diligent choices. I would also like to thank Graduate School at College of Engineering, UC for awarding me University Graduate Scholarship to help pay for the major portion of tuition without which this would have not been possible.

Contents

List of Figures

List of Tables

Chapter 1

Introduction and Overview

1.1 Ubiquitous pervasive network

An ubiquitous pervasive network incorporates today's Internet of Things/Internet of Everything Paradigm [3–5]: Everything becomes smart with at least one microprocessor and a network interface. All these are under an umbrella of IoT/IoE paradigm where everything is network capable and connected. In most of the cases, these devices have multiple microprocessors and network interfaces at their disposal. In such a scenario, bringing every application to specific network on the same platform is critical, specifically for Sensor Networks, Cloud, WPANs and VANETs. While, enforcing and satisfying the requirements of CIA triad with non-repudiation universally is critical as this can solve multiple existing problems of ISM band exhaustion, leading to excessive collisions and contentions. Cooperative Interoperability also enables universal availability of data across all platforms which can be reliable and fully synchronized. Plug and play universal usability can be delivered. Such a network necessitates robust security and privacy protocols, spanning uniformly across all platforms. Once, reliable data access is made available, it leads to an accurate situation aware decision modeling. Simultaneous multiple channel usage can be exploited to maximize bandwidth otherwise unused. Optimizing Content delivery in hybrid mode which will be the major chunk of network traffic as predicted for near future of IoE.

Today, the number of smart devices with wireless network capabilities surrounding us in our day to day life is incredible. Such devices or sensors do promise unlimited possibilities. But, in our opinion, the

biggest achievement in today's age would be making all such devices operate in a co-operative fashion. This idea comes from the fact that there has been an explosive growth of such smart devices, wearable or otherwise. But, the main limitation is that they are primarily designed to operate independently. For example, there is a sudden flood of devices like wireless keyboards, remotes, toys, sensors etc. operating in the publicly open frequency of 2.4GHz and 5GHz, which are already heavily overloaded by Wi-Fi signal. When put all together in close vicinity, they cause interference and hinder the normal operation of each other. Not only that, they also cause lot of waste of energy and RF radiation pollution. The repercussions of excessive exposure to human body by abundant RF radiation at varying intensities and frequencies is still an ongoing research. Preliminary results show the RF radiation absorption is maximum in the range of 30MHz-300MHz [1, 2] and maybe a cause of cancer in humans. Hence, its quiet essential to design devices in a way to work cooperatively with each other so as to achieve optimal bandwidth and enhanced throughput. This goal becomes almost impossible by using regular existing network protocols. The answer to this complex problem is definitely a hybrid Wireless Mesh Network (WMN). Hence, forming a network

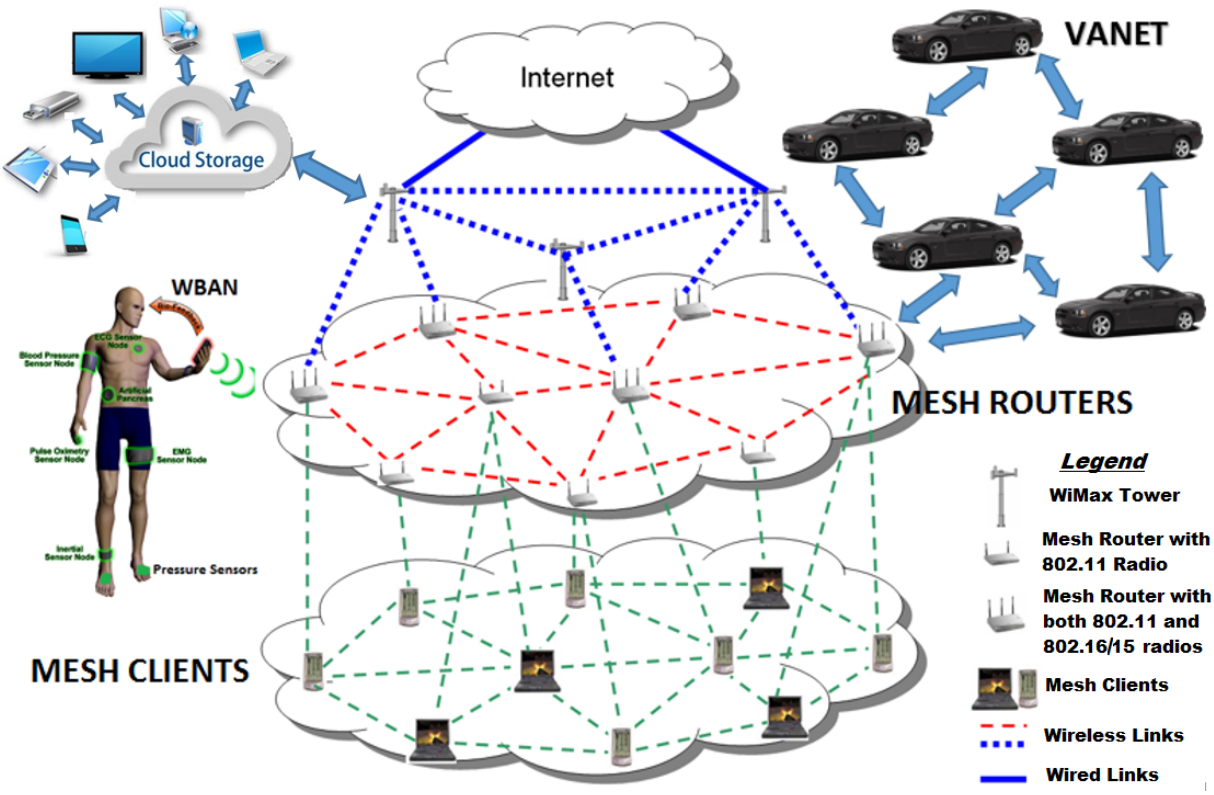


Figure 1.1: A hybrid Wireless Mesh Network

of networks which could service all kinds of devices and utilizes all different bands and radios available so to maximize the network throughput while reducing the interference to minimum. Not only that it should also provide a seamless, secure and private connectivity to different kinds of networks possible, for example, Body Area Network's(BAN's), Vehicular Network's(VANET's), Cloud Network's etc. Bringing them on the same platform so that every device is aware of other devices and networks present in it's sensing range. Further, we need to provide a communication channel irrespective of technology or frequency being used at both ends. A typical WMN is made up of mesh routers and mesh clients where mesh routers have somewhat limited mobility and they form backbone of the network whereas mesh clients are allowed to be highly mobile or completely stationary or somewhere in between. This forms a very versatile network which allows clients with different levels of mobility, interface and bandwidth requirements to be an integral part of the same network.

The communication can be achieved by directly communicating with the router by being in its range or in an adhoc fashion through several hops. A WMN is mainly designed to be dynamically self-configured and self-adjusting. This ensures large network coverage with minimum infrastructure requirements, hence low cost. Although a WMN gives multifold advantages, it is also vulnerable to several security and privacy threats being a dynamic open medium. Different types of clients such as laptops, cell phones, smart devices can join or leave the network anytime they wish. This opens up issues like fake registrations and packet sniffing. We deal with the issues of security and privacy separately in two parts in great detail by simulating countermeasures for different kinds of attacks in a WMN.

Now, such a proposed hybrid network does sound very complicated and hard to establish and maintain. However, this is the future of networks with huge leaps of technological advancement and ever dropping prices of hardware coupled with immensely improved capabilities, Such a hybrid ubiquitous network can be designed and deployed in a realistic scenario. In this work, we go through not only looking into the issues of the large scale hybrid WMN, but also minutely discovering every possible scenario of direct mesh clients or sub-nets (VANET, Cloud or BAN) associated to it. Further, we propose to design and implement a robust all around security and privacy for each and every possible unit of such a large network. Special focus is provided to the application of a BAN in medical usage with intricate details is provided in form of our recent endeavor, along with an ongoing work for a wearable device patent, Smart Shoe (Patent Pending). The

concepts explained with this example are equally applicable to any such Wireless Personal Area Networks (WPAN's).

Tools of advanced statistics such as Analysis of Variance (ANOVA), Correlation and Regression etc., have been extensively used for proof of theory, bad data identification, identifying the presence of malicious nodes/data and isolating compromised section of the network. Several routines have been proposed for network problem identification and rectification. This in turn, induces self-healing and self-configuring properties to this large scale hybrid WMN. This can said to be the most comprehensive framework for such a futuristic WMN to date. Some pattern recognition techniques have also been proposed for identifying application specific anomalies, in real time data being sampled, while switching statistical techniques depending on the presence of training data or not. Further, after identification of an anomaly, it is studied in real time to either invoke a network event or not. For example, A sudden heavy fluctuation of an ECG sensor reading can either indicate the presence of a bad sensor reading or the test subject could be actually having a cardiac arrest. The network should be equipped with enough Artificial Intelligence (AI) to invoke appropriate network event like notifying the closest health practitioner available, in this case, with an SOS signal and complete info of the test subject being monitored. This decision making process should be as free as possible from any false positives or false negative events. This has been studied in great detail as explained further in this document.

This work also deals with identifying all the major challenges faced by each sub-network of a larger WMN. Multiple best effort solutions have been proposed to individually solve such challenges encountered in different scenarios (VANET, BAN or Cloud) while preserving the integrity of such a complex network intact. Every possible scenario and parameter optimization for such a large ubiquitous network could be seen as independent research topic in itself. We have explored as much as possible within the scope of this dissertation while omitting the implied details.

Major challenges for such a network is to ensure previously discussed issues of presence of heterogeneous devices. Some of these can have serious resource Limitation: Such as Computation, Memory and Battery life, Hardware Limitation as only a single Radio with limited communication protocols at disposal. A hybrid protocol that can support or bridge all kinds of devices is found to be an effective solution.

Benefits inherited by Mesh Networking: Hierarchal division of the network enables nodes working in

Figure 1.2: Devices in the IoT Paradigm

Mesh Mode with bridging capabilities. Mesh router is the work horse of Mesh Networking. Connecting all networks provides building the Internet. Any node with multiple radios can operate in Mesh Mode. OBUs, RSUs (Roadside Units), etc.

Recent Internet developments driving towards ubiquitous architecture: Under current models, moving away from the traditional TCP/IP model and utilizing Lightweight lower layers (UDP) ensures compatibility for low end IoT devices. Further, Software Defined Networking: SDRs (Software Defined Radios) allow information availability across all layers. Most of the TCP/IP functionalities are built into the application.

1.2 Artificial Intelligence and Fog Computing

The recent developments in Artificial Intelligence and Fog Computing are groundbreaking and very relevant to this work. Network devices when equipped with Artificial Intelligence can make smart decisions based on a previously loaded rule set with little or no human intervention [6]. This capability is of utmost importance in case of highly dynamic self managing networks such as proposed in this work. Artificial Intelligence also helps critical network devices to support various clients in the network with varying services depending

on the request [7]. Advent of IoT/IoE has created a new challenge of supporting extremely large number of devices. In the traditional Internet model, such a large number of generated requests can bring down the whole network and poses a significant threat to the entire network. The concept of Fog Computing alleviates this greatly by exploiting, Artificial Intelligence heavily. Under this model, only critical data relevant for servers are sent over periodically to the cloud and in form of aggregated reports [8]. Under normal conditions, local area decisions are made by edge devices. Hence, the load of decision making process is distributed evenly over the network that greatly reduces the load from the cloud itself while still sending critical updates to the servers.

1.3 Machine Learning Methods

This is more advanced form of AI [9]: Machine Learning, Deep Learning and Big Data solutions are found be very effective for analyzing huge amount of data available in the network. Effective analysis ensures an efficient decision making process within the network. For example, classification of network traffic streams into regular behavior and anomalous behavior. Furthermore, malicious behavior within the anomalous traffic can be isolated. Machine learning methods are found to be extremely efficient in the problem of Classification and Pattern Matching. Its also used extensively for predictive analytics. Machine learning takes AI to the next level where network devices can make decisions without any explicit programming. In cases where a rule set is provided from the on set for decision making, machine learning can help to automatically adapt and modify this rule set dynamically and help it grow organically over time based on observed network data. This process is the learning part of machine learning. Common methods that are used for machine learning include Linear regression, Support Vector Machines and K-Nearest Neighbors [10].

1.4 SDN: Software Defined Networking

SDN was introduced to focus on isolating the control plane for a network and giving access to the network administrator for superior control of flow of traffic [11]. Modern SDN along with Network Function Virtualization (NFV) empowers network devices to provide feature rich services custom designed specifically for the requirement. This gives network devices much more adaptability to dynamic network requirements.

Major benefits and drivers for this development are: Cheap availability of general purpose hardware. Ex: Arduino, Raspberry Pi, etc. Our platform exploits availability of multiple radios (Ethernet, WiFi, Bluetooth) using SDN. Multiple Antennas (MIMO) and Cognitive Radios facilitate usage of all available channels for communication.

1.5 Smart Shoe Project

A part of this dissertation is also dedicated to designing novel smart wearable devices forming a Body Area Network for real time Bio-metric data analysis and feedback with the help of multiple sensors. Smart Shoe is one such device designed by us. Another example of such a device could be a wristband equipped with sensors for reading pulse, glucose level, blood pressure, location and temperature, etc. All such smart devices can work cooperatively as an integral part of the WBAN and the collective data can be used for health analysis of a human test subject. These are useful for several medical applications. A lot of health issues can be detected early on by identifying the patterns of change in such collective bio-metric data over time.

As discussed in [12], Stress fractures are well known injuries in runners caused mainly by over ex-

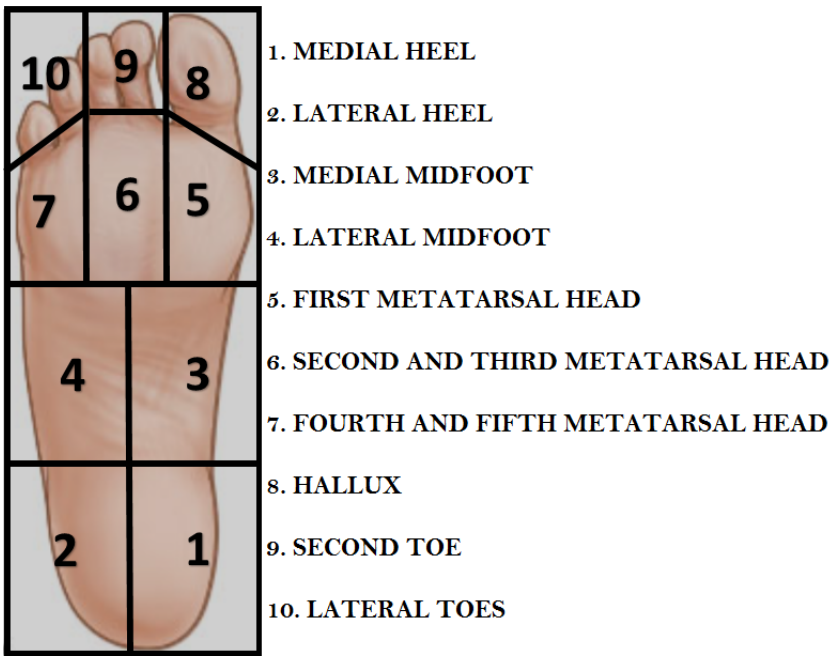


Figure 1.3: Subdivision of the footprint into 10 anatomy related masks.

haustion. Predominantly they appear most frequently in the metatarsals. Fatigue-related changes in plantar pressure patterns and its stress effects during treadmill running has been studied as possible causative factor for metatarsal stress fractures.

It is a proven fact that bone tissue keeps changing its shape by constant growth to adjust to the load and stress being put on it. Continuous sub-maximal stimuli might lessen the individual loading capability of the bone and lead to structural modifications in the regions of highest stress that may advance into stress reaction [12]. These so-called stress or fatigue fractures are the reason for most of running-related injuries. With the increasing fitness awareness, the occurrence of stress fractures has also affected more newly turned amateur athletes. The localization of these fractures is contingent on the sport movement and is focused on the metatarsals in runners. Stress fractures in the metatarsals mostly affected are the distal end or shaft of the second and third ray are also recognized as marching fractures since they were initially found in military recruits. A division of a footprint is depicted in Figure 1.3.

The authors in [12] prove that *"during the fatigued state there is a significant increase of the peak pressures, maximal forces, and impulses under the forefoot and the medial mid-foot. Investigations of the non-fatigued state showed that initial heel contact causes a plantar flexion moment. Throughout touchdown, the heel is slightly supinated, pronates during the stance phase, and returns into supination at pushoff. In the fatigued state, runners use a change in the landing technique as a compensatory strategy, which may cause an external dorsiflexion moment. This adaptational change in forefoot and midfoot loading has been suggested as a potential mechanism for the development of stress fractures. Therefore there is a potentially detrimental overloading mechanism in fatigued running with decreased calf muscle activity. The increased forefoot loading under fatigued conditions is responsible for a disturbed remodeling of the metatarsals, which increases the likelihood of the development of a fatigue fracture. It has been shown that alterations in the bony structures lead to a rapid increase in the incidence of stress fractures."* Using this breakthrough research, we design our Shoe to record important pressure patterns during various activities like running, walking and a person's manner of walking also known as Gait [13]. Several other sensors are also deployed to get additional data like temperature, humidity etc. to investigate any more correlations.

The current life style in todays era, particularly in western countries, sets up people to work uninterruptedly for a lengthy periods of time. Other than emergency situations, this is exact in many cases such

as athletes, nurses, doctors, soldiers, pilots, nightshift workers, commercial drivers, employees in hazardous environment or extreme climates, etc. Often, high level of tiredness could be fatal and detrimental to health. So, for these people to be successful, it is important to continuously monitor their fatigue level. We have devised a novel way to do so by having sensors placed and hidden inside shoe sole. To demonstrate its feasibility, we have implemented a prototype shoe as shown later in Figure 6.6.

Chapter 2

Wireless Networks and Security Issues

2.1 Network Types and Standards

2.1.1 Wireless Local Area Network (WLAN)

Wireless Mesh Network (WMN or IEEE 802.11s)

Wireless mesh network (WMN) seems to be one of the most promising wireless technologies. It consists of Internet Gateways (IGWs), mesh routers (MRs) and mesh clients (MCs). MCs can communicate with the IGW in an ad hoc fashion using multiple hops of connected MRs or directly with IGW if MC is within its communication range. MRs can act as hosts or packet forwarders to the IGW in the form of an ad hoc network. This ensures a larger coverage at a low cost infrastructure. Hence, MRs are often referred as the last mile network [14]. MCs can consist of different types of devices, like laptops, cell phones, smart devices, etc., working with different types of networks like edge, Ethernet, Wi-Fi, Wi-Max, etc. WMN makes it possible to combine characteristics of all these networks and support different types of devices using only one platform. To enable this, MRs often consist of multiple interfaces in order to perform as Network Bridge or Internet Gateway. For different technology, MCs generally have a single interface that can either be used while communicating as a host or acting as a network packet forwarder among MCs themselves in the ad hoc network mode. Hence, WMN can be said to be an advanced form of an ad hoc network which is intended to be dynamically self-designed, self-organized and healing. Existing ad hoc network protocols can be modified for a WMN.

In a WMN, MRs constitute a wireless backbone by connecting themselves through available wireless channels and MCs connect to the MRs using different interfaces in order to gain access to the internet. This creates a network hierarchical in nature where MRs communicate with each other using a wireless interface at level one while they serve the MCs using different interface at the next level and hence combine the characteristics of two different types of wireless networks. Such a network comprises of devices with varied levels of mobility and different power and computing constraints [15].

WMN offers several advantages and applications which makes further research very important. It can be directly used to provide internet access to remote areas which requires availability of low infrastructure. Another very important application of WMN is to provide different medium of wireless access. For example a cell phone in the range of a MR can route it calls through the internet via a MR at a cheaper cost instead of using the medium of higher cost low bandwidth cell phone tower. There can be several other applications where MRs can be installed to cover a large region, for example, health monitoring, traffic pattern analysis, etc.

Hybrid Wireless Mesh (IEEE 802.11s)

Hybrid Wireless Mesh Protocol (HWMP) is defined under IEEE 802.11s standard. It is an advanced routing protocol for a wireless mesh network. It is based on a hybrid of AODV and tree-based routing protocol. Even though it count on Peer Link Management protocol by which a Mesh Point known as MP discovers and tracks adjacent MPs. If any of these are linked to a backbone, HWMP works as a regular mesh, which chooses a path from those accumulated by amassing all mesh point peers into one composite map. Its called a path and not a route since under 802.11s it does not use IP addresses instead used physical MAC addresses for all addressing purposes. So, it is an hybrid approach as it can handle both scenarios where AODV is required or tree based routing [16] [17].

Vehicular Networks (VANET or IEEE 802.11p)

Vehicular transportation is by and large the largest mode of transportation used by people around the world. With increase in population time spent on road has gone up significantly. This has also led to safety issues. People spend around 10 to 15 percent of their travel time in traffic jams. Vehicular Ad hoc network is one

Table 2.1: Essential Intrinsic features of a hybrid WMN

Network Goals	**Solutions**
Energy efficient Protocols	1) Periodic Sleep and Awake Cycle function for nodes. 2) Minimizing data redundancy. 3) Low-Overhead Security Schemes.
Meeting varying level of QoS demands	1) Content-driven Routing 2) Capacity Scavenging via Un-Used link Modeling in Cognitive Networks 3) Adaptive Protocol Switching with Traffic Heterogeneity
Self-healing Protocols	1) Fault identifying and rectifying protocols 2) Intrusion detection and avoiding untrustworthy links 3) Watchdog schemes
In-network processing	On the fly decision making protocols
Mesh Routers with embedded Middle-ware	Mesh Routers equipped with multiple radios acting as cross platform bridge

of the promising research areas in wireless networks. VANETs integrate the features of Ad hoc network, Wireless and cellular technology to achieve intelligent transport systems by communicating between vehicle to vehicle or vehicle to RSUs. This is mainly due to DSRC (Dedicated Short Range Communications) standardization [18] which enables vehicles and road side units to form VANETs. Information dissemination is very important in a VANET environment. Routing plays a vital role in information dissemination. VANET routing is classified into Unicast: Vehicle to Vehicle communication, Multicast: Vehicle to multicast members through multi hop communication, Geocast: A subset of Multicast with communication targeted in a specific geographical location and Broadcast: Vehicle to all the vehicles in the coverage area.

Advantages of a VANET:

- *Vehicle Information*: Availability of Vehicular Sensor data like GPS, video cameras, detectors, sensors, RADAR, LASER, vibration and so on.
- *Traffic management*: Area Access Control, Crash Data Collection, Weather Data Collection, Intelligent Traffic Flow Control, Cooperative Planning, Adaptive Cruise Control, traffic management and so on.
- *Maintenance applications*: Software Updating, Wireless Diagnosis, Safety Recall Notice, Hardware,

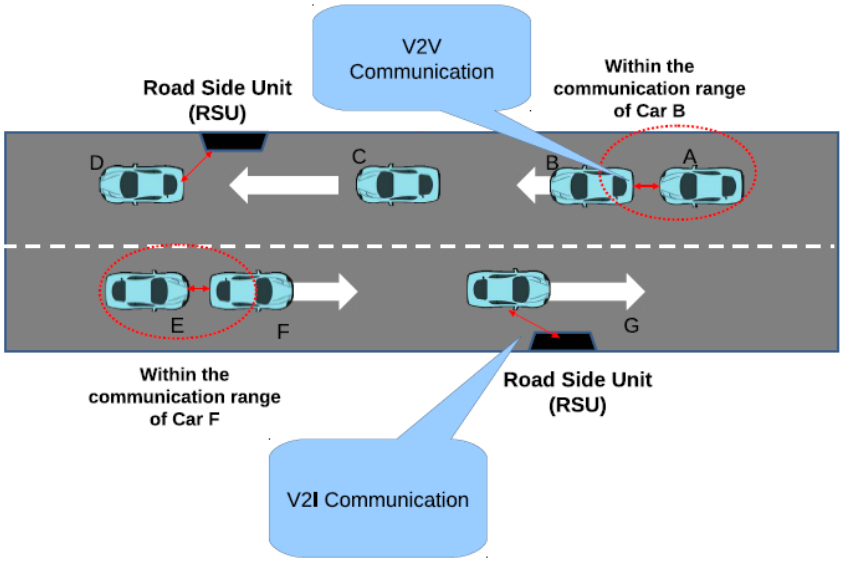


Figure 2.1: A Vehicular Network

Maintenance, Repair Notification and so on are some of the maintenance applications.

- *Enhanced driver support applications*: Internet Service Provision, Fuel Information. Media services, Region of Interest Notification, GPS Information, Location Awareness, Parking Spot Information, Route Information Downloading, Map Updating and Downloading and so on are some of the driver support applications.

Challenges in a VANET:

- *Authentication*: There should be an authentication of all the messages transmitted from one vehicle to another. Each vehicle in the network is to be authenticated by the central authority.

- *High mobility*: As the vehicle moves faster, there is a link disruption problem and handshaking is lost. By this, the vehicles are unable to interact and establish secure communication between them.

- *Location-based services*: By beaconing, we know the location of other vehicles. However, by implementing GPS, sensors, LASER, RADAR and so on we know the correct position of the vehicles.

- *Real-time system*: To develop a real-time system is a challenging task because in a high mobile area it is difficult to send a warning message in correct time before the deadline.

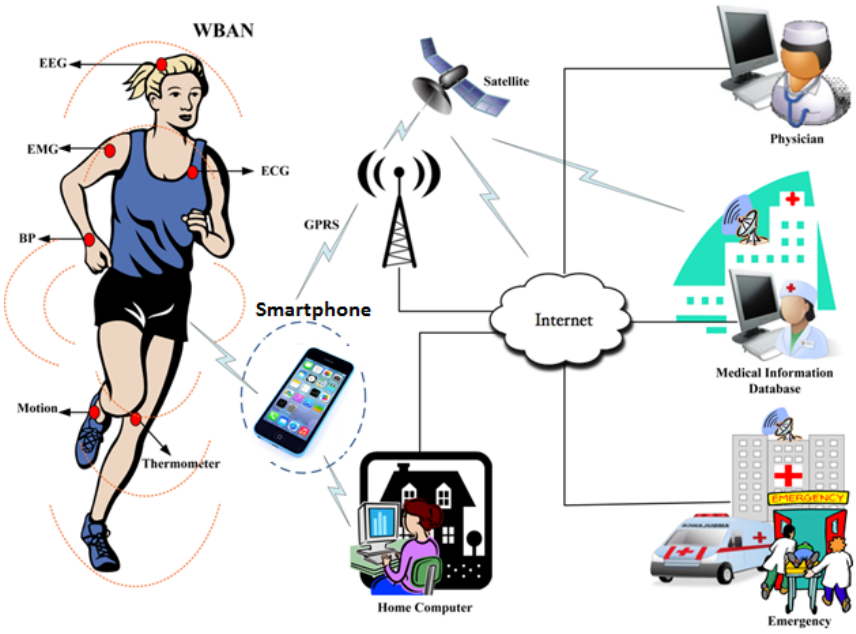


Figure 2.2: A Wireless Body Area Network

2.1.2 Wireless Personal Area Network (WPAN or IEEE 802.15)

Wireless Body Area Networks (WBAN)

Recent developments and technological advancements in wireless communication, MicroElectroMechanical Systems (MEMS) technology and integrated circuits has enabled low-power, intelligent, miniaturized, invasive/non-invasive micro and nano-technology sensor nodes strategically placed in or around the human body to be used in various applications, such as personal health monitoring. This exciting new area of research is called Wireless Body Area Networks (WBANs) and leverages the emerging IEEE 802.15.6 and IEEE 802.15.4j standards [19], specifically standardized for medical WBANs. The aim of WBANs is to simplify and improve speed, accuracy, and reliability of communication of sensors/actuators within, on, and in the immediate proximity of a human body. Several new issues have opened up in the area of Wireless Body Area Network. These sensors and actuators are available in two different forms: Wearable and Implantable.

Open issues in a Wireless Body Area Network:

- Efficient Routing Protocols
- Energy Efficiency or Preservation
- Security and Privacy
- Energy Harvesting
- Sink Node Location/Placement
- Specific absorption rate (SAR)

Figure 2.3: Cloud Services

2.1.3 Cloud Services

Cloud computing is defined as a large scale distributed computing paradigm [20]. Whereas the cloud providers or users are having their own private infrastructure, where the several types of services are pro-

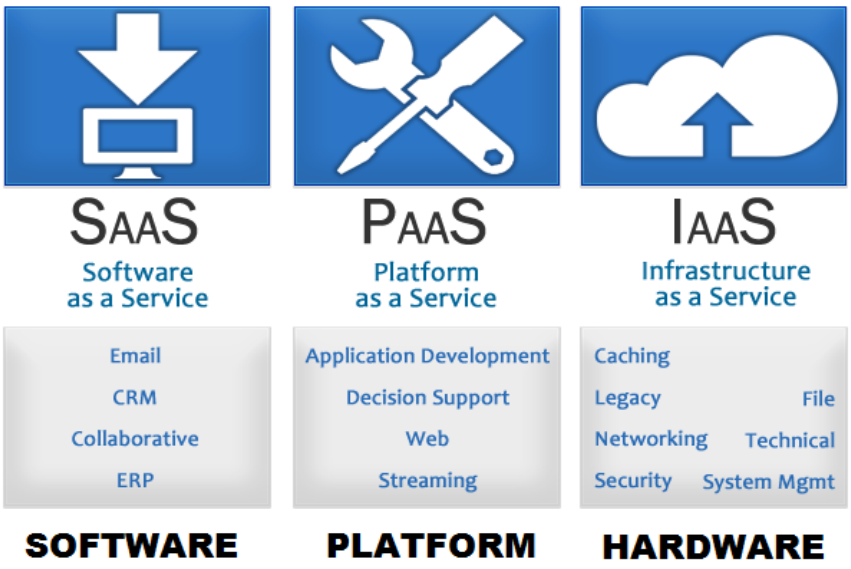


Figure 2.4: Cloud Service Classification

vided to clients using virtual machines which are hosted by providers. It includes some usage techniques which enhances the efficiency of the system.

Some are the Network Utility, Network Activity, Disk I/O utility, CPU utilization of a system and available memory for perform the operation. Cloud Computing frequently is taken to be a term that simply renames common technologies and techniques that we have come to know in IT. It may be interpreted to mean data center hosting and then subsequently dismissed without catching the improvements to hosting called utility computing that permit near real time, policy based control of computing resources. Or it may be interpreted to mean only data center hosing rather than understood to be the significant shift in Internet application architecture that it is. The major utilization methods are related to term energy. Cloud Computing can be visualized into three steps that are Cloud application, Cloud Platform and Cloud infrastructure.

Cloud computing is based on multiple utilization techniques and the services model which are IaaS, PaaS and SaaS. Cloud Computing includes IT resource consolidation Web-based applications, and mobile users who access browser- based application on mobile PCs, PDAs, smart phones, and a variety of innovative new devices. Cloud computing also highlights Web 2.0 technologies like voice and video that demand high performance / low latency connections. Several large organizations store huge amount of data in a public cloud or private cloud for backup and disaster recovery.

Cloud systems automatically control and optimize resource use by harnessing a metering proficiency at a level of abstraction relevant to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing pellucidity for both the provider and consumer of the service in use.

2.1.4 Internet of Things (IoT)

The Internet of Things (IoT) is the network of any or all physical things that are embedded with sensors, logic computer electronics and network connectivity which empowers these things to gather and interchange data. [21] The Internet of Things permits things to gather data which can be accessed remotely over the current wi-fi network [22]. IoT objects can also have motors and actuators to carry out tasks if required remotely that helps create opportunities for more direct amalgamation between the physical world and the digital world. It can also help to do mundane tasks accurately with efficiency. Every member of IoT is

uniquely identifiable through its MAC address or embedded computing system but is also capable to work along the existing Internet setup [23–25].

2.2 Security Issues

WMN is a dynamic network and hence is vulnerable to several security issues and attacks. New MCs can join or existing MCs or MRs can leave the network for a long period of time which introduces the need for some kind of authentication for all new joining devices and cancelling the authentication of old mesh nodes which no longer exist. Current security schemes for ad hoc networks and wired networks can be used to secure WMN and provide some level of security. But, Unique nature of a WMN might make most of these schemes useless. For example, public-private encryption for MC‘s certification and authentication might be computationally too complex for MCs with low power and computation availability and hence rendered impossible to use. Other schemes, like utilizing session keys might be useful. But, when a large number of MCs join and leave the WMN, it might become extremely difficult to keep track of all the keys and a large number of keys is required. Otherwise, the security could be easily compromised. The delivery of the session key securely to the right MC over a wireless medium during the initiation/registration phase is also a challenge. Furthermore, the mesh client need to be provided with some mechanism of secure communication after authentication phase most likely in form of keys keeping in mind the power and computing constraints of the MCs.

A WMN can be at the receiving end of several types of attacks like:

- False Handoffs
- Fake Registrations
- Node Capture attacks
- Snooping
- Traffic analysis
- Replay attack
- Masquerading
- Repudiation
- Sybil attack
- Tunneling
- Spamming
- GPS spoofing
- Jamming

2.3 Privacy Issues

Privacy is a very important issue to be dealt with in a WMN, specifically the location privacy. In several cases, it is very critical to hide the location of a mesh node in the WMN as there could be a physical threat or a threat of losing sensitive information to an adversary. For example, in most cases, a MC would not like it to be disclosed that it is the one in the network initiating a sensitive bank transaction. Since most of the connections in a WMN are over wireless channels which can easily be sniffed and vulnerable to packet sniffing attacks. In this way the adversary works in a passive way by just sniffing the data being transferred over a wireless connection. This information can be collected and be used to crack the transaction keys by performing statistical analysis. In this case, the biggest threat comes in the form of a global attacker which has access to all the ongoing wireless connections and keeps collecting data packets on them to analyze them to get information like keys, etc., in order for a future active attack. In [26] an active global attacker is defined which can be even more dangerous as an active global active attacker not only sniffs packets being transmitted globally but it also devises dynamic methods or algorithms in order to identify the targeted node initiating the sensitive communication by using data like transmission event duration, time taken by the packet to traverse from source to destination, packet size etc. Hence, it is very important to come up with privacy schemes to keep the mesh client anonymous in a WMN.

Chapter 3

Information Security Industry Standards

*This chapter was also published in the text book [27] as the leading chapter 1 in its entirety.

According to current industry standards a comprehensive Security and Privacy policy for an enterprise is defined as one that operates in the following eight domains:

1. **Security and Risk Management:** Confidentiality, integrity, and availability concepts.
2. **Asset Security:** Information and asset classification Ownership (e.g. data owners, system owners).
3. **Security Engineering:** Cryptography, Physical security.
4. **Communication and Network Security:** Secure network architecture design Protecting against network attacks.
5. **Identity and Access Management:** Physical and logical assets control, Protection against access control attacks.
6. **Security Assessment and Testing:** Assessment and test strategies, Security control testing.
7. **Security Operations:** Logging and monitoring activities, Physical security.
8. **Software Development Security:** Security in the software development lifecycle.

The issues related to network data security were identified shortly after the inception of the first wired network. Initial protocols relied heavily on obscurity as the main tool for security provisions. Hacking into a wired network requires physically tapping into the wire link on which the data is being transferred. Both these factors seemed to work hand in hand and made security somewhat possible with simple protocols. Then came the wireless network which changed the playing field radically. How do you secure something that travels in the free to air medium? Further, wireless technology empowered devices to be mobile making it harder for security protocols to identify and locate a malicious device in the network while making it easier for hackers to access different parts of the network while moving around. Quite often it is discussed that: Is it even possible to provide complete security in a wireless network? It can be debated that wireless networks and perfect data security are mutually exclusive. Availability of latest wideband wireless technologies have diminished the predominant large gap between the network capacities of a wireless network versus a wired one. Regardless, the physical medium limitation still exists for a wired network hence security is a way more complicated and harder goal to achieve for a wireless network. So, it can be safely assumed that a security protocol that is robust for a wireless network will provide at least equal if not better level of security in a similar wired network. Henceforth, we will talk about security essentially in a wireless network and readers should assume it to be equally applicable for a wired network.

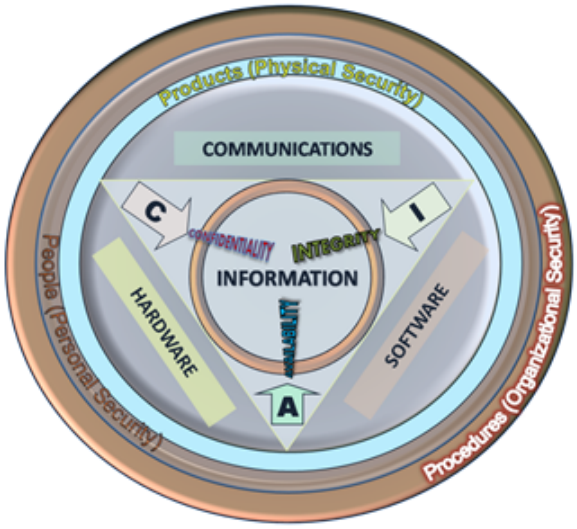


Figure 3.1: The CIA Triad

3.1 Introduction

Although a wireless network offers multifold advantages albeit it is also vulnerable to several security and privacy threats, it being a dynamic open medium. Different types of clients such as laptops, cell phones, smart devices can join or leave the network anytime they wish. This opens up issues like fake registrations and packet sniffing. This chapter deals with the issues of security and privacy in great detail by discussing countermeasures for different kinds of attacks in a network. We will discuss privacy separately and its importance which is also known as network anonymity, usually achieved employing redundancy at the cost of some associated overheads. We will start off from introductions to the basic idea of data security then discuss available standards for different types of networks and powerful tools like Encryption. From there we will build up to known types of attacks and a brief study of major data breaches of recent times. We will also talk about proposed experimental measures and solutions. Ending the chapter with our thoughts on data security and the summary. [28–32]

3.2 Goals of Security

Data Authentication: Verifying and guaranteeing the identity of the sender and receiver of the data before any data transmission is initiated [33].

Data Confidentiality: This feature is the core of security mechanism which assures that the data being transferred is only divulged to the authenticated sender and receiver. Inclusive of data attributes like date, time, content type, etc.

Data Integrity: This property assures that the data remains intact during the transmission from the sender to receiver in its original form. Meaning, no one is able to modify the data along the way during transmission which should also be verifiable at both ends of communication. Checksum is an example of such a service.

Non-Repudiation: is generally a combination of Authentication and Integrity of the data. This service facilitates proof of origin and integrity of data. In other terms no user can falsify the true ownership of data. Digital Signature is an example of such a service.

Data Availability and Reliability: In addition to all the previous features the security mechanism should also guarantee a certain threshold level of quality of service (QoS) while adding overheads to provide all such features. By having measures for intruder detection and combating various networks attacks while providing uninterrupted service at the required QoS level.

3.3 Data Encryption

Encryption is the process of cryptography in which messages or information are encoded in such a way that only authenticated people can access it [34]. An encrypted message can be intercepted along the way of transmission but by the inherent quality of the process, renders it useless to interceptor, no meaningful information is divulged. The process of encoding is referred as encryption and decoding as decryption. The original data in its true form is referred to as plaintext. The data received after performing an encryption algorithm on the plaintext is called ciphertext. A small key portion of the algorithm in form of information, which can be a seed value for the decryption algorithm, works as a missing piece of a puzzle which is kept secret. This secret is called a Key which is essential to decrypt a ciphertext to plaintext. This key is only shared with authorized people. Anyone in the possession of this key can read all the data being transmitted.

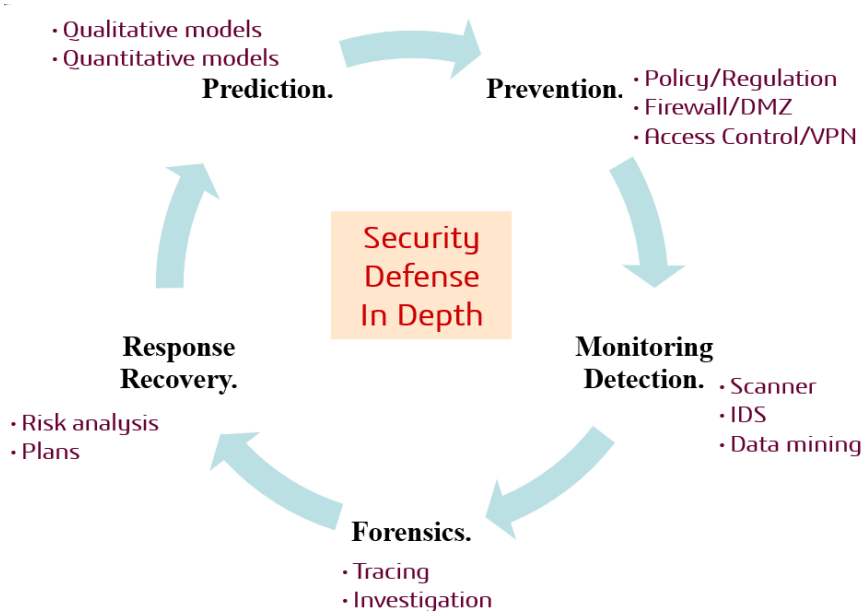


Figure 3.2: Persistent Security Process Cycle

The harder it is to crack the key or the encryption algorithm the better is the encryption algorithm. Technically, two factors are most important for reverse engineering an encryption algorithm to crack it, time and computation power required. Any good encryption algorithm designer tries to keep both these values as high as possible. Encryption schemes can be divided into two main categories, symmetric and asymmetric [35].

3.3.1 Symmetric-Key Encryption

In a symmetric encryption scheme the same key is used to encrypt a message as well as to decrypt it. This being the major weakness of this scheme. If the secret symmetric key is captured by an interceptor

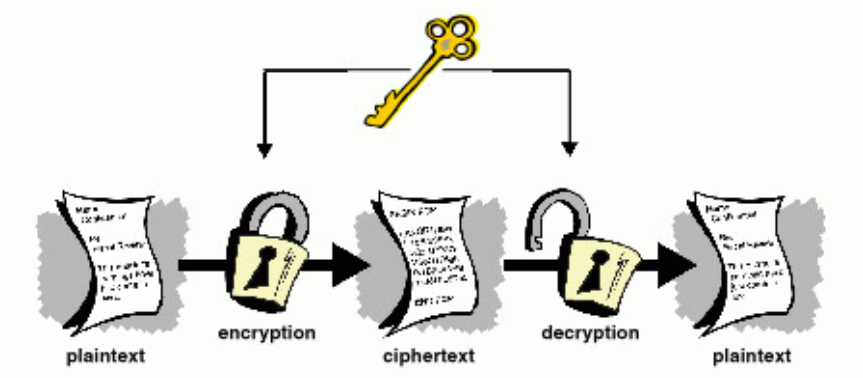


Figure 3.3: SYMMETRIC ENCRYPTION

the whole system fails and no information transmitted is secure anymore. In a symmetric key scheme the sender and receiver have to first agree on using a specific unique key for encryption. This phase is called key establishment phase which should be done over a secured medium of communication. In a network of N nodes, number of possible sender-receiver pairs can be N(N-1)/2, requiring a unique key for each pair. This number grows rapidly with increase in number of nodes in the network. Hence, requiring a very large number of keys for secure communication in the network making it very poor for scalibility. All these factors make symmetric encryption schemes vulnerable to linear cryptanalysis [36], known-plaintext attacks, chosen plaintext attacks, differential cryptanalysis, etc.

3.3.2 Asymmetric-Key Encryption

Also known as Public-Key Encryption, asymmetric encryption uses two keys. One known as the public key which is published publically and the second secret key known as the private key which is only known by the person it belongs to. Asymmetric encryption was the landmark invention in the field of cryptography. Most of the well known robust encryption schemes even today are based on asymmetric keys. As shown in Figure 2 public and private keys are used for encryption and decryption respectively. This is made possible by using sophisticated complex mathematical structures which are discussed in detail further. But, as a result of higher complexity asymmetric keys require significantly more computing power as compared to symmetric encryption due to their complexity. Asymmetric encryption does have a major advantage over symmetric encryption, possessing better scalability as number of required keys grows only linearly with the size of the network. A majority of modern schemes generally employ a hybrid approach where a symmetric key is established for communication during the key establishment phase using asymmetric channel. Once asymmetric encryption facilitates the communicating nodes with a secure channel for key sharing then further communication can take place over a secure channel using only the symmetric key which has lower overheads.

3.3.3 Stream Cipher and Block Cipher

STREAM CIPHER: When using a stream cipher, encryption or decryption is done one bit or character at a time hence the name [37]. The plaintext stream is hashed together using the key stream using the

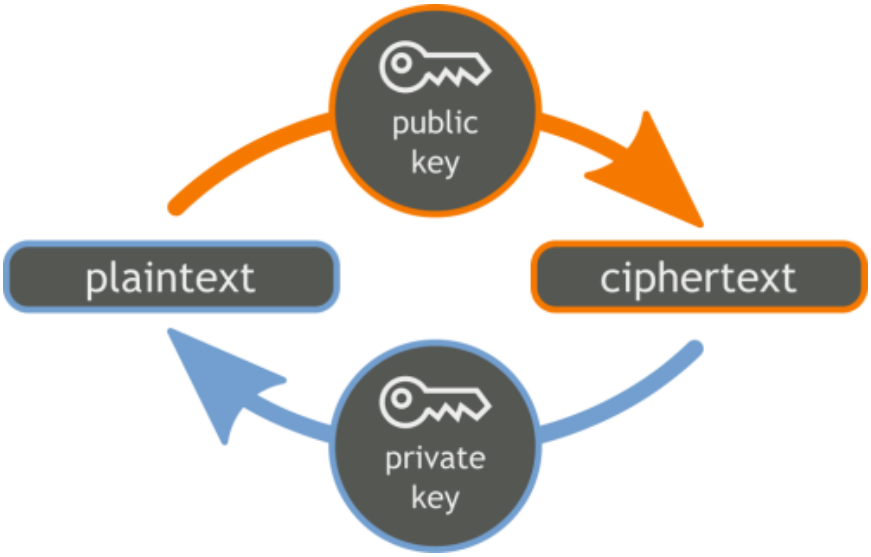


Figure 3.4: ASYMMETRIC ENCRYPTION

encryption algorithm to output a ciphertext stream. This function can be as simple as a XOR operation. Now the key stream can be formed in several ways either use a predetermined array of keys or generate one key at a time using an algorithm at a required required frequency. When designing such a key generation algorithm, dependencies of key values on plaintext, ciphertext or earlier used keys can be added to make the scheme robust. Figure 3 shows the concept behind a stream cipher.It can be observed that both source and destination should have the same key stream and the index needs to be synchronized for the process of encryption or decryption. Stream cipher is also known as state cipher as encryption of each character is dependent on the current state of the cipher. It is intuitive that in case the receiver doesnt have the correct state of the key stream even though it possesses the correct key stream it might not be able to decipher the message [38].

BLOCK CIPHER: Whereas, in a Block Cipher, the plaintext of size n characters is broken into equal m sized blocks. Each individual block of plaintext is encrypted with a key of size k bits. Figure 4 shows the basic idea behind block ciphers. It can be observed that in a block cipher in its simplest form, if the block size m=1, works like a stream cipher. However, when used in application block cipher has several other differences to a stream cipher making it much more versatile. Block cipher is the foundation of most of the cryptographic algorithms of recent times [39].

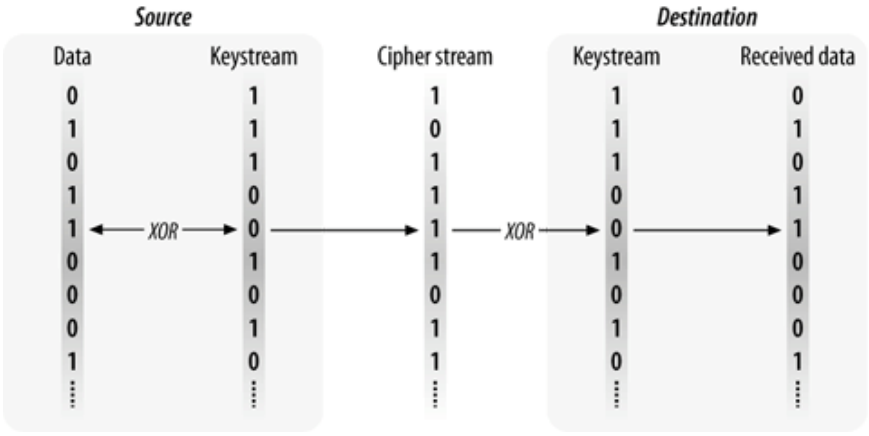


Figure 3.5: AN EXAMPLE OF STREAM CIPHER

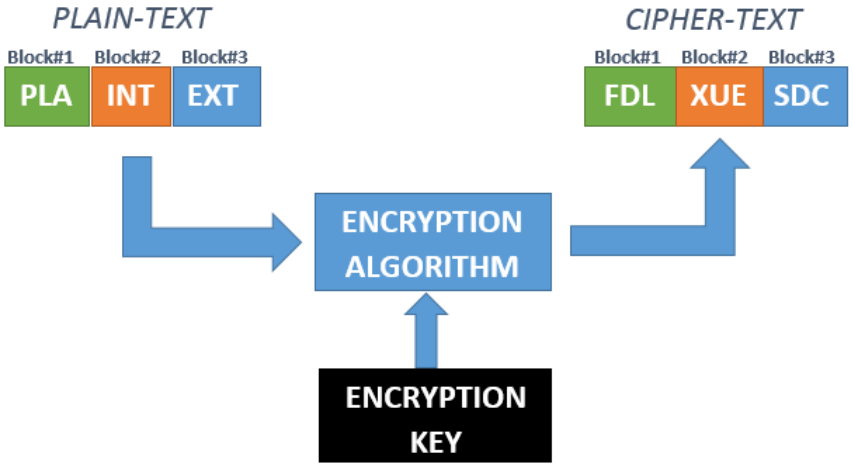


Figure 3.6: AN EXAMPLE OF BLOCK CIPHER

3.4 Confusion and Diffusion

Confusion and Diffusion are the two quantifiers for the efficiency of a good Cryptographic system. These were first introduced by Claude Shannon in 1945 [40]. To create confusion each character of the ciphertext should depend on several different parts of the key in different ways. Meaning there exists an involved and complex relationship between plaintext, key, and ciphertext. An eavesdropper should not be able to guess a deterministic relationship that can predict the effect of changing one chatracter in plaintext has on the encrypted ciphertext. The major goal of confusion is to make it impossible to generate the key even if the eavesdropper has a large number of plaintext and ciphertext pairs that were created by using the same key. Diffusion means a very slight change in the input which can be expressed as change in one bit of plaintext should have a very large impact on the ciphertext. Further, since encryption is an invertible process this should also be true in the reverse direction. A slight change in ciphertext should also effect in a huge change in the plaintext produced when decrypted. As quoted by Claude Shannon ”diffusion refers to dissipating the statistical structure of plaintext over the bulk of ciphertext”. In practice both confusion and diffusion properties are achieved by using bit substitution and permutation of the order of bits respectively. A Substitution-permutation network is a very good example of such a structure that provides robust encryption by iteratively performing substitution and permutation in a specific order. Shannon also describes this in terms of information entropy, the lower the amount of information that is divulged related to the plaintext by a data packet sniffed by an eavesdropper the higher is the entropy of the packet. Higher entropy is desired from a good security scheme which is achieved by maximizing confusion and diffusion. For a good cryptosystem it means it would require a very large number of packets by an adversary to reverse engineer it [41].

3.5 Malleability

A cryptographic algorithm posseses malleability [42] if an encrypted known ciphertext when replaced by another ciphertext (chosen specifically to attack) by an adversary followed by decryption using the algorithm gives meaningful result. This meaningful result could be a function of original plaintext hence it is related or close to the original plaintext. In this case even though the original plaintext is not revealed some parts

of information is leaked which can be exploited by a malicious node to intelligently modify the original message in the data stream. That is, for a given message M and the corresponding ciphertext C = Encrypt(M), it is possible to generate C = F(C) so that Decrypt(C) = P = F(P) with arbitrary, but known, functions F and F. Generally speaking, malleability is considered a flaw in a cryptographic system and can be used to define weakness of a particular block/stream encryption scheme. However, in some cases this is a desired property from a cryptosystem which is known as Homomorphic encryption. Homomorphic encryption schemes are purpose built to be malleable. This property allows computations to be performed on data without decrypting it. Which empowers use of homomorphic systems in the field of cloud computing to guaranty the confidentiality of processed data. For example, encrypted search terms can be searched in an encrypted database without having to decrypt the whole database and in-turn creating a vulnerability. Homomorphic algorithms have also been deployed for private information retrieval, collision-resistant hash functions, to perform computations securely and in secure electronic voting systems.

3.6 Substitution-Permutation Network

To further our understanding of block ciphers we must understand a Substitution-permutation network (SPN) which is a sequence of chained mathematical operations used in block cipher algorithms. Such a network accepts a block of the plaintext and the encryption key as input, and applies several iterations known as rounds of substitution boxes (S-boxes) and permutation boxes (P-boxes) to generate the ciphertext block. Now several combinations of S and P boxes can be generated for each round. Figure 5 shows how they are used in a SPN. The S-boxes and P-boxes converts blocks of input bits into output bits. This operation can be as simple as a XOR operation followed by bitwise rotation. A different round key is used in each round to encrypt the input bits. Decryption is done by using the inverses of the S-boxes and P-boxes and applying the round keys in reversed order.

Substitution Box: An S-box works like a lookup table, when given an input of m bits it returns n bits as an output. Generally speaking, it is not necessary for m to be equal to n. This substitution should have the property of one to one in order for the S-box to be invertible which is essential for decryption. This substitution step is essential to provide obscurity to the key and the resultant cipher hence providing the property of confusion. A good S-box is supposed to possess a quality known as avalanche effect. This

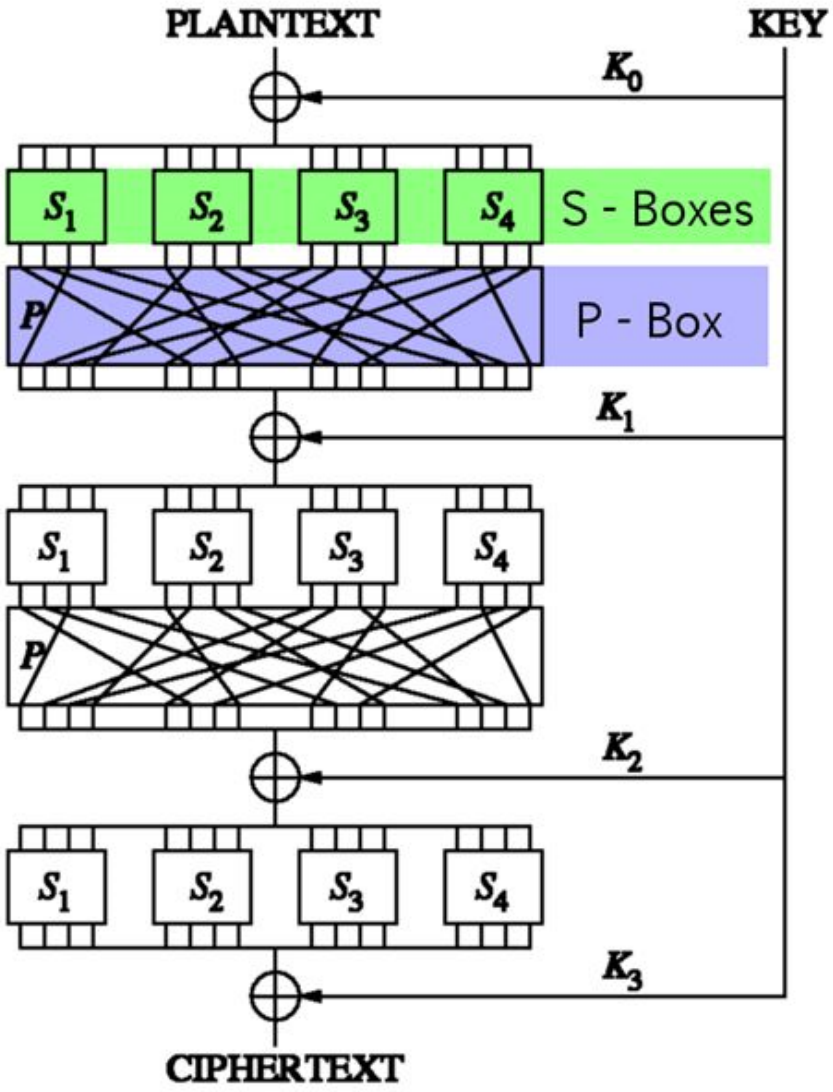


Figure 3.7: A SUBSTITUTION-PERMUTATION NETWORK (SPN)

means that a very small change in the input for the S-box greatly changes the output given. Under the strict avalanche criterion when a single input bit is changed to the S-box the probability of each output bit changing should be 50%. In simpler terms it is desired from a good S-box that changing even 1-bit of the input should change atleast half of the output bits. Permutation Box: A P-box is basically a shuffling of all the input bits coming from different sources as in our case it will be from different S-boxes and then sending them to next set of S-boxes as shown in the SPN network figure above. A desired property of a good P-box is that it divides the bits coming from one particular S-box to as many different S-boxes possible in the next round. To enhance security, the output of the P-box is hashed together with the round key using some operation which can be as simple as XOR. A P-box could be imagined as a transposition cipher, whereas, an S-box could be perceived as a substitution cipher. Individually when used by itself, they do not provide much security to the cipher but when used in combination together as shown in an SPN they provide pretty high level of security.

3.7 Encryption Standards

DATA ENCRYPTION STANDARD (DES): Even though DES is deemed obsolete now but it has inspired several successful cryptographic schemes. DES is a symmetric key algorithm with 56-bit key size. In DES a unique symmetric key is used to encode and decode a message, so both the source and the receiver must securely establish a shared private key among each other. Now, DES has been superseded by the more secure Advanced Encryption Standard (AES) algorithm as it is considered to be insecure for many applications. The advent of Data Encryption Standard opened up the field of cryptography and the development of better encryption algorithms. It was invented at IBM during early 70s but was kept open to public unlike its predecessors that were kept private by military and government intelligence organizations. This ensured anyone interested in security could study how the algorithm worked and try to crack it [43]. DES is a typical block cipher which takes a fixed-length string of plaintext bits and converts it through a sequence of complex operations into a ciphertext, which is a string of the same length as the plaintext. DES uses 64-bit block size hence the original plaintext is broken into 64-bit blocks. A shared private 64-bit key is also hashed during this transformation to ensure security. Even though the key has a length of 64-bits only 56-bits are used for the actual key. Rest of the eight bits are used for checking parity. The DES modified and used by NSA had

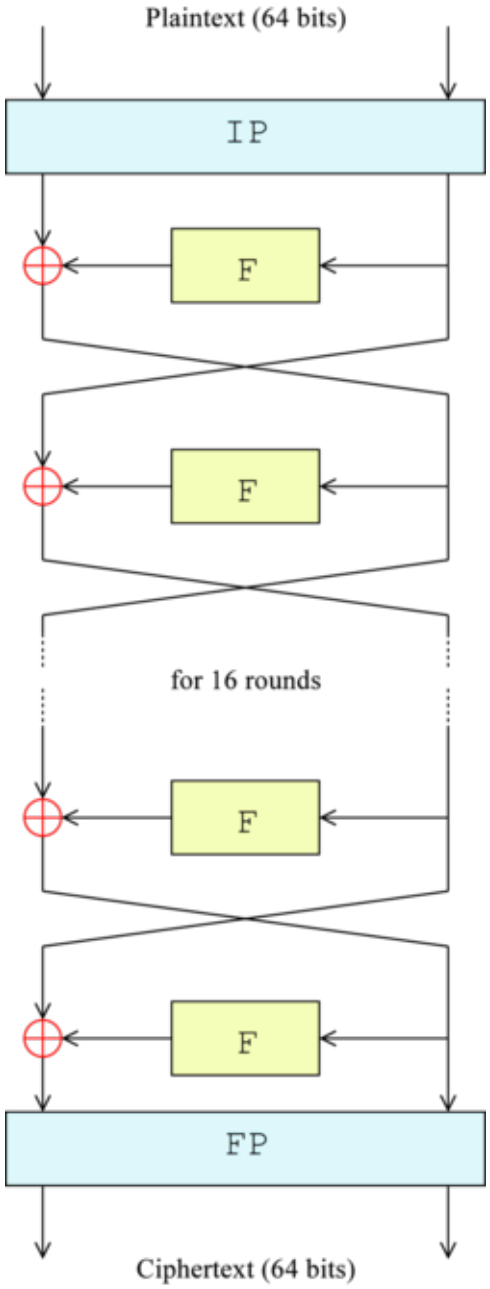


Figure 3.8: OVERALL STRUCTURE OF DES

a structure of S-boxes the complete details of which are still kept a secret. This secrecy led lot of people to believe that NSA had built in a backdoor for itself in DES [44].

ADVANCED ENCRYPTION STANDARD (AES): In the year 2001 DES was replaced by much more secure standard called AES. It uses a SPN network for encryption unlike DES which uses a Feistal network. AES is also a symmetric key algorithm hence same key is used for encoding and decoding. AES is a variant of Rijndael algorithm which has a fixed block size of 128 bits [45], and a key size of 128, 192, or 256 bits. Further, AES is found to be very fast in hardware as well as software. The decryption algorithm follows a similar path as the encryption algorithm, only replacing the steps by their inverses. The round keys of have to be used in the reverse order during decryption. Brute force attack or slightly improved versions of a brute force attack are the only known successful attacks for AES. Although none of these known attacks are computationally feasible in realtime to date.

RC4: RC4 (ARC-Four) was the most widely used stream cipher [46]. RC4 was designed by Ron Rivest of RSA Security in 1987. It was used with secure socket layer (SSL), which was used to secure private information and money transfers over the Internet. Furthermore, it is used in WEP (Wired Equivalent Privacy) which is liable for securing wireless data. RC4 showed that is secure enough for certain systems, but it was found out that it does not offer that level of security to wireless communications, making it fall short for many security standards. Remarkable for its simplicity and speed in software, multiple vulnerabilities have been discovered in RC4 [47], rendering it insecure. Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. TLS is the successor to the Secure Sockets Layer (SSL). Several organizations and companies like Microsoft and IETF have recommended not to use RC4 with TLS due to security concerns [48].

3.8 Wireless Standards

WIRED EQUIVALENT PRIVACY (WEP): WEP is a standard network protocol that augments security to 802.11 wireless networks while working at the data link layer [49]. The idea behind WEP was to provide the similar level of security on a wireless link comparable to a wired network. Nevertheless, the fundamental technology behind WEP has been confirmed to be pretty insecure compared to newer protocols like WPA. WEP exploits a data encryption system named RC4 with a mixture of user- and system-generated key

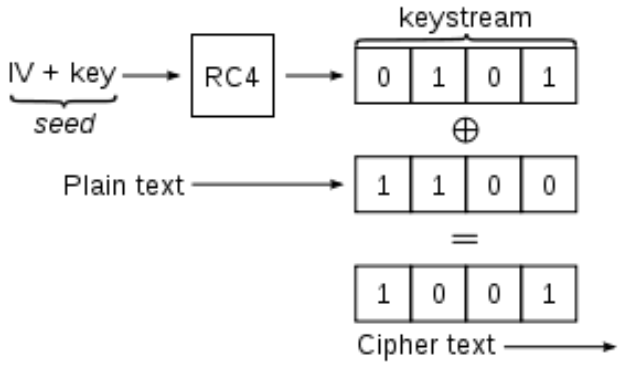


Figure 3.9: WEP ENCRYPTION

values. The original applications of WEP used encryption keys of length 40 bits and 24 additional bits of initialization vector (IV) to form the RC4 key (64 bits in total). In an effort to escalate security, these encryption techniques were modified to accomodate longer keys of length 104-bit (128 bits of total data), 152-bit and 256-bit. In Shared Key authentication, the WEP key is used for authentication in a four-step challenge-response handshake [50]. In the first step client directs an authentication request to the Access Point, in response to which Access Point responses with a clear-text challenge. Then, the client encodes the challenge-text using the established WEP key and sends it back in another authentication request. Finally, the Access Point decrypts the message received. If this is found to be same as the challenge text, the Access Point sends back a positive response. After the authentication and association phase, the pre-established WEP key is also used for encoding the data frames using RC4.

WI-FI PROTECTED ACCESS (WPA): The Wi-Fi Alliance introduced WPA as an intermediate fix to take the place of WEP which had serious security concerns. Temporal Key Integrity Protocol (TKIP) was implemented for WPA under 802.11i standard [51, 52]. WEP used a 40-bit or 104-bit encryption key that was manually entered at the wireless access points and clients and was not changed. TKIP uses a new key for each data packet, it dynamically generates a new 128-bit key using the RC4 cipher for each packet and thus thwarts the types of attacks that rendered WEP insecure. WPA uses a message integrity check algorithm named Michael to verify the integrity of the packets. Michael provides a sufficiently strong data integrity guarantee for the packets and it is much stronger than a Cyclic Redundancy Check (CRC) which was used in WEP and later found to be weak. 802.11i (WPA2): WPA2 was introduced to replace WPA. It is even more robust than WPS as it supports CCMP (CTR mode with CBC-MAC Protocol [53]) instead of

TKIP which is an AES based encryption mode with stronger security. This was a compulsory requirement of WPA2 under the accepted guidelines of 802.11i by the Wi-Fi alliance [54].

3.9 Security Attacks

As stated earlier, the main difference among wired and wireless network is the medium used for data transmissions. The open air broadcast characteristic of a wireless network makes it easy for everybody to attack the network if not properly secured, due to the nonexistence of physical hurdles, where the range of wireless signal can be from 100meters to 1000meters. Lack of need for physical medium and easy setup helped the exponential growth of wireless networks which is another hurdle on augmenting the network security. A lot of times establishing network security can be time consuming or cost expensive which can be a deterrent for people. Lack of proper knowledge or education can also prevent people from having good network security. All these factors can lead to vulnerabilities and attacks which can be categorized in several different categories.

ACTIVE ATTACKS: MASQUERADING, REPLAY, MESSAGE MODIFICATION, DOS, ETC. An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data enroute to the target. Types of active attacks: In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized [55].

PASSIVE ATTACKS: EAVESDROPPING, TRAFFIC ANALYSIS It is a type of attack wherein adversaries listen in on packets that are in transit. Even though it seems the simplest kind of attack, passive eavesdropping can prove very dangerous over a period of time. When paired with advanced and aggressive probabilistic algorithms the data collected over time can help crack almost any encryption algorithm out there. For this very reason keys are desired to be dynamic in any good security scheme which should be renewed frequently, well before its integrity becomes questionable.

SIDE-CHANNEL ATTACKS In the year 1996, one of the best examples of a side-channel attack was discovered by a cryptographer named Paul Kocher, in which he measured electric power consumption of microprocessors. In a side-channel attack an attacker instead of using a brute force approach or targeting theoretical vulnerabilities of the cryptosystem algorithm information is gathered related to the physical implementation parameters. For example, parameters like amount of electric power being consumed by the

processor, runtime of the algorithm, electromagnetic emanation from a smartcard, etc. In Paul Kocher's attack he exploited the power consumption amounts of the microprocessor and plotting it on a curve he could deterministically identify which conditional branch was followed by the algorithm. Further, it has been found that if the identified conditional branch depends on a secret key, then a lot of information about the key is divulged. In another case similar side-channel attacks were able to completely hack smart cards, forcing the manufactures to withdraw their product and causing huge losses. Several popular security algorithms have been found to be prone to these attacks by losing the secret key to hackers and hence rendered useless. In his work of 96 Paul talks about timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems.

MAN IN THE MIDDLE ATTACK A man-in-the-middle attack is one in which a malicious user covertly captures and relays data packets among two users who trust they are connecting directly [56,57]. It's a form of eavesdropping but the entire communication is controlled by the man in the middle, who even has the capability to modify each data packet. Sometimes, referred to as a session hijacking attack, it is successful if the man in the middle can impersonate each user to the satisfaction of the other. This attack poses a serious threat to online security because it gives the attacker the capability to sniff and control sensitive information in real-time while pretending as a trusted user during all communications.

MODERN ATTACKS:

Adware: or advertising-supported software, is a software that automatically shows advertisements for marketing purposes and in turn generating money for the author. The ads can be in the user interface of the software or on a screen presented to the user during the installation.

Backdoor: A backdoor in a computer system or a cryptosystem is a technique of bypassing customary authentication, obtaining unauthorized remote access to a computer, or attaining access to plaintext while trying to stay concealed.

Bluejacking: is the distribution of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which usually holds a message in the name field (bluedating or bluechat) to another Bluetooth-enabled device by means of the OBEX protocol.

Bluesnarfing: is the unauthorized access of data from a wireless device over a Bluetooth connection, fre-

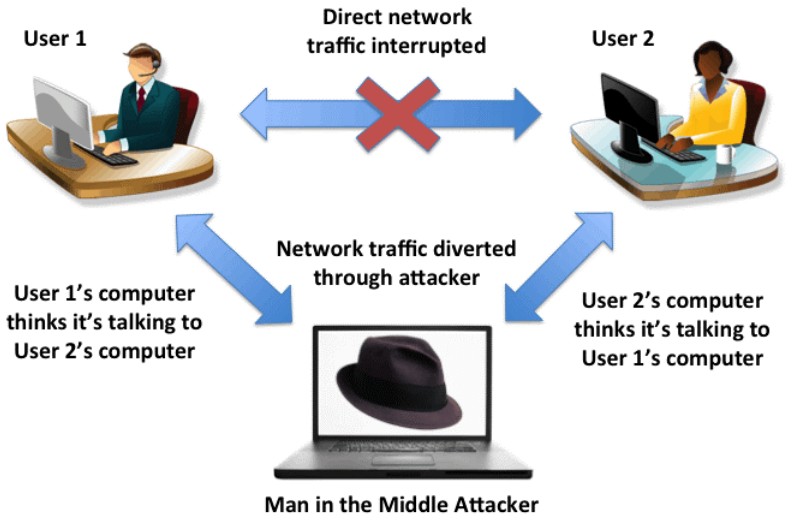


Figure 3.10: MAN-IN-THE-MIDDLE ATTACK

quently between phones, desktops, laptops, and PDAs.

Boot Sector Virus: A boot sector virus is a virus that infects the master boot record of a storage device, usually a hard drive but occasionally a CD. These can be sometimes very hard to remove.

Botnet: (zombie army) is a number of computers connected to the internet that, without the knowledge of the original owner, forward transmissions, which could be spam or viruses, to other computers on the Internet.

Browser Hijackers: is a form of unwanted software that changes a web browser's settings without a user's authorization, to insert annoying advertising into the user's browser. A browser hijacker may switch the existing home page, error page, or search page with its own.

Chain Letters: Chain letters are letters/emails that assure an unbelievable return in exchange for a very small effort. The simplest form of a chain letter contains a list of x people. You are supposed to send something to the top person on the list. Then you remove the top person on the list, sliding the second person into the top position, add yourself in the bottom position, make y copies of the letter, and mail them to your friends. The assurance is that you will ultimately receive x times y of something as an award.

Cookies: session hijacking, at times also known as cookie hijacking is the manipulation of a valid computer

session, sometimes also called a session key, to achieve unauthorized access to data or services in a computer system. Specifically, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server.

Crimeware: is intended to commit identity theft using social engineering or technical stealth in order to steal a computer user's financial accounts for the purpose of taking funds from those accounts or making unauthorized online purchases. On the other hand, crimeware may well steal confidential or sensitive corporate data. Crimeware signifies a rising problem in network security as many malicious code threats seek to steal confidential information.

DDoS: is a type of DOS attack where multiple hijacked internet devices, frequently infected with a Trojan, are exploited to target a single system triggering a Denial of Service (DoS) attack.

Dropper: A dropper is an executable file that drops a document to disk, opens it, and silently executes an attacker's payload in the background stealthily. Droppers can carry viruses, backdoors and other malicious scripts so they can be executed on the hijacked device.

Exploit: An exploit is a piece of software, a chunk of data, or a sequence of commands that exploit vulnerability or a bug in order to cause unintended or unanticipated behavior to occur on computer software, hardware. Such behavior often includes attacks like attaining control of a computer system, sanctioning privilege escalation, or a denial-of-service attack.

Fake AV or Scareware: is a Trojan that intentionally misrepresents the security status of a computer. These programs try to persuade the user to purchase security software in order to remove non-existent malware or security risks from the computer.

Keylogger: A keylogger is a type of surveillance spyware software that has the ability to record every keystroke made on the keyboard to a log file. A keylogger recorder can record instant messages, e-mail, and any information typed at any time using the keyboard. The log file created by the keylogger can then be sent to a specified receiver.

Mousetrapping: Mousetrapping is a procedure used by some malicious websites to keep visitors from leaving their website, either by launching an endless series of pop-up ads or by re-launching their website in a window that cannot be easily closed. Many websites that do this also employ browser hijackers to change the user's default homepage.

Obfuscated Spam: Obfuscated spam is email that has been disguised in an attempt to bypass or avoid detection by the anti-spam software. By obfuscating the key terms used by the anti-spam software to filter spam messages which can be achieved by inserting unnecessary spaces between the letters of key spam words.

Pharming: is a cyber attack planned to forward a website's traffic to another, fake site. Pharming can be conducted either by altering the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. It is a form of online fraud very similar to phishing as pharmers rely upon the same bogus websites and theft of confidential data.

Phishing: is the attempt to acquire sensitive info such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Spyware: is software that aims to gather information about a person or organization sneakily and that may send such information to another entity without the user's consent, or that takes control over a computer without the user's knowledge. Spyware is of four types: system monitors, trojans, adware, and tracking cookies.

SQL Injection: is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

Trojan: is any malicious computer program which misrepresents itself as useful, routine, or interesting in order to convince a victim to install it.

Virus: is a malware program that, when executed, reproduces by inserting copies of itself into other computer programs, data files, or the boot sector of the hard drive; when this duplication succeeds, the affected areas are then said to be ”infected”.

Wabbits: A Wabbit, Rabbit or Computer Bacterium is a type of self-replicating computer program. Unlike viruses, wabbits do not infect host programs or documents. Unlike worms, wabbits do not use network capabilities of computers to spread. Instead, a wabbit constantly duplicates itself on a local computer. Wabbits can be programmed to have malicious side effects.

Worms: A computer worm is a standalone computer malware that replicates itself in order to spread to

other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.

Linear cryptanalysis: is a general form of cryptanalysis based on finding affine approximations to the action of a cipher.

Chosen plaintext attacks: A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information which reduces the security of the encryption scheme.

Known-plaintext attacks: The known-plaintext attack (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books.

Differential cryptanalysis: Differential cryptanalysis is a form of an attack targeted mainly towards block ciphers. Stream ciphers and hash functions are found to be equally prone too. In the broadest sense, it is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformations, learning where the cryptosystem displays non-random behavior, and misusing such attributes to recover the secret key.

3.10 Security in WMAN (802.16)

The WMAN or WiMAX was introduced as the ”last mile” network bringing connectivity to far off remote areas. The 802.16 standard was accepted and released in Dec 2001. Which was after the serious security flaws in the 802.11 WEP security protocol were widely known and acknowledged. Although the designers of 802.16 security module were aware of security loop holes prevalent in 802.11 WEP design, they still had several shortcomings in the security design. Since the telecommunications standard, Data Over Cable Service Interface Specifications (DOCSIS) was known to solve the ”last mile” problem for cable communication, it was incorporated in the 802.16 standard. However, wired networks greatly differ from wireless ones, 802.16 fails to protect the 802.16 communication and has serious vulnerabilities [58].

Physical Layer Attacks: The 802.16 standard relies completely on MAC layer security and has no security provisions for the physical layer. Due to this vulnerability 802.16 network is highly prone to attacks

like radio jamming and an attacks named water torture in which the attacker sends a series of data packets to drain the victims battery charge. No Base Station Authentication: A major defect in the authentication process used by WiMAX's privacy and key management (PKM) protocol is the absence of base station (BS) or service provider authentication. All authentications are one way and the key is also generated by the BS and the user has to trust the BS not to be malicious. This makes WiMAX networks vulnerable to man-in-the-middle attacks, exposing users to numerous confidentiality and availability attacks. The 802.16e amendment augmented provision for the Extensible Authentication Protocol (EAP) to WiMAX networks. However, EAP protocol provision is currently optional for service providers.

PKM Authorization drawbacks: Insufficient key length and flawed use of cipher modes providing weak security. WiMAX uses DES-CBC cipher with 56-bit key length which necessitates an unpredictable initialization vector to initialize CBC mode. TEK uses 3DES encryption, but uses it in ECB mode which has vulnerabilities.

Lack of Integrity Protection: Since the SA (Security Associations) initialization vector is constant and public for its TEK. Additionally, the PHY synchronization field is extremely repetitive and predictable and the MPDU initialization vector is also predictable. IEEE 802.16 fails to provide data authenticity. Small KeyID for AK and TEK: AK-ID is only 4-bit long, where TEK-ID is only 2-bit long. This creates the chance of reusing keys without detection. Due to these major flaws 802.16 protocol, it is known to be highly prone to the following attacks:

1. Rouge Base Station
2. DoS (Denial of Service) Attacks
3. Data Link-Layer attacks
4. Application Layer attacks
5. Physical Layer attacks
6. Privacy Sub-Layer attacks
7. Identity Theft
8. Water Torture

9. Black hat attacks

Due to the obvious vulnerabilities in PKM a newer and better version PKMv2 was introduced. PKMv2 introduces a solution to mutual authentication between BS and SS. It also provides a key hierarchy structure for AK derivation. Availability of two authorization modes RSA and EAP. AK is derived from PAK in RSA mode and PMK in EAP mode.

3.11 Cloud Security

Cloud computing provides users and organizations with numerous capabilities to store and process their large amount of data in third-party data centers. Organizations use the Cloud in a range of diverse service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community) [59]. There are many security issues/concerns linked with cloud computing but these issues fall into two general categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The accountability goes both ways, however, the service providers have a greater responsibility to ensure that their infrastructure is secure and that clients data and applications are secure at all times while the end user must take measures to strengthen their applications by using strong passwords and authentication methods [60].

Cloud data is stored in huge servers that are purpose built and stored in large secure physical locations know as data centers. When an organization stores data over the cloud they lose the physical control over the location. Hence, it is of utmost importance to secure the physical locations of data centers. It has been learned from recent data center attacks that most of them were conducted with the help of an inside attacker. Subsequently, it is very important to conduct extensive background checks before hiring employees at the data center [61].

Clouds serve multiple clients sometimes in the same domain handling sensitive consumer data. It is similar like a bank safety deposit box. Just like the banks cloud service providers need to protect the stored data not only from outside attackers but also preventing one customer's data to be accessed by other customers unless authorized for such an access by the original owner of the data [62]. On top of big data

manipulation algorithms cloud providers need to deploy robust protocols for logical storage segregation. This means access rights and rules should be strictly enforced.

The broad use of virtualization in employing cloud server infrastructure introduces novel security apprehensions for customers or users of a public cloud service. Virtualization modifies the connection between the Operating System and underlying hardware be it computing, storage or even networking. This presents an additional layer of virtualization that itself must be properly configured, managed and secured. Major concern with virtualization is that it is a logical implementation and not physical hence bugs or loopholes can be disastrous if exploited [62]. An attacker can exploit such a loophole to gain administrator access to the cloud which gives full access and control over the cloud bypassing the virtualization layer. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole data center to go down or be reconfigured by an attacker.

Cloud security protocol is effective only if the robust security implementations are enforced [63]. A good cloud security architecture should identify the issues that can arise with security management. The security management addresses these issues with security controls. These controls are put in place to protect any weaknesses in the system and reduce the effect of an attack. Further, if such an attack is detected it should be dealt with immediately. Although there are many types of controls for a cloud security architecture, they can be categorized in one of the following categories:

Deterrent controls: These controls are envisioned to diminish attacks on a cloud system. Much like a warning sign on a fence or a private property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for the wrongdoer. This type of control can be considered a subset of preventive controls.

Preventive controls: fortify the cloud system against attacks, by an effort to minimize if not completely eliminating vulnerabilities and weaknesses present in the system. Strict policies for authentication of cloud users, for example, makes it less probable that unauthorized users can access the cloud, and more probable that cloud users are positively identified.

Detective controls: Detective controls are intended to detect and combat appropriately to any suspicious activity that occur. In the event of an attack, a detective control will warn the preventative or corrective controls to address the issue immediately. System and network security monitoring, including intrusion

detection and prevention measures, are normally employed to detect attacks on cloud systems and the supporting communications infrastructure.

Corrective controls: Corrective controls minimize the negative impact of an incident, typically by controlling the damage. They come into action while or immediately after an incident. Restoring cloud system backups in order to reconstruct a compromised system is an example of a corrective control.

3.12 Privacy

Privacy is a very important issue to be dealt with in any computer network, specifically the location privacy [64]. In several cases, it is very critical to hide the location of a client in the network as there could be a physical threat or a threat of losing sensitive information to an adversary. For example, in most cases, a node would not like it to be disclosed that it is the one in the network initiating a sensitive bank transaction. Since most of the connections in a wireless network are over wireless channels which can easily be sniffed and vulnerable to packet sniffing attacks. In this way the adversary works in a passive way by just sniffing the data being transferred over a wireless connection. This information can be collected and be used to crack the transaction keys by performing statistical analysis. In this case, the biggest threat comes in the form of a global attacker which has access to all the ongoing wireless connections and keeps collecting data packets on them to analyze them to get information like keys, etc., in order for a future active attack. An active global attacker [65] can be even more dangerous as an active global active attacker not only sniffs packets being transmitted globally but it also devises dynamic methods or algorithms in order to identify the targeted node initiating the sensitive communication by using data like transmission event duration, time taken by the packet to traverse from source to destination, packet size etc. Hence, it is very important to come up with privacy schemes to keep the client nodes anonymous in a network.

3.12.1 The Onion Routing (TOR)

For a computer network, Onion Routing was invented by Michael G. Reed, Paul F. Syverson, and David M. Goldschlag to provide anonymity. In this scheme, the path is pre-computed at the source and the data packet is encrypted in multiple layers with the public key of the forwarding node along the path to destination in a sequential order and each node removes their layer of encryption after receiving the packet and forward

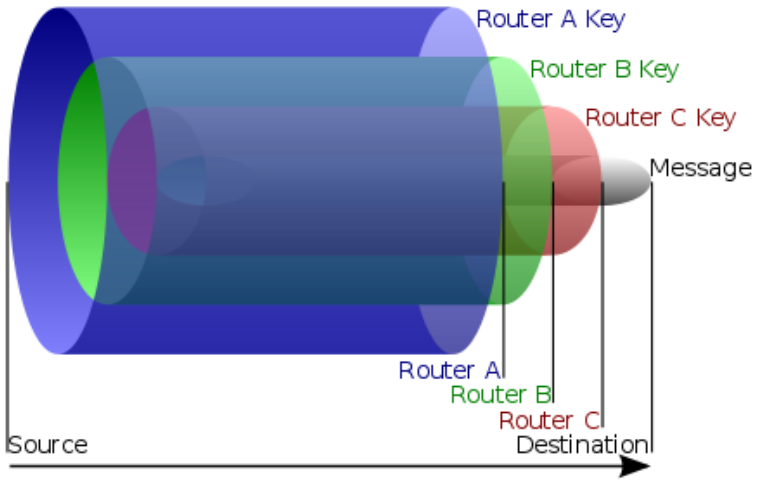


Figure 3.11: AN ONION PACKET

the remaining packet called the onion to the next hop and finally the decrypted data with all the layers of encryption removed is received by the destination. Using this approach, each node is only aware of the previous or next hop node which ensures anonymity of the source and the destination [66].

The list of nodes is maintained by a directory node. Directory node shares this list with users of the network. The path and its members are always computed by the source. Hence, no node in the network knows its location in the chain except the exit node which is the final node in the chain. When the chain of communication route is established, the source can send data over the Internet anonymously. When the destination of the data sends data back, the intermediary nodes continue the same link back to the source, with data again encrypted in layers, but in reverse such that the final node this time removes the first layer of encryption and the first node removes the last layer of encryption before sending the data, for example a web page, to the source.

3.13 Thoughts on Security

3.13.1 Best Practices

Careful planning and precautions can protect against majority of the security threats. Following are some of the most important precautionary steps an individual can take to protect themselves:

SECURITY SOFTWARE: This is one of the most important preventive actions that can save from an attack. Modern security softwares come in different flavors like firewalls, antivirus protection, email-protection, malware-protection, web-protection, etc. Generally, its a good idea to get a comprehensive suite from a reputable merchant like Norton, Mcafee, etc. These softwares are always running in the background and monitor any suspicious activity. Whenever any illegal activity is observed the suspected file is blocked and quaranteened and the user is asked for permission to permanently disinfect by deletion.

PRINCIPLE OF LEAST PRIVILEGE (PoLP) [67]: Administrator access should be strictly used on need only basis. Account privileges of all users should be closely monitored, people who are not authorized should not be given admin rights. User account with limited access/rights should be used for basic daily use.

KEEPING SOFTWARES AND OPERATING SYSTEM CURRENT: Regular update checks should be performed to keep the OS and softwares state current. Specifically, it is very important to keep antivirus definition files updated to latest version. These files make sure the antivirus software is fully equipped to detect and thwart any new and recent attacks discovered. Softwares can be updated by applying the latest service packs and patches. It is also very important to verify the source of these updates by verifying their digital certificates before installation.

CREATING SYSTEM BACKUP/RESTORE POINTS: Even after taking all the previous steps a system still might get infected which sometimes can lead to losing all the data on the system. It is a very good idea to keep multiple backups of data which can save a lot of frustration. In case of an operating system crash, hardware failure, or virus attack the system can be recovered to last known stable state easily by using the backup file.

ADDITIONAL SUGGESTED PRECAUTIONS:

1. Avoid opening email attachments from unknown people.

2. Deploy encryption whenever it is available.

3. Do not click random links.

4. Do not download unfamiliar software off the Internet.

5. Do not forward virus hoaxes or chain mail.

6. Log out or lock computer when not in use.

7. Never share passwords or passphrases.

8. Remove/Uninstall programs or services not needed.

9. Restrict/Disable remote access.

10. Secure home network with a strong password.

3.14 Recent Proposals

Internet of Things (IoT) is the biggest new development in the field of wireless networks this year [68]. As the name implies its the network of physical objects embedded with electronic hardware and software along with network capabilities. In IoT each entity or ”thing” is uniquely distinguishable through its embedded computing hardware but is able to function within the existing Internet infrastructure. The Internet of Things empowers objects to be controlled remotely and collect data from sensors utilizing existing network infrastructure, creating prospects deeper integration between the physical world and the digital cyber world, and subsequently promising enhanced efficiency, reliability, accuracy and financial gains.

IoT guarantees the automation of pretty much every field of life by interconnecting virtually everything. IoT gives the capability of converting every day to day mundane object into smart devices and communicating with each other. This helps deployment of advanced applications like Smart Grid and taking it to the next level to create a smart city. At the advent of Internet and other groundbreaking networking inventions the biggest question was Security and Privacy. Similarly, IoT raises very similar questions, but this time the problem is literally huge. IoT proposes to include 20 billion devices by the year 2020. This brings us to the issue of capturing, manipulating and securing a humongous of data. This data set is so big that there is a whole new field of study for handling extremely large data sets known as Big Data [69]. Currently the internet community doesnt really know for sure how to handle security in such a complex domain. So for now IoT has been rolled out with very basic security protocols at hand. Several scholars have expressed serious concerns related to security and privacy issues in IoT and makes them wary of this new age ubiquitous computing revolution as this would literally effect the life of everyone present everywhere. People are also

concerned about issues related to environmental impact and effect of IoT on younger people and children. Not only does IoT promises to bring remote access and control via internet to every step of our daily life, it also brings issues like cyber attacks and cyber bullying right into our bedrooms. This means security is the biggest issue related to IoT. Advanced algorithms need to be developed to guarantee security and privacy with low overheads since most of the IoT things have low resources.

3.15 Summary

In this chapter we discussed various aspects of network security. It is a very broad field that requires extensive in depth study even for a basic understanding of concepts related to it. With time networking technologies keep evolving providing faster connectivity to even the farthest places on earth and beyond. This keeps presenting new challenges for the network security designers. Newer hybrid networks like the Mesh, Smart Grid, IoT, WiMax, etc. create unlimited possibilities while creating new security challenges. There would always be a need for newer, better, smarter and faster security architectures.

Chapter 4

Network Coding with Enhanced Onion Routing

*This chapter was also published as an article in the International Journal of Computer Networks and Communications [70].

4.1 Wireless Mesh Network (WMN)

A WMN consists of Internet Gateways (IGWs), Mesh Routers (MRs) and Mesh Clients (MCs). MCs are served by MRs which are connected together using wireless links in an ad hoc mode and constitute as the backbone of a WMN. Some MRs act as IGWs to provide access to the Internet and makes the network very cost-effective. MRs could be of different types, such as Wi-Fi, WiMax routers etc. and could have different interfaces. This leads to two levels of hierarchy, MRs at higher level with many different wireless interfaces, and MCs constitute the lower level and are served by MRs using separate interfaces with the presence of few IGWs wired to the Internet, the cost is low, while easy to expand using additional MRs. In this way, it is easy to expand WMNs, especially in the sparsely populated areas and makes them easily scalable. Another very important application of a WMN is to provide different medium of wireless access. Hence, WMN can be said to be dynamically self-organized and auto-healing.

Versatilities of a WMN is especially important in an open wireless medium where MRs are owned by

different independent entities. Such networks mainly rely on an ad-hoc packet transmission mechanism as MRs forward along the route from source to destination acting as relay nodes. Several possible misbehaviors could be identified as impersonations, packet sniffing, selfish behavior etc. There are several works to date focusing on identifying and rectifying many such misbehavior [71]. In this paper we introduce a scheme to utilize the concept of network coding that maximizes efficiency of the WMN with low overheads and high level of security and anonymity by using encryption at each link along the path.

4.1.1 Background and Related Work

Security

The field of Wireless Mesh Network is still in its early stage and hence security is open. The protocol for WMNs are still to be developed. In a WMN the MRs are pretty static while MCs move around at different speed and get connected to MRs in their vicinity. In the year 2006 [72] described various attacks like sinkhole and wormhole attacks and also look into numerous vulnerabilities of a WMN. Many ideas have been proposed to combat these attacks using different techniques, including shared private keys and public-private key pairs. RSA-based public key cryptography is one example. The Asymmetric key system are complex for authentication and data communication as it is computationally very expensive. Hence, to maintain low energy consumption in MCs with limited energy sources, we want our scheme to be light weighted.

Use of symmetric keys seems to be an attractive option. In [73], Eschenauer and Gligor proposed a random key distribution scheme such that each device randomly selects a group of keys from a large pool of P keys. A major disadvantage of this scheme is that if the number of keys given is small, most of the devices are sparsely connected and are not capable of communicating with each other as they may not have even one key in common. Hence, lots of devices remain disconnected. When the number of keys given is large, the scheme becomes susceptible to a device capture attack. This could force a large amount of secret to be lost, thereby compromising a large portion of the network. Furthermore, each pair of devices to have a shared symmetric key each device must be given at least n-1 common keys to spawn capability of complete connectivity. Chan et al. [74], revised the Eschenauers and Gligors model by having at least q (where $q>1$) keys in common between two adjacent wireless devices instead of just one common key, so

that they can have a secure wireless link between them. They call their scheme to be q-composite random key pre distribution scheme. This is one way to enhance the network resilience against any device capture attack. Blom also introduced a symmetric key generation scheme (SKGS) [75], where a pair of devices can independently generate a common key between them by exchanging a small amount of secret information. However there could be dependencies between the keys in this particular approach and a number of users have to collaborate in resolving the ambiguity of unknown keys. This makes this scheme vulnerable to device capture attack when the number of captured devices exceed a given threshold value which is directly proportional to the amount of secret divulged. In [76], Blundo et al. proposed a secure key distribution scheme for systems where a device may leave or enter the network dynamically, by that constantly changing the network topology. Therefore, they proposed a t-degree bivariate symmetric polynomial pre distribution scheme. Such a strategy is equally pertinent to any hierarchical networks. Usually, the communicating wireless devices swap polynomials by substituting the variables with their respective IDs. It is possible to compute a common secret key between them due to the symmetric attribute of the polynomial. This scheme is called as k-secure where k pertains to the degree of the symmetric polynomial.

Yi Cheng et al. [77] have presented a pair wise key establishment mechanism (EPKEM) by generating keys and arranging them in a matrix so that a common shared key between any communicating nodes can be achieved. Each user is allocated a row and a column of keys to form $(2m-1)$ set of keys. The selected $(2m-1)$ elements from the matrix are then loaded into each device along with the (i,j) coordinates of the respective elements to form its key ring and then they are deployed randomly. In this scheme, two devices discover a common key between them by broadcasting their respective IDs while the indices (i,j) of keys are exchanged that were used at the time of key pre-distribution. This scheme drastically reduces the number of keys that are needed to be pre-stored on the devices during the deployment phase, while assuring at least two common keys among a pair of any adjacent devices.

Preliminaries: Polynomial Based Scheme

In [78], we proposed a bivariate polynomial function based security scheme that is highly scalable at a very low cost. In this scheme, we introduced a novel scheme to allow a secured authenticated connection between

any two entities in a WMN. The two adjacent nodes can be an IGW, one MR or any MC. The crucial step of this scheme is to furnish each node a set of bivariate polynomials during the pre-deployment phase by the central authority. Once deployed, this secret polynomial are used to independently generate symmetric secure key and once achieved, we say that the two nodes have an generated an authenticated association with each other. It should be noted that during the pre-deployment phase, three different sets are given to each node as follows:

1. A shared key K for initial secure information exchange.
2. A set of Bivariate Polynomial Functions $F_{i,j,k}(x, y)$(where $0 \leq i < l, 0 \leq j < m, 0 \leq k < m$) picked randomly from a 3D matrix of polynomials and the indices of the selected polynomial functions.
3. A function H( ) known as the hash function to compute the shared key from the values received by the bivariate polynomial functions.

This three dimensional matrix has been adapted from Yi Cheng's scheme in [77] and [79] by randomly selecting the polynomials. From the get go each device undergoes three stages of

1. Acquiring Secrets.
2. Authenticated Association.
3. Pair-wise secure channel establishment from a Mesh Client to an IGW or the AAA server.

A standard Bivariate Polynomial distribution is construed as follows:

$$F_{i,j,k}(x, y) = \Sigma_{rs=0}^{p} a_{rs} x^r y^s$$

Where the coefficients a_{rs} are randomly selected over a Finite Field $Gf(X)$ where X is a very large prime number and i, j, k are the indices for the position of the polynomial in the three-dimensional matrix used at pre-deployment and p is the degree of the function $F_{i,j,k}$ (x,y). A Polynomial Function is called a Bivariate Polynomial if it satisfies the following elementary prerequisite:

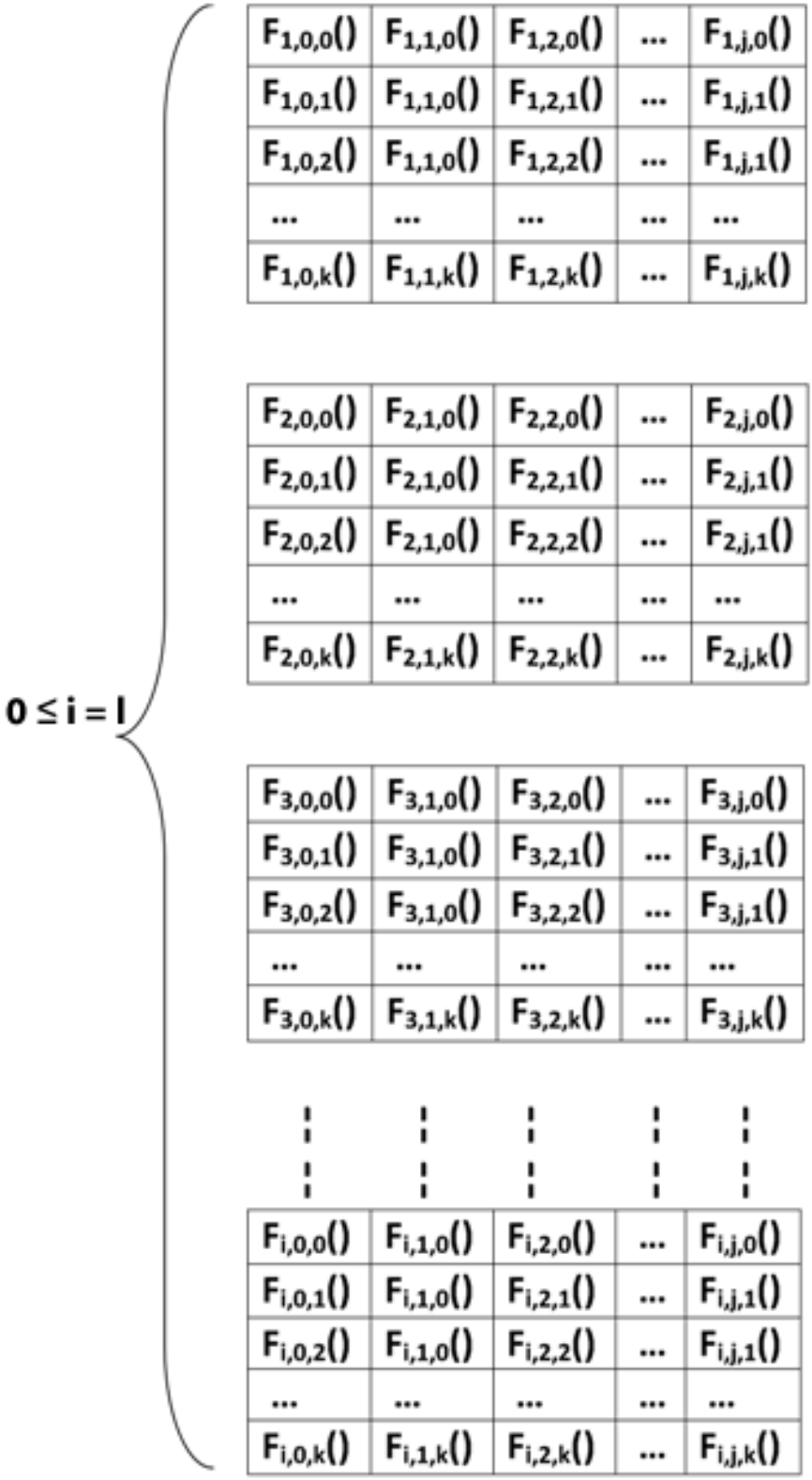


Figure 4.1: A three dimensional matix of bivariate polynomials

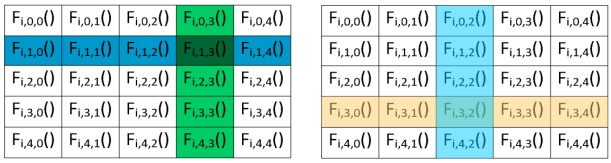
$F_{i,0,0}()$	$F_{i,0,1}()$	$F_{i,0,2}()$	$F_{i,0,3}()$	$F_{i,0,4}()$
$F_{i,1,0}()$	$F_{i,1,1}()$	$F_{i,1,2}()$	$F_{i,1,3}()$	$F_{i,1,4}()$
$F_{i,2,0}()$	$F_{i,2,1}()$	$F_{i,2,2}()$	$F_{i,2,3}()$	$F_{i,2,4}()$
$F_{i,3,0}()$	$F_{i,3,1}()$	$F_{i,3,2}()$	$F_{i,3,3}()$	$F_{i,3,4}()$
$F_{i,4,0}()$	$F_{i,4,1}()$	$F_{i,4,2}()$	$F_{i,4,3}()$	$F_{i,4,4}()$

Figure 4.2: A $M \times M$ Matrix

$$F_{i,j,k}(x,y) = F_{i,j,k}(y,x)$$

A three dimensional matrix is conceived containing a bivariate polynomial at each unit position of this matrix. The bivariate polynomials selected to populate this three dimensional matrix are randomly chosen from a large pool of such possible bivariate polynomials. For explicit understanding we can contemplate such a matrix as a set of i two dimensional mxm matrices with degree t. This allows us to compute the total number of bivariate polynomials from a three dimensional matrix as explained below: Total number of polynomials = $l \times m \times m$ such that: $0 \leq t \leq m$ and $0 \leq i \leq l$ We can easily say that a function at the position i, j, k can be written as $F_{i,j,k}(x, y)$ as displayed in the Figure 4.1. Now by selecting a set S randomly of matrices containing bivariate polynomials from l, i.e., the total number of $m \times m$ two dimensional matrices can be obtained as: $S \geq \lceil (l+1)/2 \rceil$. where $\lceil x \rceil$ is the ceiling function that gives the smallest integer $\geq$ x. Using the ceiling function, We ensure that S is an integer always greater than or equal to $l/2$. This further guarantees that two different randomly selected sets S_a and S_b always have atleast one $m \times m$ Matrix in common. After selecting the random set S of matrices with one random column and one random row from each of these matrices in S, all the functions contained in the selected row and column are given to a mesh entity. For example refer Figure 4.2.

Now, since this matrix is of the order $m \times m$ it has m rows and m columns. So, the number of polynomials contained in one row and one column selected randomly are $m + (m - 1)$. Now, there are S such matrices hence total number of bivariate polynomials given to each MC are:



(a) S_a (b) S_b

Figure 4.3: Common Matrix between sets S_a and S_b

The total number of bi-variate polynomials = $S \times (m + (m-1)) = S \times (2m-1)$

Now, Let us analyze how two clients on the mesh can have common functions to establish a secure communication channel. Since we know two different set of matrices S_a and S_b have atleast one matrix in common. Let the two common matrices be as shown in Figure 4.3

Assuming the highlighted rows and columns were randomly selected row and column for sets S_a and S_b respectively. It is obvious that both these sets will have atleast two functions in common. In a better case, there could be more common matrices, leading to more common functions between two mesh entities. So, this technique of allocating polynomials guarantees any two MCs to have atleast two common bivariate polynomial functions which are used for secured communication.

Achieving a Secure Link for Communication: When the network is formed, each MC identifies its neighbors and exchanges information to generate a secure key for communication. Say for example, Once two neighbors C and D find each other, they share each others node ID and the indices of the polynomial functions they possess. This information is encrypted using a common Key K which is given to each node for an initial handshake and exchange information to generate a secured key on the fly. Using the polynomial function indices, both the nodes separately determine which function they have in common.

Assuming the node IDs are IDC and IDD and the common functions are $F_{2,7,6}()$ and $F_{2,3,4}()$.
At node C, seed values will be computed using the common functions and node IDs of C and D.

$$\text{Seed } 1_C = F_{2,7,6}(\text{IDC , IDD})$$

$$\text{Seed } 2_C = F_{2,3,4}(\text{IDC , IDD})$$

Similarly, at node D, it would compute its seed values:

$$\text{Seed } 1_D = F_{2,7,6}(\text{IDD , IDC})$$

$$\text{Seed } 2_D = F_{2,3,4}(\text{IDD , IDC})$$

Since functions $F_{2,7,6}()$ and $F_{2,3,4}()$ are bivariate polynomial we get using this property:

$$F_{2,7,6}(x, y) = F_{2,7,6}(y, x)$$

The same is true for any other common function therefore:

$$\text{Seed } 1_C = \text{Seed } 1_D$$

$$\text{Seed } 2_C = \text{Seed } 2_D$$

This is applicable to any further seeds.

So, the seeds generated independently at both the nodes would be identical. Each node uses a one way hashing function $Hf()$ that is assigned during the deployment phase. All the seed values are hashed to generate a final secured key for communication and since the same hash function is used at both the nodes and seed values being identical, they both have the same identical unique key for encryption or decryption. This key is never sent over the network and is just used for encryption at the sender end and decryption at the receiver which ensures the key not to be stolen by other entities that might be overhearing the communication.

$$SecureKey = Hf(Seed\ 1_C, Seed\ 2_C, \ldots)$$

If the two nodes have more than two common functions, they generate more than two seed values. This provides more than two seed values to the hashing function which makes it even stronger and more secure. In this fashion, all the nodes establish secure encryption technique with their one hop neighbors. Assuming a node A needs to communicate to the Internet Gateway which is five hops away from it. Each of the four links on the way would be a secured connection using pairwise key. This pairwise secure key establishment ensures end-to-end secured transfer.

Privacy

A lot of work has been done in the field of security [77, 79] for a WMN. But, multiple vulnerabilities still remain open in the field of privacy. Several researchers have attempted to address the privacy issues related to a wired network and there seems to have a lot of scope in this field especially in a wireless network scenario. For example, in a wired network, Onion Routing [80] was invented by Michael G. Reed, Paul

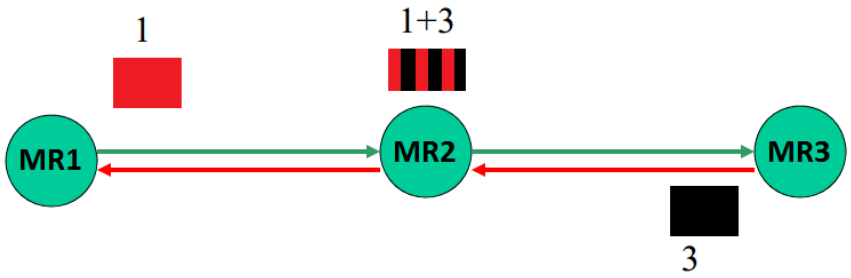


Figure 4.4: Coding Gain with oppurtunistic listening Example 1

F. Syverson, and David M. Goldschlag to provide anonymity of destination. In this scheme, a path is pre-computed at the source and the data packet is encrypted in multiple layers with the public key of the forwarding node along the path to destination in a sequential order and each node removes their layer of encryption after receiving the packet and forward the remaining packet called the onion to the next hop and finally the decrypted data with all the layers of encryption removed, received by the destination. The work in [81] resorts to a quantitative approach towards privacy. Authors in [82] specifically approach provisions for privacy preservation but lack efficiency of gains achieved from the network coding. The basis of privacy performance parameters are well defined in [83].

In [84], Wu and Li introduced an onion ring protocol for wireless mesh networks where onion rings are formed starting at the IGW and using all the cycles in the network. Data only travels in one direction and data sessions are only initiated at the gateway router. This provides a good anonymity, while fails on several issues such as a bottleneck is created at the gateway router as all the scheduling is done at the gateway. Moreover, this scheme works on the concept of finding cycles. In a dynamic WMN, uplink messages are initiated at the MR to traverse through the network to the IGW, which could fail in a realistic scenario. Another problem in this protocol is all the other nodes in a ring have to wait while one node communicates.

The work [85] talks about a layered onion ring approach in which some routers are considered trusted nodes and is similar to [84]. Communication starts and ends at the MR and some level of anonymity is present in the network. But, this work strongly relies on finding the cycles in the network.

Random Linear Network Coding

In Random Linear Network Coding (RLNC), participating nodes combine their incoming packets linearly using randomly chosen coefficients. It has been observed to be very efficient with reference to the network

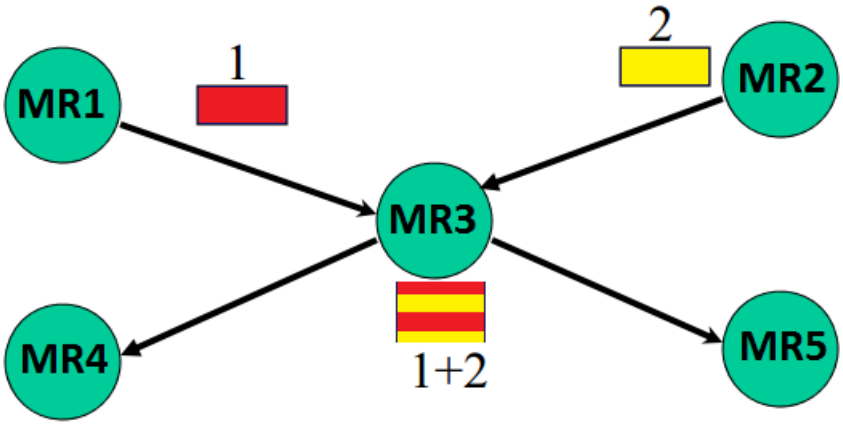


Figure 4.5: Coding Gain with oppurtunistic listening Example 2

coding exemplar [86]. The basic idea behind network coding is when a node overhears multiple incoming packets, it simultaneously places a linear combination of all the overheard packets and retransmits this single coded packet which when received, can be decoded to obtain original packets if sufficient information is available at the decoding node. Example of coding gain achieved as explained in [87] is shown in Figures 4.4 and 4.5. Intuitively, these gains are huge and open new doors to multicast networks like P2P and WMN's. As any new superior technology not only does it create several new possibilities and strengths to wireless networks, it also opens new doors for exploiting new security and privacy schemes. Inherently network coding approach does provide some security due to its intrinsic nature. But, being an application for content distribution efficiently it works on cooperative networking and all nodes are trusted with sharing several parameters for information extraction which faced with any smart malicious node fails miserably. Intrinsically Network Coding approach has a huge conflict with strong anonymous schemes like onion routing and are actually unusable in their original form. Our approach modifies both these well known schemes and combines them together to work cooperatively while removing any conflicts systematically. Some existing similar approaches employing network coding and achieving privacy can be found in [88] and [89]. Authors in [90] introduce an enhanced scheme for network coding and promise even superior gains. The work in [91] achieves groundbreaking results in deploying network coding for a realistic wireless network and provides huge gains over conventional packet forwarding mechanisms. In our proposed scheme, we use the foundation of network coding using XOR scheme. This work is our further enhancement to the work previously published in [92].

Figure 4.6: Message Propagation

4.2 Proposed Scheme: Network Coding with Enhanced Onion Routing

We assume that all MCs have Omni-directional Antenna with uniform transmission range. Network Initiation takes place with neighborhood discovery by MCs, MRs and IGW's. Each MC discovers its one hop neighbor MR's which we define as a neighborhood as given in Table 4.1. Our scheme has two salient features. First, a group key is generated using bivariate polynomial among devices in a neighborhood. The second step is to merge the message with the group key similar to network coding so that actual message is never transmitted, but extracted at each intermediate MR as illustrated in Figure 4.6. When the message propagates from MR1 to MR2 and so on. As MR2 knows the group key K1 between two MRs, the message can be easily extracted. Then, MR2 encrypts message by mixing with K2 similar to network coding and so on till the message reaches the IGW.

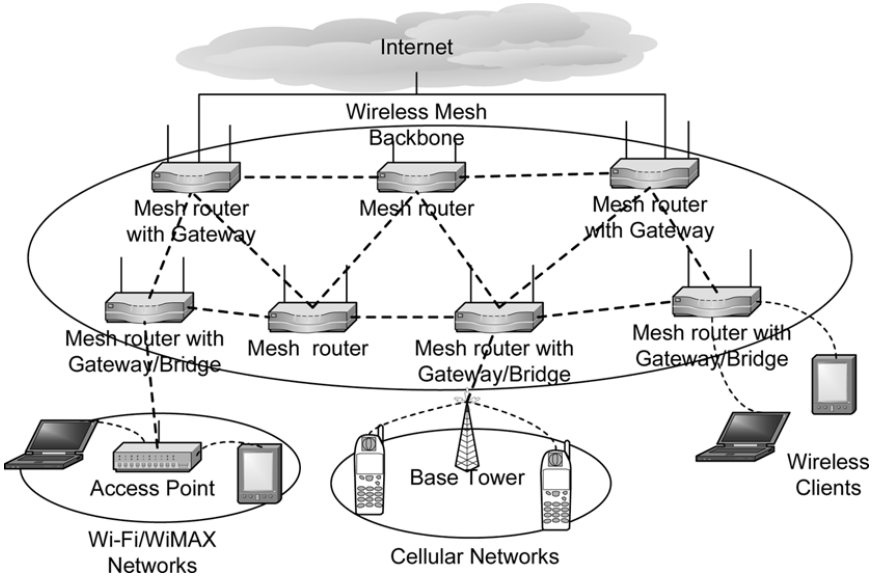


Figure 4.7: A Wireless Mesh Network

4.2.1 Network Initiation

Network initiation starts with one hop neighbor discovery and creating authenticated secure communication paths. Each MC registers its membership with the MR over a secure communication channel. After MC's registration is complete MR processes the network map creating a uniform spanning tree with branches of the tree that gives routes going through various MRs and eventually to an IGW.

Table 4.1: A Branch Table Entry

BID	Nextid	Previd
34	A3E	C5F

Having multiple MRs makes our scheme even stronger as it enables routers to work cooperatively while providing higher privacy and sharing the load. In such cases branches starting and ending in a MR can be created for the network topology of Figure 4.7 and the corresponding network model of Figure 4.9. Creating such Neighborhoods gives the scheme multiple strengths. All the members of the neighborhood that are a part of a path in which data flows, is illustrated in Figure 4.8.

4.3 Implementation Details

This section describes how our scheme reacts in different network scenarios and how network coding is intertwined with onion routing using onion packets providing very high level of privacy at a low cost and achieving the coding gain utilizing opportunistic listening and coding as in [87]. In our proposed scheme we have segregated MRs into one-hop neighborhoods. This logical network sectioning makes our scheme robust and distributed hence ideal for a Wireless Mesh Scenario.

We use a similar network coding scheme as proposed in COPE in [87]. Additionally we empower the relay nodes by providing just enough information to be capable of deciphering routing information to

Figure 4.8: Route for Mesh Routers to IGW

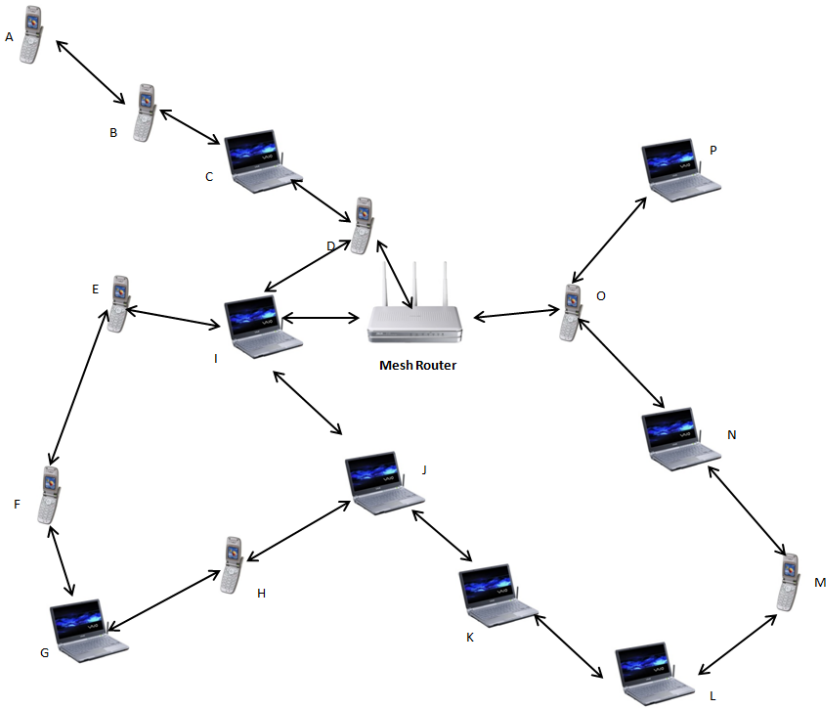


Figure 4.9: Network Map at MR (center)

the next hop in the correct direction towards the destination node. This is achieved without disclosing a source-destination pair and the payload of the data packet. At the same time a relay node is capable of opportunistically decoding and encoding data packet again together but with a very different key. This makes the COPE [87] coding scheme even more efficient and utilizes lower overheads while keeping high gains.

4.4 Performance Analysis

In [78], we have shown that our PBS (polynomial based scheme) is highly scalable and perfectly secure which is provided at a very low cost. With very few functions stored on a MC, we can support a very large network. The proposed Network Coding combined with Onion Routing(NC&OR) scheme takes this to the next level and fills the gap of privacy in case of an attack by a global adversary. Very high level of anonymity is achieved at the cost of an incremental overhead, like decryption and encryption with a new key at each stage. The overheads are caused by Multiple Encryption as per onion routing. It can be easily observed that the onions incur a heavy cost of usage. But, in NC&OR, we only use forward path. This helps us in keeping

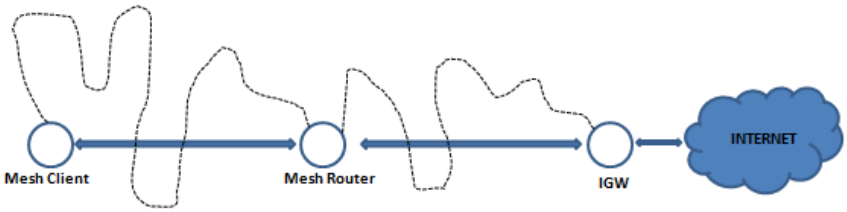


Figure 4.10: A Packet Propagation Path from Client to IGW

the cost to bare minimum for multiple encryptions as compared to a pure onion ring routing in [84] and layered onion ring routing approach of [85] where they always use onions for any type of communication. Redundancy in Network Coding and Modified Onion Routing is much more efficient than Phantom Routing of [93] which is based on flooding to ensure privacy among a group of nodes that necessitates too many re-transmissions.

Anonymity:

To an outside observer, all the MRs in a WMN act exactly the same way. The encrypted communication combined with the usage of dummy packets makes it impossible even for the global observer [94] to isolate the node initiating the communication session. Additionally, a session is never initiated at the MC as it can only request for a session to a MR. In case of presence of an inside attacker, information can not be leaked as each MC only knows about the 1-hop information among the branch (previous and next entity). The data packets are forwarded by an inside attacker and are encrypted. Hence, a dummy packet and a data packet are indistinguishable by an inside attacker as they appear exactly the same in their encrypted form.

In our scheme, the flow of traffic goes through two layers of branches which makes it impossible to isolate the session initiator. It randomly propagates the packet towards the IGW. In our case, the selection of branches on different levels is totally independent which makes it difficult to predict what path the packet is going to take by each MR. Additionally, availability of multiple branches adds further randomization to the selection of the final path taken. Multiple layers and availability of several branches makes our scheme more or less private and secure. Furthermore, each encryption key can be changed dynamically over time, using the bivariate polynomial.

Experimental Results:

We now evaluate our scheme using realistic wireless settings. Our evaluation is based on applying real

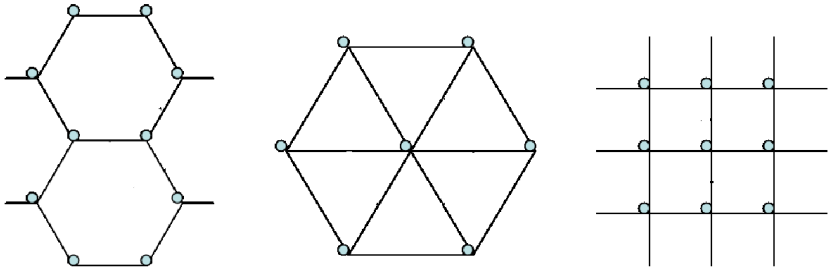


Figure 4.11: Regular MC Deployment in Hexagon, Triangle and Square Patterns

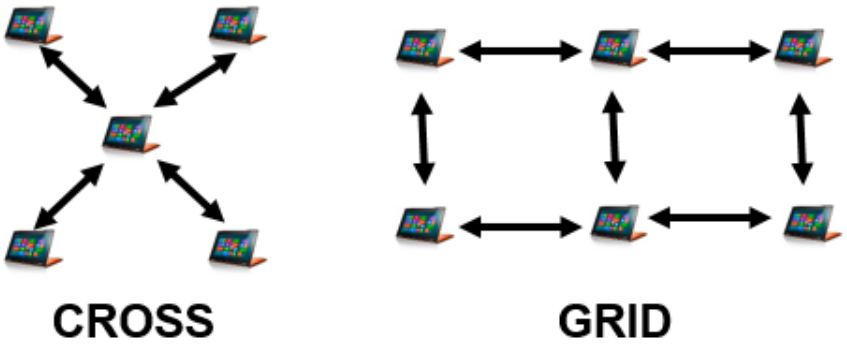


Figure 4.12: Regular Network Topology

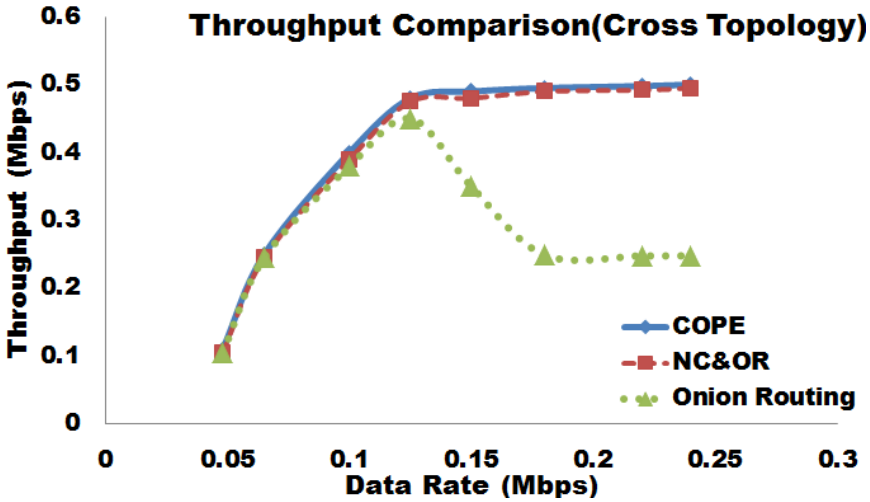


Figure 4.13: Average Throughput in Cross Topology

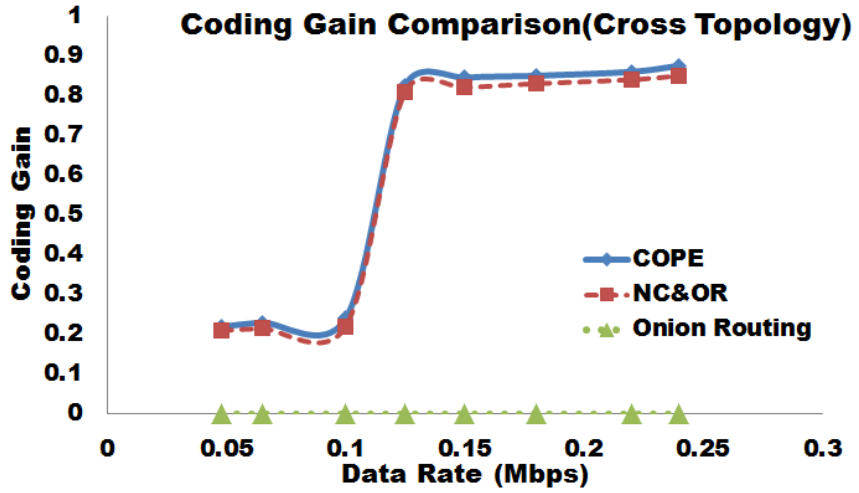


Figure 4.14: Coding Gain Achievement Comparison in Cross Topology

network metrics into the well known ns-2 network simulator. In our experiment two types of nodes are deployed. A MR acting as the sync node and rest of the MRs are all relay nodes with network coding capabilities and few nodes are randomly selected to act under an active session with the MR. We compare our scheme with the following two routing protocols:

1. COPE, the routing protocol with network coding (simulated by using our algorithm without any encryptions under same constraints and parameters),

2. TOR (The Onion Routing) protocol between initiating MR and IGW with no network coding (simulated by using our algorithm without any network coding under same constraints and parameters).

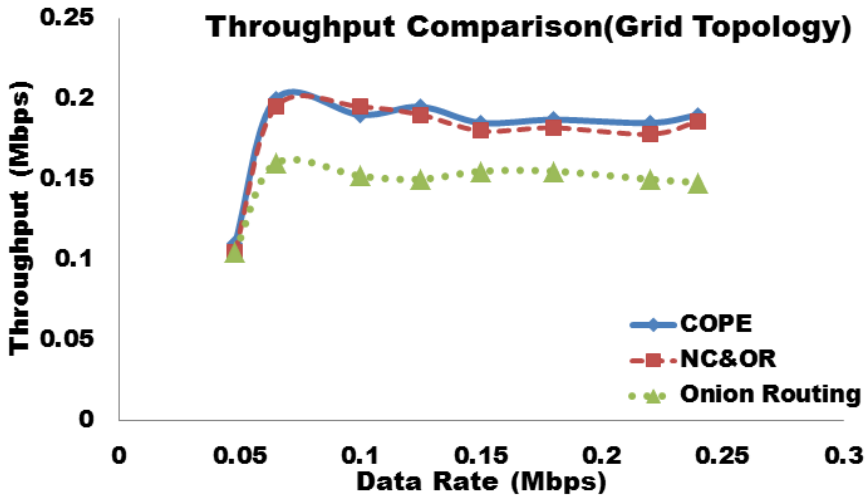


Figure 4.15: Average Throughput in Grid Topology

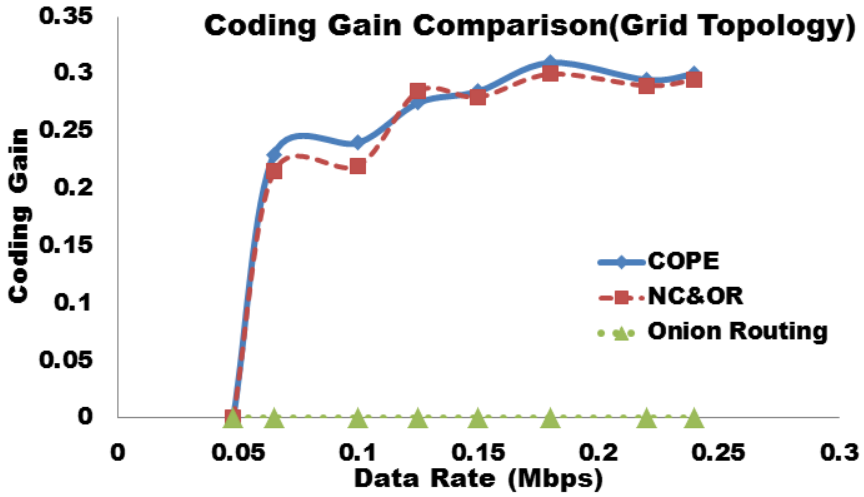


Figure 4.16: Coding Gain Achievement Comparison in Grid Topology

Our results are compared on the basis of performance in these three parameters:

1. Average Throughput over entire runtime.

2. Coding Gain (Fraction of total packets that were coded before forwarding)

3. Encryption/Decryption Cost, the computational cost of packet processing when encryption is used.

With our earlier experience with regular network deployments [95], we considered three standard deployments namely: Triangular, Square and Hexagonal as displayed in Figure 4.11. Triangular and Hexagonal deployments essentially break down into the cross topology and square deployment is represented by the grid topology as shown in Figure 4.12. We used all default seed values of 802.11b wireless networking specification using UDP data packets with transmission range is set to 250m. Results are averaged over 15 simulations for each setup. Graphs 4.13, 4.14, 4.15, and 4.16 show how our scheme Network Routing and Onion Routing (NC&OR) gives high level of coding gain almost equivalent to COPE while maintaining Onion Routing's high level or security and privacy. Further we deduce from our results that Cross topology outperforms Grid topology.

4.5 Conclusion

In this chapter, we propose solution to an substantial problem that when a wireless network unfolds network coding, previously operational privacy-sustaining methods no longer operate correctly or are left non-functioning. To this end, we propose a superior hybrid scheme which combines the strengths of onion rout-

ing and embedding it with Network Coding , a contemporary anonymous communication protocol which can function for distributed dynamic wireless networks. Both analytical and experimental results suggest that our scheme not only keeps the advantage of network coding for an effective use of the capacity, but also ensures enhanced privacy for MCs without much overhead.

Our proposed scheme encounters various complex network scenarios in a random network topology scenario. The research work is ongoing in a realistic random deployed WMN. Preliminary results obtained experimentally show promising prospects for high gains and efficient performance of our scheme NC&OR in a random WMN.

Chapter 5

Implementation Details

5.1 Ubiquitous Hybrid Network

Existence of several application specific network technologies like Sensor Networks, Cloud, Personal Area Networks (WPANs), Vehicular Networks (VANETs), Content Delivery Networks and Wifi operating oblivious to each other in the same ISM band creates numerous problems like contention for the same bandwidth leading to excessive collisions and hence lower throughput. This calls for a hybrid mesh framework that is capable of supporting heterogeneous devices in an IoT paradigm. This work proposes exactly that kind of environment.

There are several benefits of deploying a hybrid mesh to bridge numerous types of networks and devices, like availability of more data and in some cases, redundant data leads to high reliability. Further, Cooperative interoperability assures higher throughput and efficiency. In case of universal rich data availability, accurate and situation aware decision modeling is achieved. For example, In case of a vehicular network, accurate driving decisions can be made. Additionally, Higher and reliable data availability leads to detailed knowledge and perception which can be further exploited to ensure high level of Security in the network.

Motivation for an unified platform:

1. Robust security and privacy protocols spanning uniformly across all platforms.
2. ISM band exhaustion leading to excessive collisions and contentions.
3. Cooperative Interoperability desirable.

4. Universal availability of data across all platforms which is reliable and synchronized.

5. Plug and play universal usability.

6. Reliable data availability leads to accurate situation aware decision modeling.

7. Multiple channels usage to maximize bandwidth usage otherwise unused.

8. Optimizing Content delivery in hybrid mode which will be the major chunk of network traffic as projected.

5.1.1 Challenges

Archaic Internet Model:

Internet was originally invented by DARPA keeping in mind a service oriented model. This model was built under the assumption of a very linear and one-dimensional relationship known as the client server model as displayed in Figure 5.1. This was followed by a distributed multiple server model. Internet had an explosive and distributed growth after it was widely accepted in the public domain. The advent of peer to peer (P2P) ensured the move towards a hybrid topology. The archaic IP model offers several benefits but has serious limitations for ubiquitous futuristic networks. Keeping these in mind existing solutions and products are only as good as our visualization of the problem.

International Standards Organization (ISO) introduced a layered approach for the network model which comprised of 7-layers as shown in Figure 5.2. This model considered too cumbersome, was replaced by a 4-Layer TCP/IP model later. Both of these layered approaches have several benefits like ease of operation and a modular approach. The advent of Software Defined Networking(SDN) in recent times have made the layered approach pretty much outdated. Since, most of the features and benefits are provided and guaranteed within the application layer. This approach ensures keeping all the lower layers to their bare minimum. This extremely useful approach is advantageous to low power devices with low MAC and PHY layer capabilities and also gives the user greater control by capability of customizing every network parameter within the application.

In the light of IoE, everything becomes smart with a microprocessor and network interface. All under an umbrella of IoT paradigm where everything is network capable and connected. My goal is to bring every

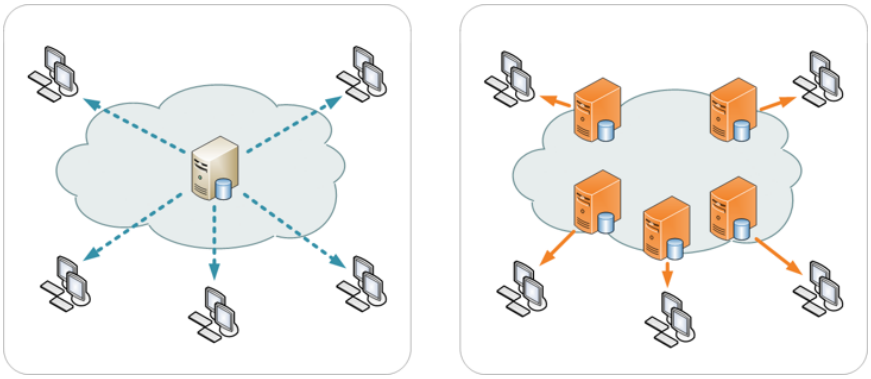


Figure 5.1: Archaic Client-Server Model

application specific network together on the same platform, specifically, Sensor Networks, Cloud, WPANs and VANETs while enforcing and satisfying the requirements of CIA triad with non-repudiation universally.

Challenges for an unified platform:

1. Heterogeneous devices.
2. Resource Limitation: Computation, Memory and Battery life.
3. Hardware Limitation: Single Radio with limited communication protocols at disposal.

Advent of Software Defined Networking:

1. Cheap availability of general purpose hardware. Ex: Arduino, Raspberry Pi etc.
2. Multiple Radios (Ethernet, WiFi, Bluetooth)

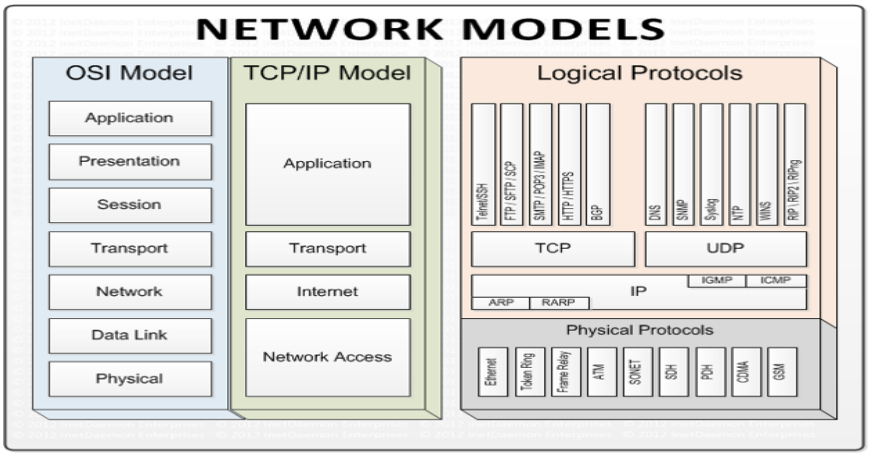


Figure 5.2: OSI and TCP Layered Approach

3. Multiple Antennas (MIMO)

4. Cognitive Radios

5. Use all available channels for communication.

6LoWPAN devices

The 6LoWPAN model is based on the idea that even the smallest devices should be able to exploit the Internet Protocol and resource limited low-power devices with restricted processing capabilities should be capable of joining in the IoT. These devices generally have extremely limited PHY and MAC layer capabilities. They do not have a network IP address capability rather working with a hardware MAC address. Bridging these devices to our ubiquitous network is one of the major tasks achieved. All such devices are connected to a mesh router in our network that acts as a cluster head. The Mesh router in this case preprocesses the IPv4 or IPv6 header for such 6LoWPAN devices and carries out encapsulation and header compression. This process can be viewed as a typical Network Address Translation (NAT) operation by a gateway router.

5.2 Building Trust in the Network

There are several intrinsic benefits of our large ubiquitous network that can be exploited for building trust into the network. Further, availability of redundant data from multiple sources gives opportunity for verification of data integrity. The first step of building a trust network is by the neighborhood discovery. Once all channels of communication are established, a Trust value is computed for each individual node and each communication path in a distributed fashion. Default trust values for a particular node is awarded based on its level in network hierarchy. Trust values/Reputation are computed both locally and queried from the network in a hierarchal fashion similar to DNS queries. Trust values are defined for both a network node and communication channel.

5.2.1 Trust Value

Default trust values for a particular node is awarded based on its level in network hierarchy. These values are dynamically adjusted or corrected based on observed behavior and received reports from trusted entities like Certification Authorities in the network. Again, Trust Values are queried and computed locally when required as a function of received values from trusted nodes and locally observed behavior if any available.

Trust Value for a channel: The trust value of a channel is another dynamic metric computed as a function of aggregated trust values of each member node along the chain. In the simplest case, it is defined as a weighted average over the trust value of each individual nodes along the path of that particular channel.

Example: $TrV_{channelA} = (w_1 trv_1 + w_2 trv_2 + w_3 + \ldots + w_n trv_n)/(w_1 + w_2 + w_3 + \ldots + w_n)$

Since low trust level nodes expose the channel to the maximum risk, lower node trust values get the highest weight. Hence, reducing the Trust Value for the channel which can be observed intuitively. As mentioned earlier, trust values are broadcast regularly piggybacked on the beacon signal for neighborhood discovery.

5.2.2 Plausibility

Plausibility, also known as reliability or believability of a message received over a channel is defined or computed as a function of trust value of the channel. Hence, the reliability or authenticity of a received message is directly proportional to the trust value of the channel it was received over and the trust value associated with the sender of the message.

$P_{Message} = F(TrV_{channel}, trv_{sender})$

During the decision making process, within the network, a Markov model is used for state changes. Probability for state change is computed based on the Plausibility, e.g., Driving correction based on traffic data received for a Vehicular Network.

5.2.3 Malicious node detection

Once a Trust metric is established and Plausibility defined, this is extensively used efficiently for behavior modeling. In this behavior modeling, underlying behavior patterns are used for conclusively detecting and isolating malicious node behavior with high level of confidence. For example, a malicious node, in order to increase the plausibility of its data, a malicious node might advertise its own trust value as very high. Additionally, it can also try to announce trust values for other neighbors as extremely low in order to bias the scheme so as to maximize traffic routing through itself. Since, trust values for particular identities are queried from trusted sources and regularly updated based on availability of reports from neighbors, such misbehavior can be easily identified. Supplemental to this, availability of direct sensing and ad-hoc redundant data comparison gives positive detection of presence of a malicious node in case of an anomaly detection. Multiple reports sourced from neighboring crowd also in sensing range help confirm this activity. Only reports from nodes with minimum threshold trust value are taken in account while others are dropped. This method is found to be very efficient in helping converge the network trust status and identifying selfish misbehavior.

Next, when such selfish misbehavior is observed, it is accounted for immediately. This is achieved by penalizing heavily the trust value of the identified misbehaving node with exponential decrease. Whereas, good or expected behavior is awarded with a small additive increase based on above threshold number of positive reports received from neighbors. This ensures not only fast but also reliable trust value convergence.

Performance evaluation and assessing Security and Trust performance of a policy depends heavily on the underlying Threat Model used during simulation.

Highlights of our scheme:

1. AI and Machine Learning Methods exploited.

2. Observing and recording behavioral patterns.

3. Isolating Malicious behavior patterns.

4. Classifying behavior patterns.

5. Using non-malicious patterns for identity and access control as described as Human Layer or 8th layer in the layered Internet Model.

5.2.4 Access Control

To enforce access control a persistent and reliable Group policy is applied on top of a Firewall gives full access control. An effective group policy can only be exploited along with the deployment of an Identity service which depends on availability of trusted certification authorities that issues certificates to network entities to prove their identity. This unified platform depends strongly on the availability of such architecture. Another assumption taken into account is the manufacturer installs a unique identifier on each network device which can not be easily spoofed. Like certificates pre-installed on On-board Units of smart vehicles.

Example of Access Control: Sensor data from the perception layer in an autonomous vehicle can be accessed by an authorized user by using a secure channel.

5.3 Anomaly Detection by Statistical Analysis

We use multiple robust methods for anomaly detection in the captured data. Additionally, we also use this for network intrusion detection as described further. Anomaly detection refers to the problem of finding patterns in data that do not conform to an expected behavior. These non-conforming patterns are often referred to as anomalies, outliers, discordant observations, etc.

There are two different approaches used to identify contaminant data:

- Knowledge Based: With Training Data Available.
- Abnormal behavior: Without Training Data Available.

The techniques available to test for anomalies in the data are as follows:

- Bayesian Networks
- Rule-Based Systems
- Parametric Statistical Modeling

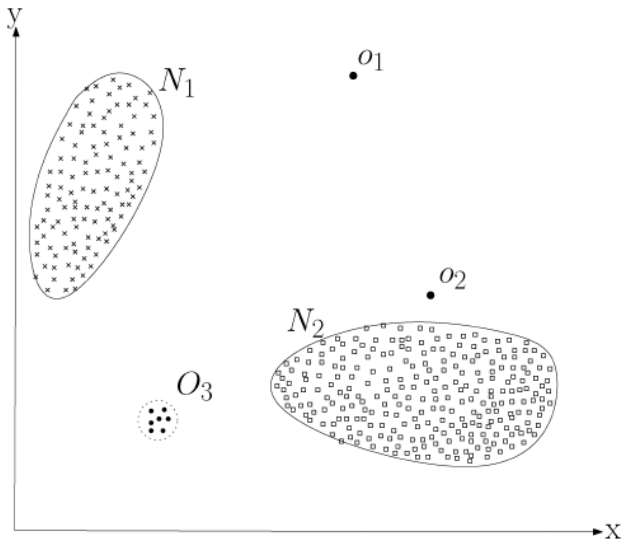
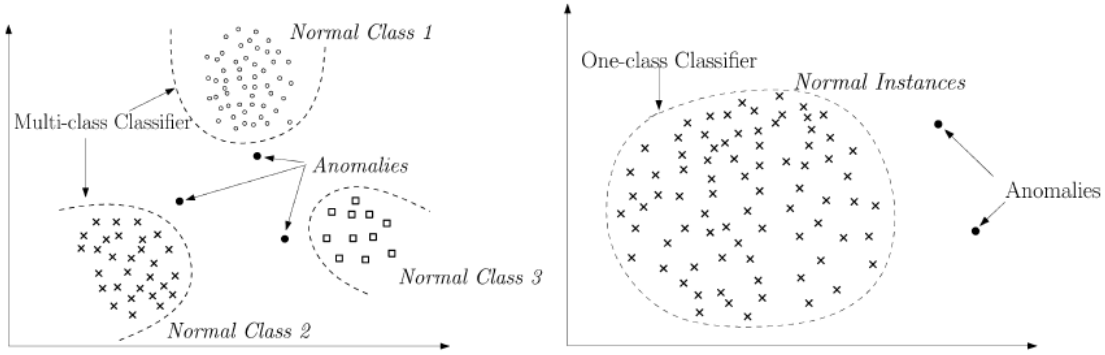


Figure 5.3: Example of spurious data in a two dimensional data set

- Nearest Neighbor-Based Techniques
- Spectral



(a) Multi-class Anomaly Detection (b) One-class Anomaly Detection

Figure 5.4: Anomaly Classification

Chapter 6

Simulation and Implementation of Various Network Scenarios

6.1 Simulation

We have used open source network simulator OMNeT++ to simulate various network scenarios and gauge the queuing delays and end to end delay etc. Additionally we have used Castalia framework which is a simulator for Wireless Sensor Networks (WSN), Body Area Networks (BAN) and generally networks of low-power embedded devices. It is based on the OMNeT++ platform and can be used to test their

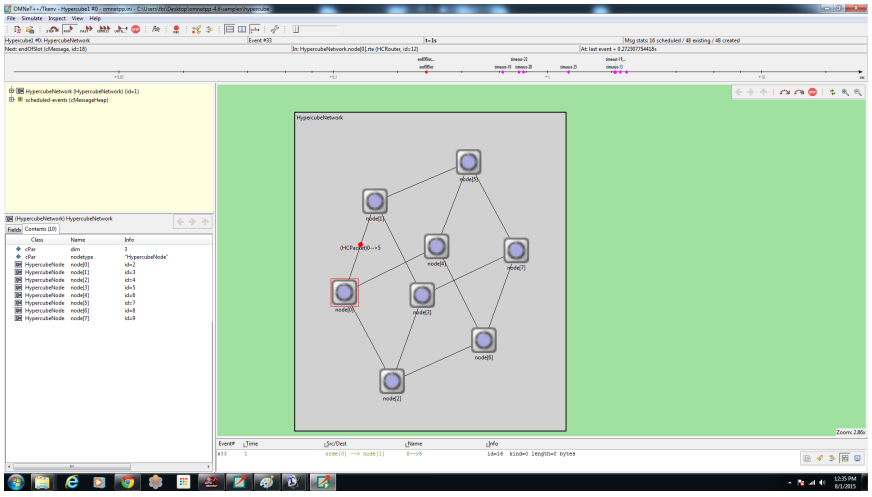


Figure 6.1: A Simulation of 8 sensors in a BAN over a hypercube

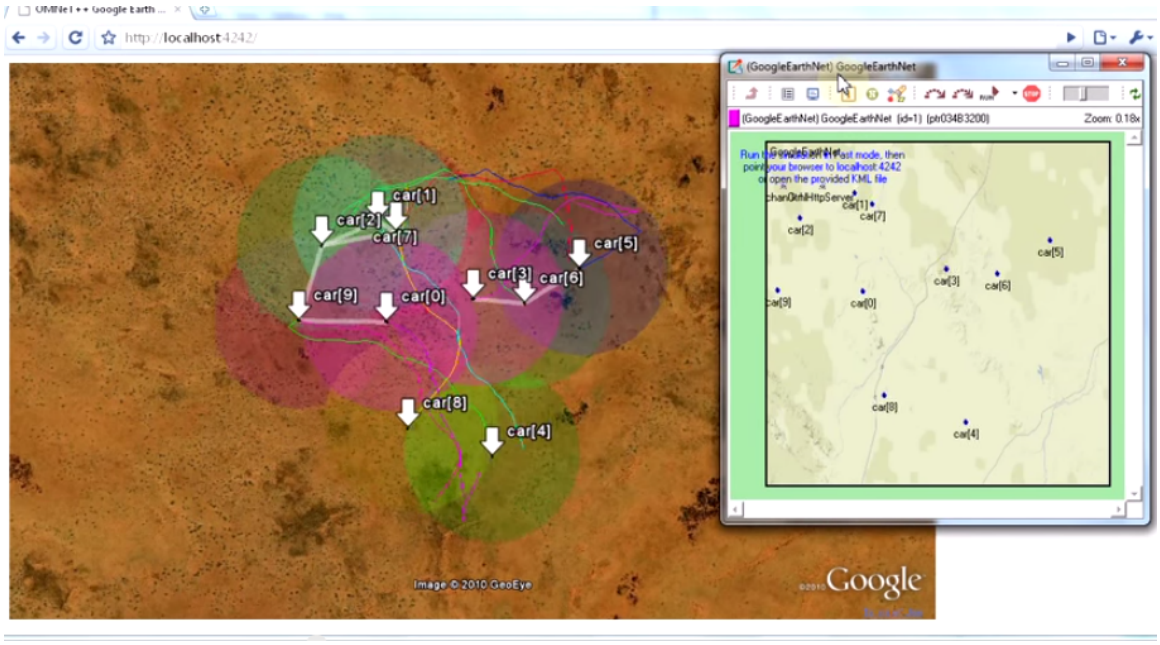


Figure 6.2: A Sample Simulation of a VANET in OMNeT using Google Earth Plugin

distributed algorithms and/or protocols in realistic wireless channel and radio models, with a realistic node behavior especially relating to access of the radio. Castalia can also be used to evaluate different platform characteristics for specific applications, since it is highly parametric, and can simulate a wide range of platforms. The selection of these framework and platform was on the basis of their ease of availability and user friendly GUI.

6.2 Vehicular Network

For a Vehicular Network scenario a highway topology as shown in Figure 6.3 was considered and studied. A modified onion routing scheme was used as described earlier in chapter 4 for ensuring security and anonymity. The performance and results of this scheme is described in detail in chapter 4. Clustering was used during platoon formation along with a platoon leader selection for the following benefits:

1. Packet Scheduling at cluster head.

2. Load balancing.

3. Collision and contention avoidance.

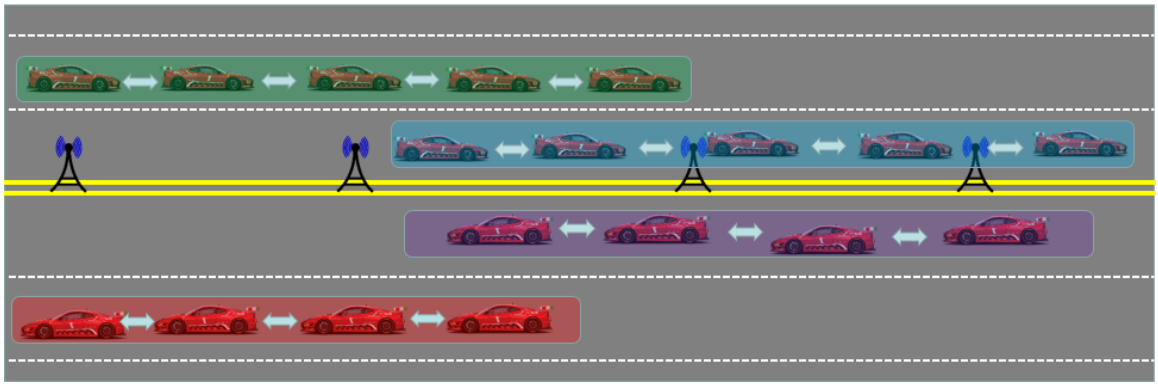


Figure 6.3: Clustering/Platoon formation with Cluster head/Leader selection.

4. All communication initiated at cluster head.

5. Anonymity induced within the platoon.

Communication within a platoon: Once a platoon is formed every member node enters the platoon information in a table which is used for further communication.

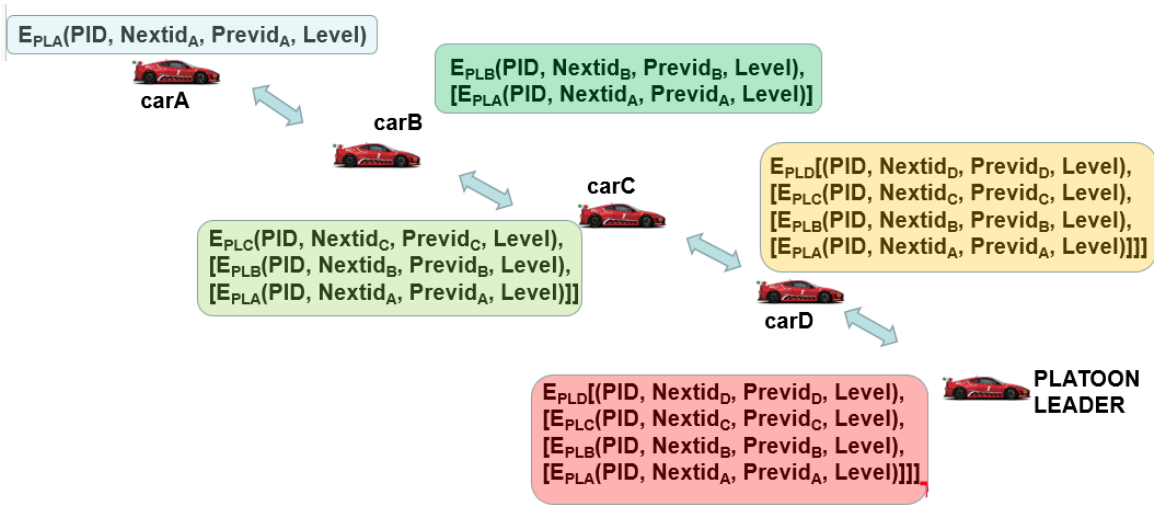


Figure 6.4: Onion packet traversal for Platoon/Cluster formation

Platoon ID	Platoon Key	Next Node ID	Prev Node ID	Security Level
qedw232	c23cxs	ewdf32d	23fc3	87%

Figure 6.5: A sample entry in the platoon table

6.3 Biometric data gathering Smart Shoe

*This work was patented as described in [96].

A smart shoe as shown in Figure 6.6 has been implemented and tested for data transfer. It has 7 round Force-Sensitive Resistor (FSR) on its sole that are connected to Teensy 3.1, 32-bit ARM Cortex-M4 platform compatible with Arduino to select any of the FSR reading to be transmitted. The Software backbone is Arduino platform with Arduino Platform libraries with an on-board powerful 32-bit ARM Cortex Micro-controller and extremely small form factor which is an open-source platform which provides the capability of programming in C language. Its an ideal platform for a project that involves getting sensor readings and sending control signals to actuators in a mobile compact environment.

Teensy 3.1 was chosen as our major component in the project due to its versatile compatibility with Arduino Platform libraries with an onboard powerful 32-bit ARM Cortex Micro-controller and extremely small form factor. Teensy provides several also digital and analog inputs accommodating all of our sensor inputs. This micro-controller platform is paired with Bluefruit LE - Bluetooth Low Energy (BLE 4.0) which provides wireless connectivity to our Teensy Chip to an iOS or Android based device to transmit the sensor readings over a wireless Bluetooth 4.0 Low Energy connection to any entity with Bluetooth capability such as laptop, cell phone, iPad and iPod. This chip was chosen for its exploitation of Bluetooth 4.0 LE hence very low energy consumption and extremely small form factor. These readings are gathered by the Teensy board

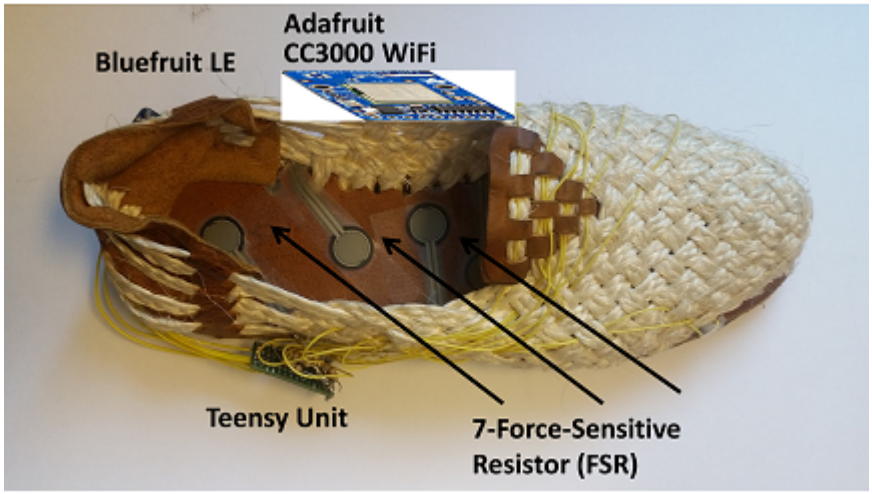


Figure 6.6: Shoe with 7 pressure sensors and other wireless devices

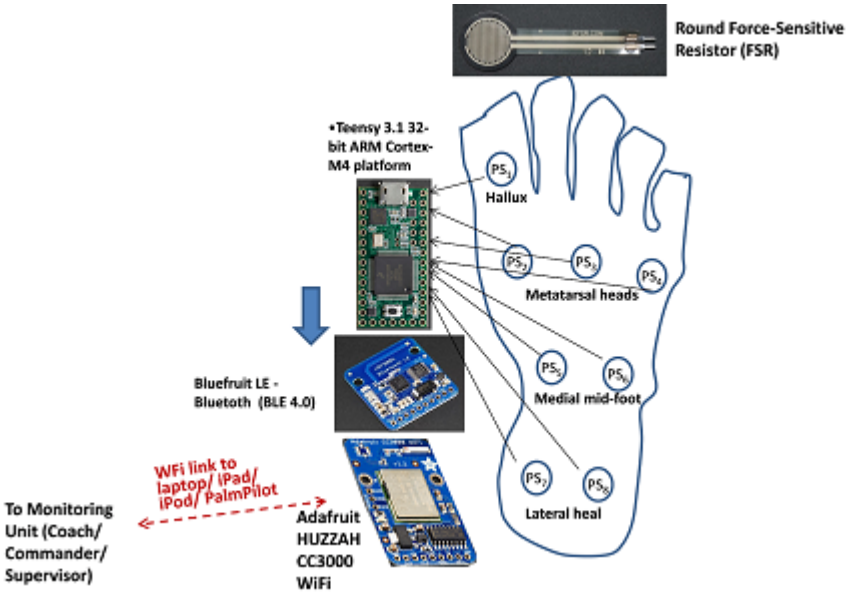


Figure 6.7: A Generic Personal Fatigue Determination using 7-pressure/force sensors

all analog readings are automatically converted into digital values by the inbuilt Analog to digital converter. Then these values are passed on to the Bluefruit Bluetooth board over the wired connections which are further transmitted to a paired Bluetooth 4.0 LE capable iOS or Android device over the Bluetooth wireless channel. Besides relaying real-time data from seven Pressure/Force, reading about Vibration, Acceleration, Temperature and Humidity readings are also obtained with sensors with the Teensy board. All the data logging, analysis and filtering is done at the iOS or Android device which can be an iPad, cellphone, or any tablet device.

The Adafruit HUZZAH CC3000 WiFi is totally compatible with Arduino Platform and data can be pushed as fast or slow as needed to a longer distance of approx 400 feet as compared to Bluefruit LE (30 feet). It has an asynchronous connection and supports 802.11b/g, open/WEP/WPA/WPA2 security, TKIP and AES. TCP and UDP in both client and server modes are possible with up to 4 concurrent sockets.

Our generic concept of determining fatigue level of an individual by the monitoring station is illustrated in Figure 6.7. For example, players play in the field and vital pressure values are transmitted to the coach monitoring on the side lines. The coach carrying an iPhone or similar device can get the data from 7-pressure sensors of both the shoes of a selected player and analyze it to determine fatigue level of the player. We will adopt and implement algorithm given in [12] to determine the muscle fatigue. The work in [12] suggested

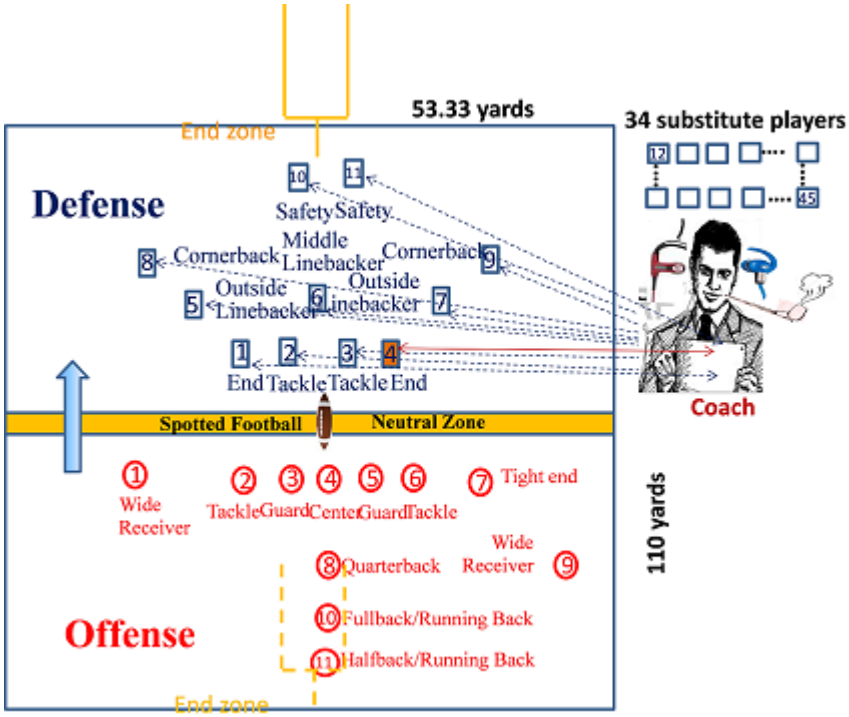


Figure 6.8: Football Players in action on playing ground

use of 10 sensors in each shoe and determining difference in pressure from two feet. The pressure pattern indicates ECM fatigue level. We looked at this work carefully and observed that only 7 pressure sensors show difference in reading between two feet while remaining three remain unchanged. So, we used only 7 pressure sensors in each shoe. The details of a football game is illustrated in Figure 6.8 and data from a player is obtained by the coach siting on the sideline is shown in Figure 6.9. The coach can send data to a central station for further processing and getting feedback about status of a given player.

It is interesting to note that whether an individual is walking, resting, climbing up stairs, running, etc., can be easily determined by the monitoring unit as variation in the pressure will indicate that phenomenon. This is shown in Figure 6.10, indicating co-relation between the body forces at different angles of the shoe worn by an individual. This scheme can be used in determining fatigue levels in soldiers, medical interns, and nurses.

Starting 1988, NCAA and National Athletic Trainers' Association have been using an injury surveillance system that collects injury reports submitted by trainers for roughly 380,000 male and female college athletes. Through 2004, there were 200,000 injury reports filed when an athlete misses a day or more of

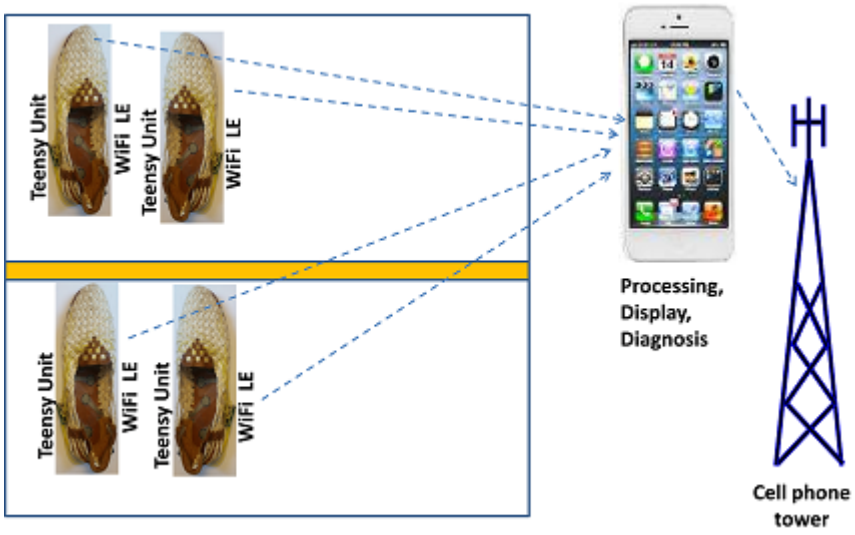


Figure 6.9: Data from a Player to Coach and central unit for monitoring and determining fatigue level

practice or competition which works out to about 12,500 injuries per year. That number has been relatively consistent over the years [97]. When a college athlete sustains an injury, one of his or her main concerns are how sooner he or she can return to the sport. The answer to this question is not easy as each athlete and each injury are unique. Returning too soon can increase the risk of re-injury or developing a chronic problem that will lead to a longer recovery time. However, waiting for too long can lead to unnecessary reconditioning. Return-to-play decisions are fundamental to the practice of sports medicine but vary greatly for the same medical conditions and circumstances. Although there are published articles that identify individual

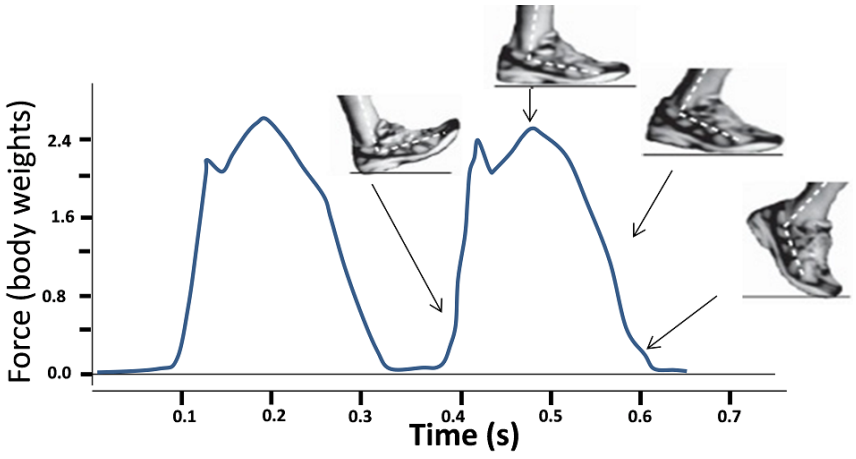


Figure 6.10: Variation of body force at different angles

components that go into these decisions, there exists neither quantitative criteria for allowing an athlete to return to play nor a model for the sequence or weighting of these factors within the medical decision-making process. Although some rudimentary exercises have been identified, there is a need to develop an objective decision-based model for clinical use by sports medicine practitioners that take into account the forces causing the injury to the players and produce individualized quantifiable outcomes. The performance of athletes in collegiate sports is very important for the reputation of Universities in North America. While large sums of money are spent on recruiting the best coaches and trainers, athletes are often suddenly forced out of games due to injuries that they may have happened during training or picked up while in an actual game. In body-contact games such as football, it is often difficult to ascertain the nature of the injury since there is so much action on the field. The injuries are often brought to the attention of coaches and/or trainers when the athlete has suffered a concussion that may affect his playing abilities. The coach should also have an ability to monitor performance of the athletes, thus help in determining current level of athletes injury, and help in preventing career threatening and/or fatal injuries. Furthermore, it should be possible to monitor players during the course of a game and determine the extent of concussions arising from a normal game-play. Therefore, technological solutions enabling the monitoring of athletes motion and physiological signals during sports and exercise are gaining increased attention as tools for preventing overload and for supporting rehabilitation in movement activities.

The number of injuries in different games keeps on increasing day by day. Among various games, football still has the highest injury rate with 36 injuries per 1,000 male athletes [2]. It is also observed that the transient body pressure on each leg depends on the angle of the toe as illustrated in Figure 6.10 [98]. However, under steady state, people exert different amount of pressures on two legs if a person suffers from Parkinsons disease [98]. Such imbalance in exerted force has also been observed in football games [99]. It may be noted that the mechanism proposed here can be used for other fast sports such as soccer, ice hockey, basketball, etc.

The primary objective of this research is to build a system that can monitor postural balance and stability of the athletes in real time and provide valuable feedback to the coaches so as to minimize the injury to the athletes and maximize their playing potential. Additionally, the system would possess capabilities to log the data for quick detection of concussion. Wireless technology employing small sensors are particularly

beneficial in this situation as it allows monitoring of kinematic, kinetic and physiological data without affecting individuals in executing their motions. Advances in miniaturized and wireless technology are beginning to push the capture measurement of real time game situation forces from being simulated in the training room that indicates what actually happens on the playing field.

Development of lightweight, wearable electronic force monitors has the potential to produce data for contact and injury forces. As discussed earlier, these data can be stored and analyzed to provide the coach with a complete picture of an athletes fitness and thus enable him to pick the eleven athletes playing for the whole team. We plan to monitor the impact suffered by athletes and determine the level of postural instabilities following a concussion. Our system would be versatile and be able to support other sensing devices over the same wireless transmission backbone. The data acquired by the system would be stored in a database accessible through a secure portal for analysis and feedback. This data can be used by coaches, doctors and other specialists in the field of athletic medicine in order to make informed decisions following injuries to players. As with any modern portal, our system would be completely scalable and support a wide range of devices from traditional desktop computers and laptops to handheld devices such as tablets and smart phones. This will be our ultimate step in building a comprehensive platform for enhancing athlete performance and improving their general well being.

To illustrate the proof of the concept, we designed shoe soles, each unit with three sensors connected to a laptop via appropriate interface as shown in Figure 6.6. We let a person stand on the shoe and take the reading by letting him do on-spot exercise. Our overall objective is to create a system that can send results to different devices like tablets and advanced mobile phones besides a lap top and such a generic scheme is shown in Figure 6.9. A variety of user interfaces would be supported in our proposed system. The most basic of them would be a website that can display the requested information. Additionally apps for the iOS, Android and the Windows Phone platform would be developed that would enable our system to be used from these portable devices. The user interface would enable the user to logon and view physiological data pertaining to a particular individual. Controls would be provided on the user interface that would allow the user to view historical data and compare the same with the current data. If analysis of the data is required, additional web services would be called that would result in the database/analysis server computing the

results and the resulting output would be rendered on the device.

6.4 Experimental Setup for a WPAN

6.4.1 A simulated body area network as a WPAN

16-strategically placed body sensor nodes have been used, 4 different transmit power levels and 6 different Mobility models depending on the varying body postures are used for simulation purposes. Simulation of the Wireless Body Area Network (WBAN) runs for 5 minutes for each combination of power level and a body posture. Data is recorded at each sensor while acting as a sink node/data gathering node, for receipt of a packet from rest of the sensors in the WBAN at each time interval t. In this case value of t is 100ms as the packet rate is 10 packets per second. For example simulation is run for 5mins (300secs) with power level 0 dBm while the test subject is walking which is our mobility model in this example.

Power Levels used:

1. -18 dBm
2. -12 dBm
3. -6 dBm
4. 0 dBm

Total number of power levels = 4

Total number of postures = 6

Total number of sensors = 16

Number of data packets per second = 10

Simulation runtime for each combination= 5mins= 5X60 = 300 seconds

Total number of combinations = 6x4 = 24

Total Runtime for entire Simulation = 24 X 300 = 7200 seconds = 120 mins = 2hrs

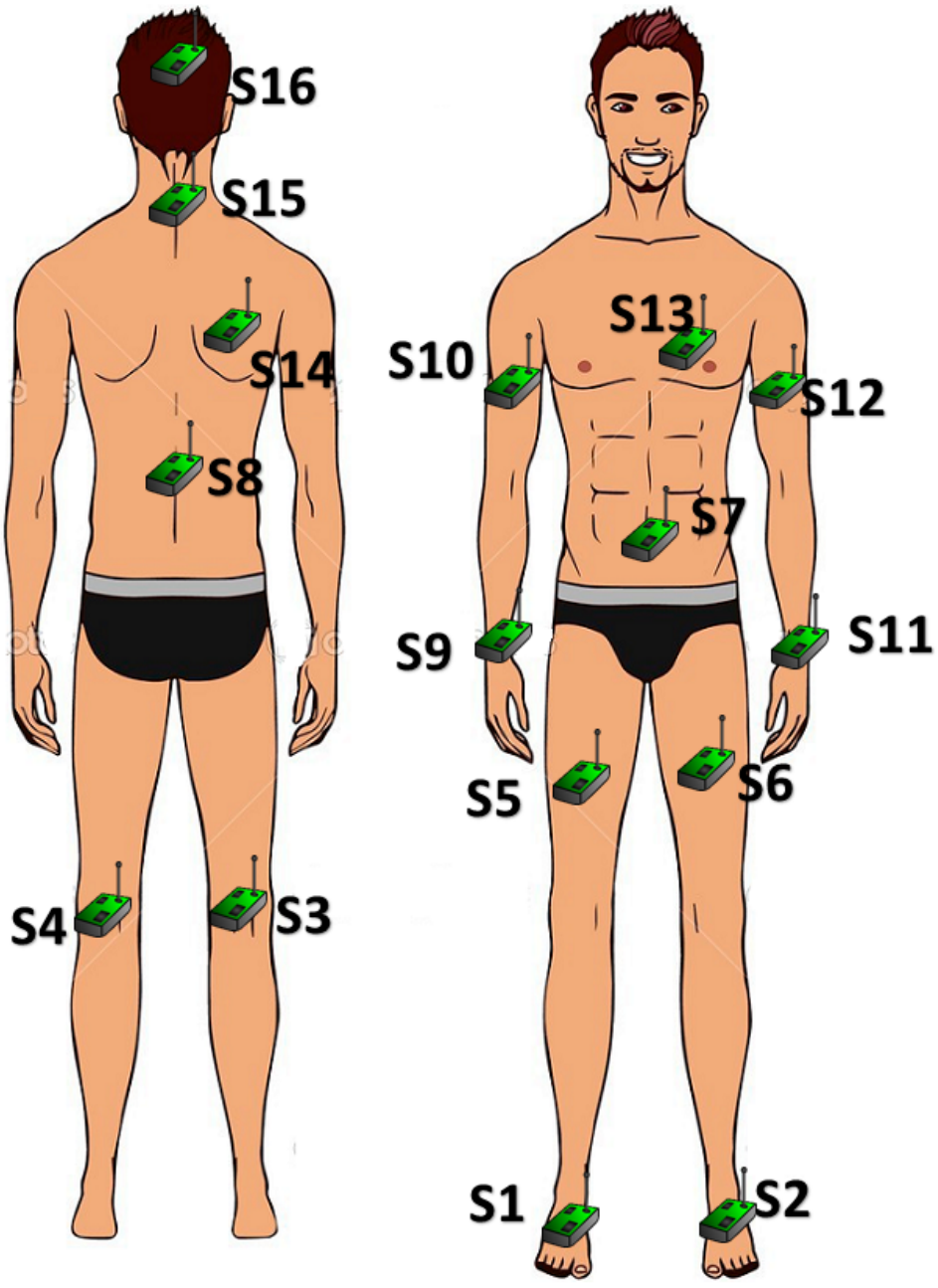
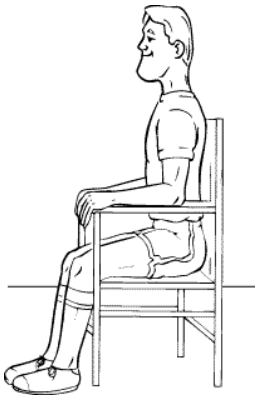
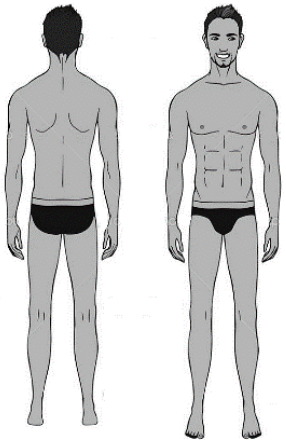


Figure 6.11: Sensor Placement on a human body front and back



(a) Sitting in a chair

(b) Sitting on Ground (Yogi)



(c) Standing

(d) Walking

(e) Lying down

(f) Running

Figure 6.12: Body Postures

Table 6.1: Parameters Used for Body Area Network Simulation

Simulator Used	OMNet ++ Version 4.6
Add-On Framework Used	MiXiM Version 2.3
Protocol Used	IEEE 802.15.4
Band Used	2.4Ghz ISM
Data Rate	2 Mbps
Packet Size	32 bytes fixed
Sensor Modes used	RX, TX, or Standby modes
Varying Power Levels Used	-18 dBm, -12 dBm, -6 dBm, 0 dBm
Varying Mobility Models used for simulation	Sitting on a chair, Sitting on the ground, Standing, Walking, Lying down, Running
Packet Rate	10 packets per second
Channel Access	TDMA, CSMA/CA

6.4.2 Effect of Mobility and Body Posture

The function defining the body posture and the motion of the complete body over time plays a very important role for routing and sink node selection. If we want to design an effective hybrid dynamic protocol that gives best efficiency i.e. with acceptable throughput while preserving energy and minimizing errors we have to integrate this in our protocol. Since there can be infinite number of postures and directions for a human body movement function over time we break it down into discrete events and try to study it and integrate the changes required in our model. That is why we start with six postures and simulate to calculate the packet loss in each body posture as shown in Figure 6.12

6.4.3 Result Analysis

At Power Level1 = -18 dBm

Looking at these results it seems like Sensor 13 comes out to be the winner among all the Wireless sensors according to the average number of packets received when power level is fixed at -18dBm. Sensor number 13 in our experiment is the one that has been placed on the chest in the close vicinity of the heart.

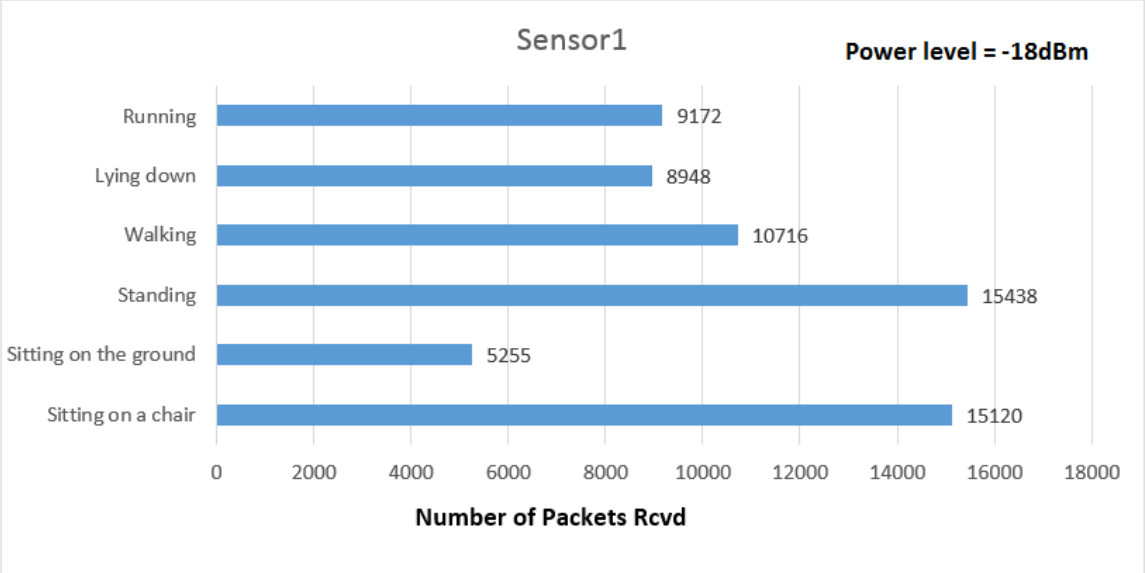


Figure 6.13: Packets received by Sensor1 at Power Level1

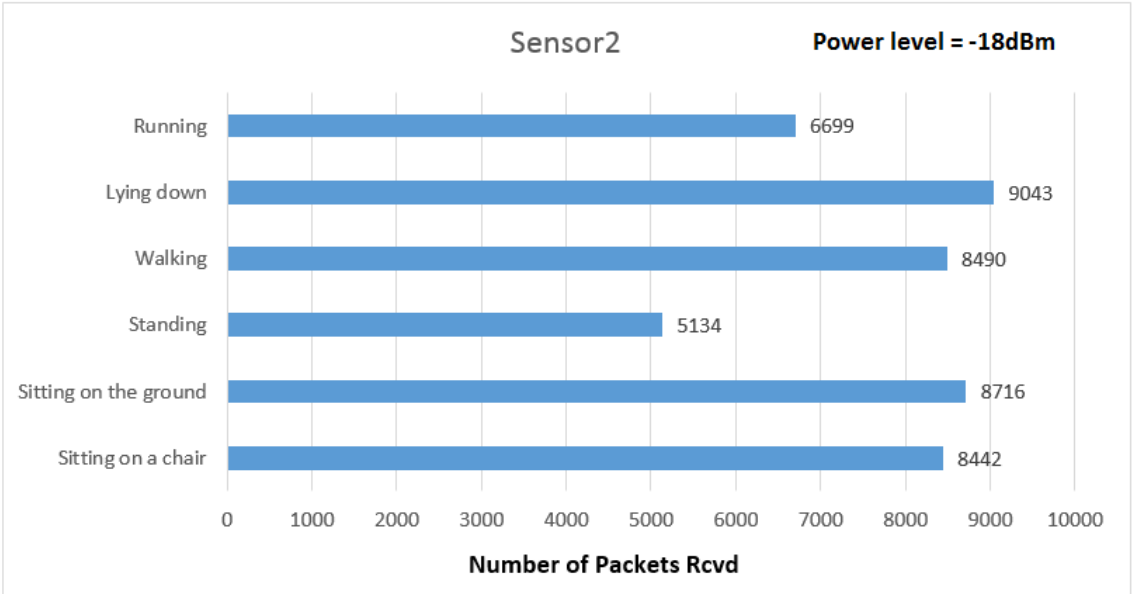


Figure 6.14: Packets received by Sensor2 at Power Level1

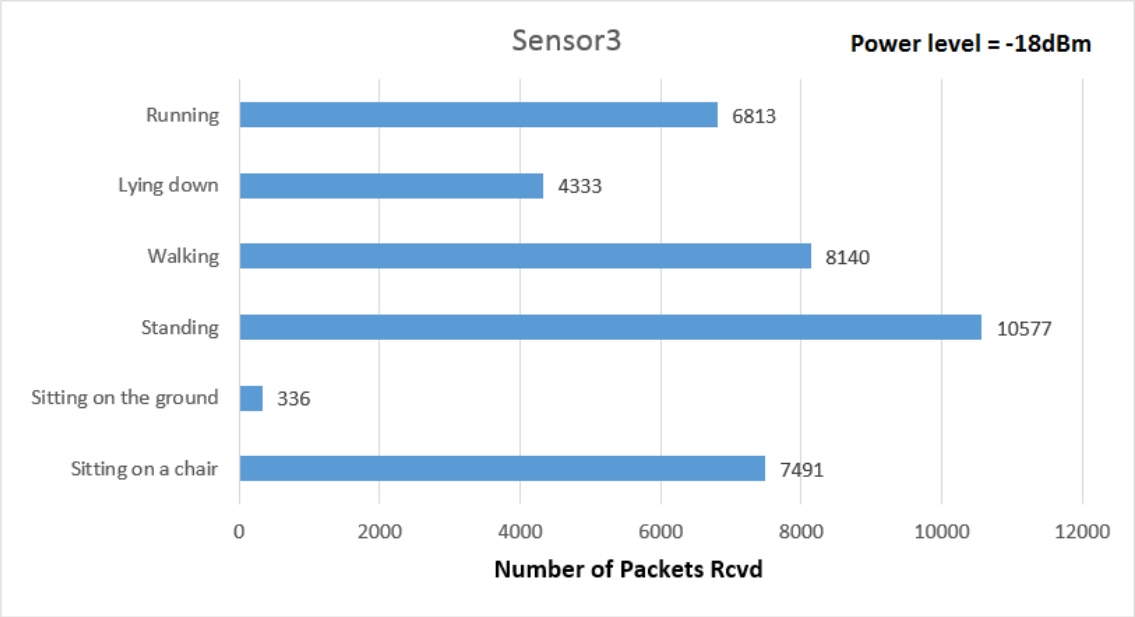


Figure 6.15: Packets received by Sensor3 at Power Level1

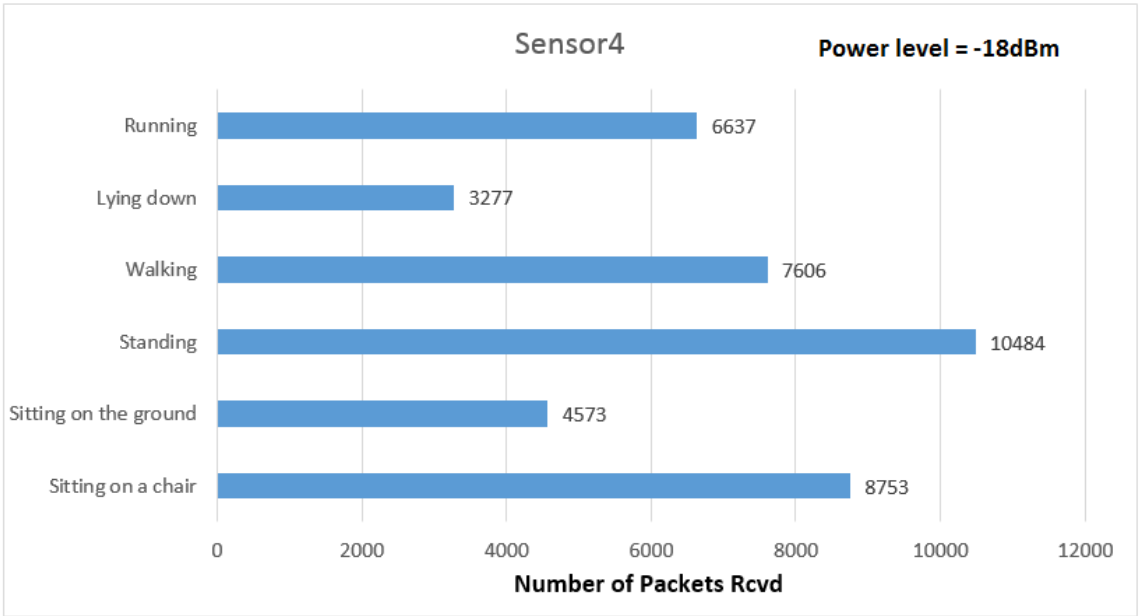


Figure 6.16: Packets received by Sensor4 at Power Level1

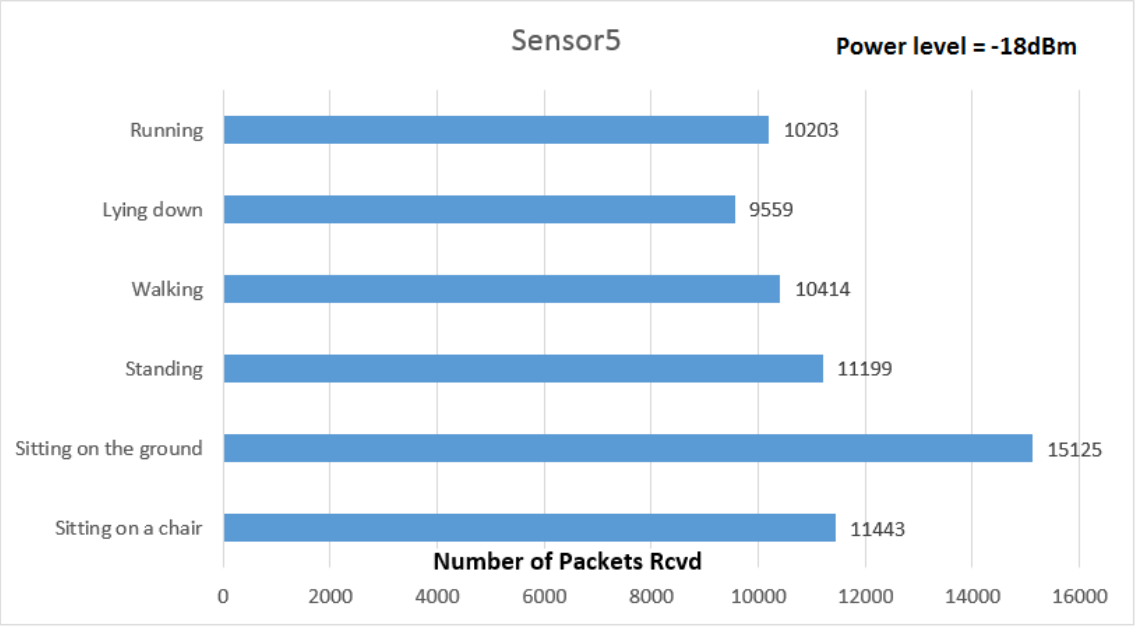


Figure 6.17: Packets received by Sensor5 at Power Level1

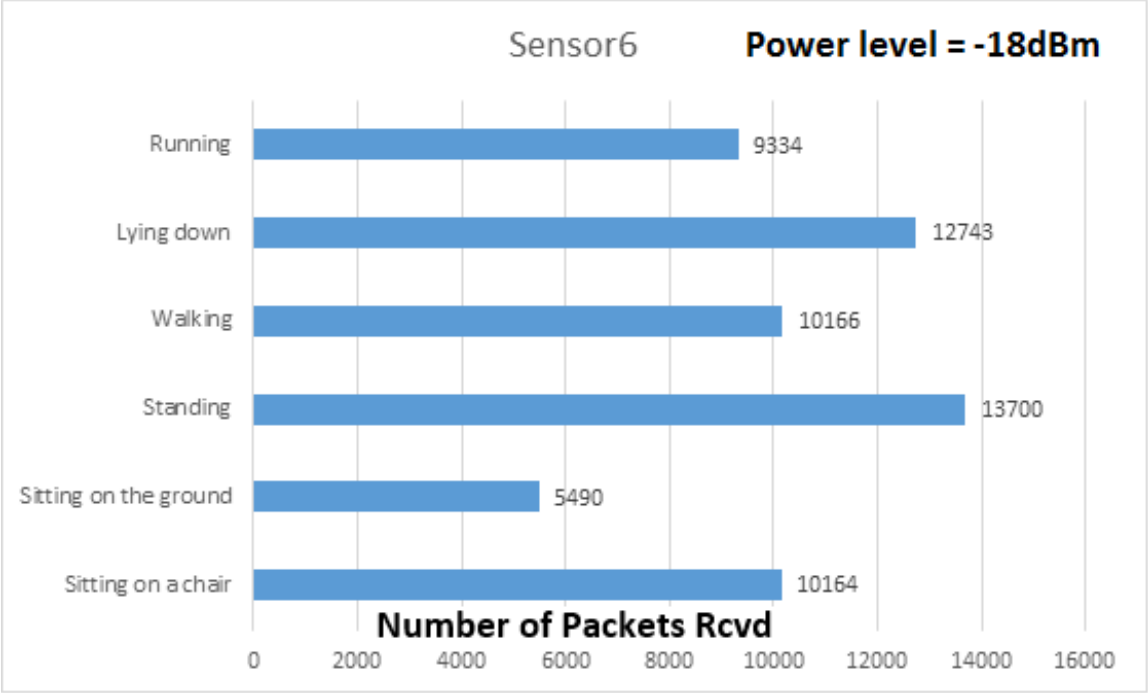


Figure 6.18: Packets received by Sensor6 at Power Level1

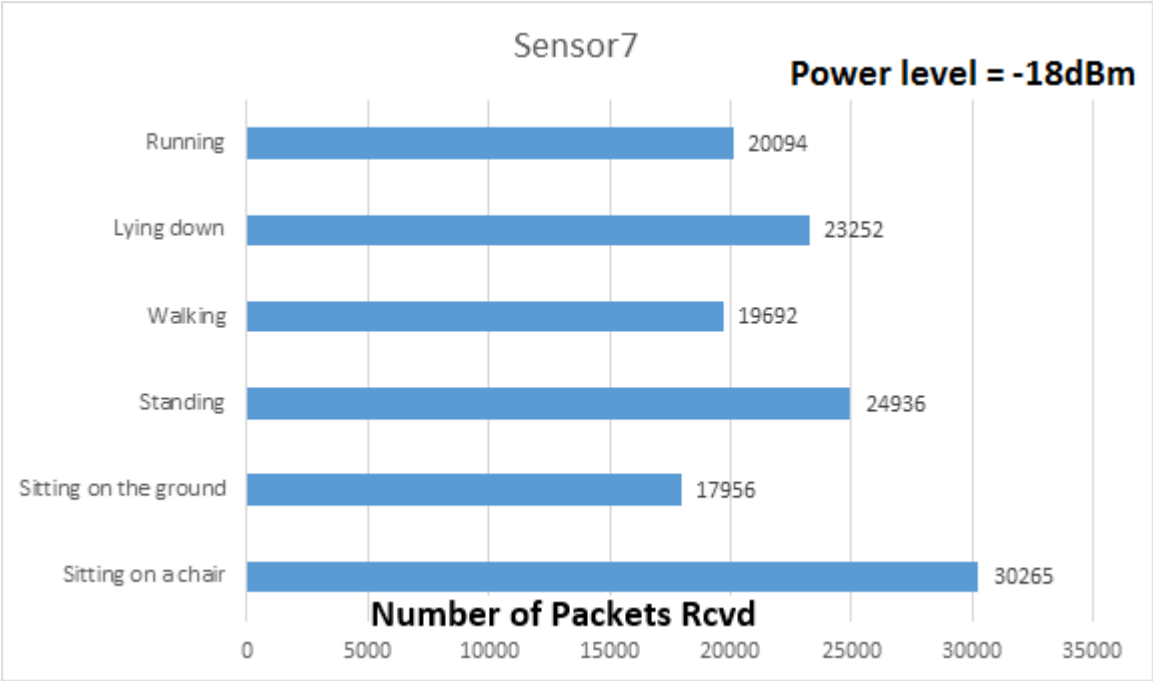


Figure 6.19: Packets received by Sensor7 at Power Level1

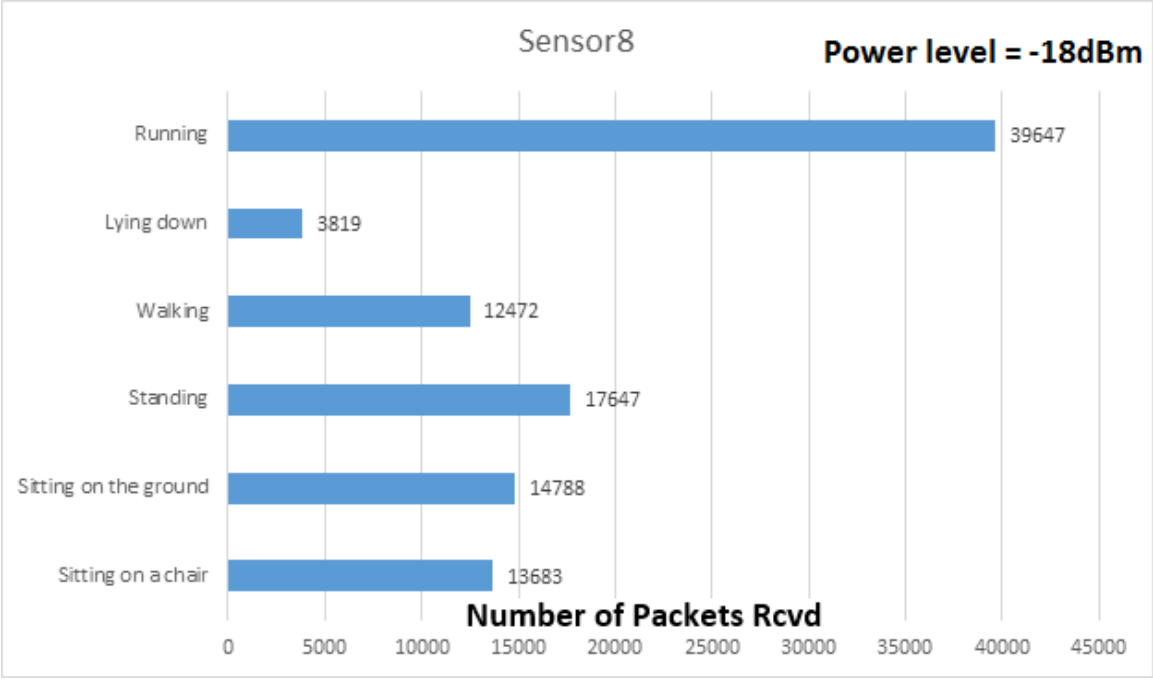


Figure 6.20: Packets received by Sensor8 at Power Level1

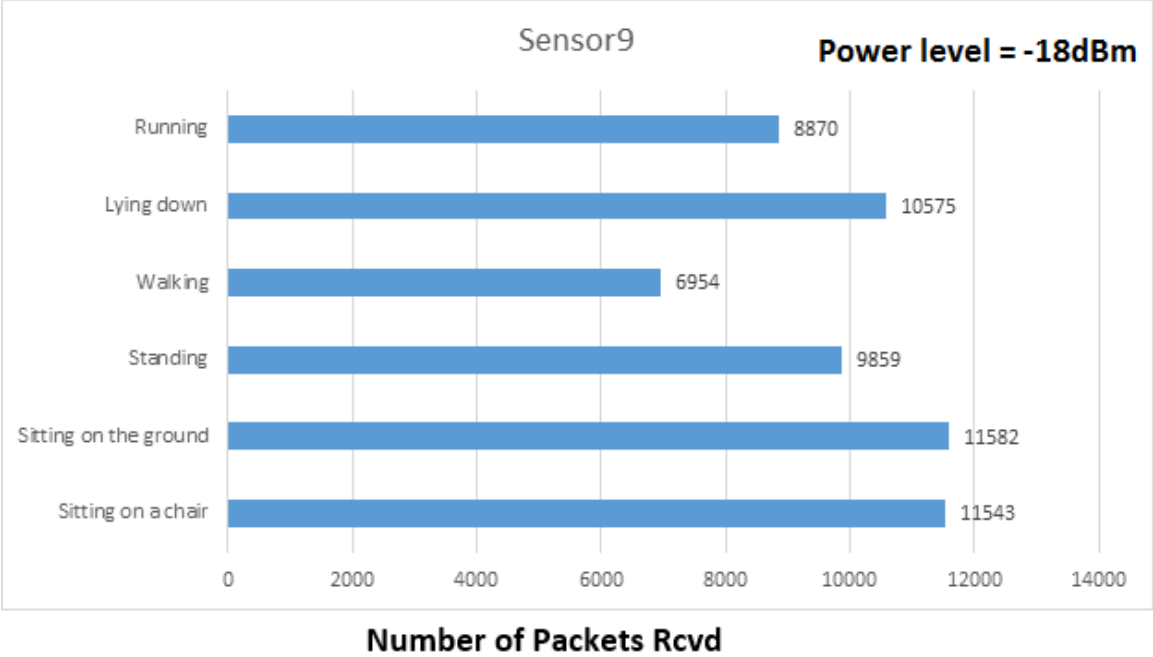


Figure 6.21: Packets received by Sensor9 at Power Level1

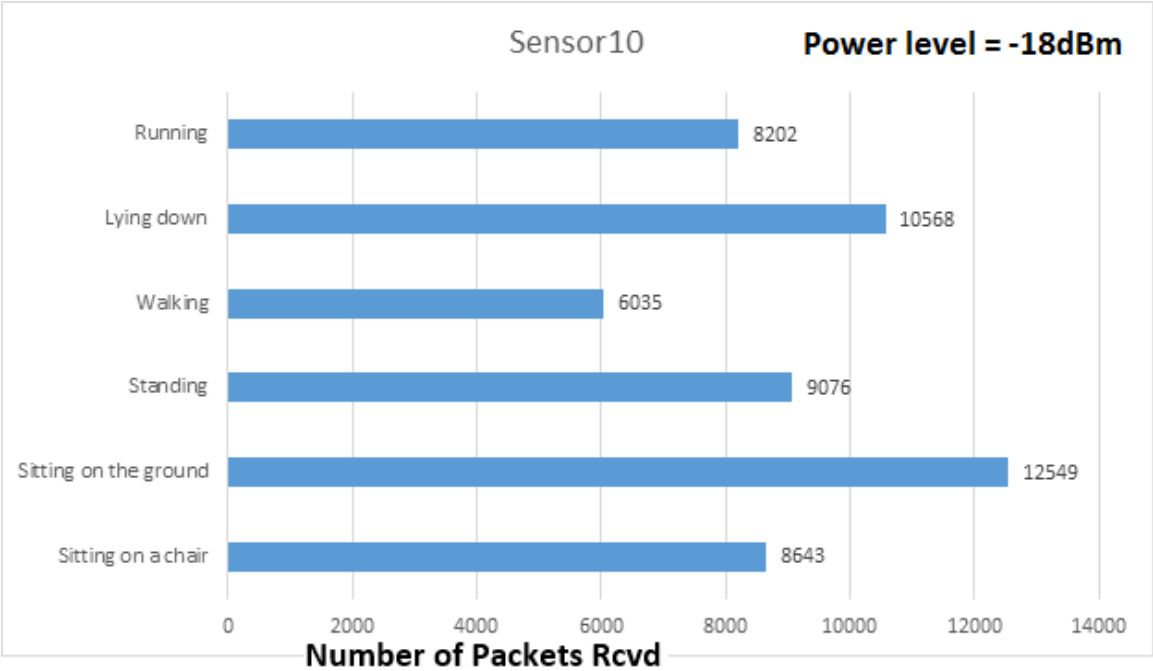


Figure 6.22: Packets received by Sensor10 at Power Level1

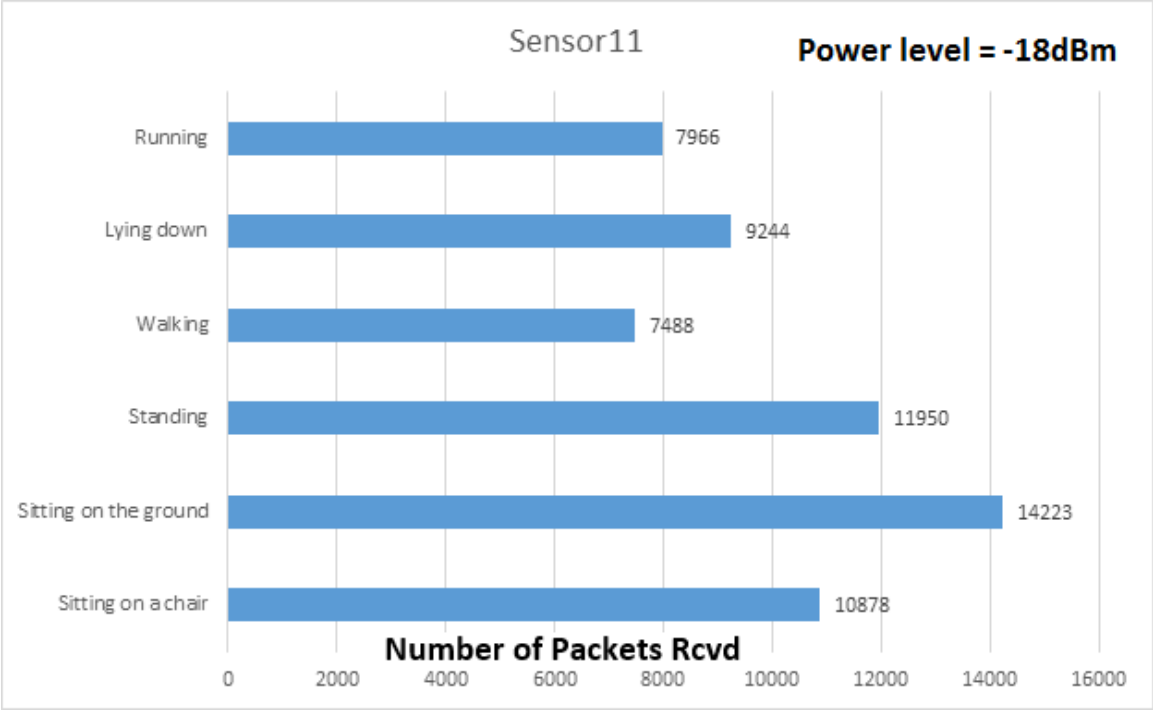


Figure 6.23: Packets received by Sensor11 at Power Level1

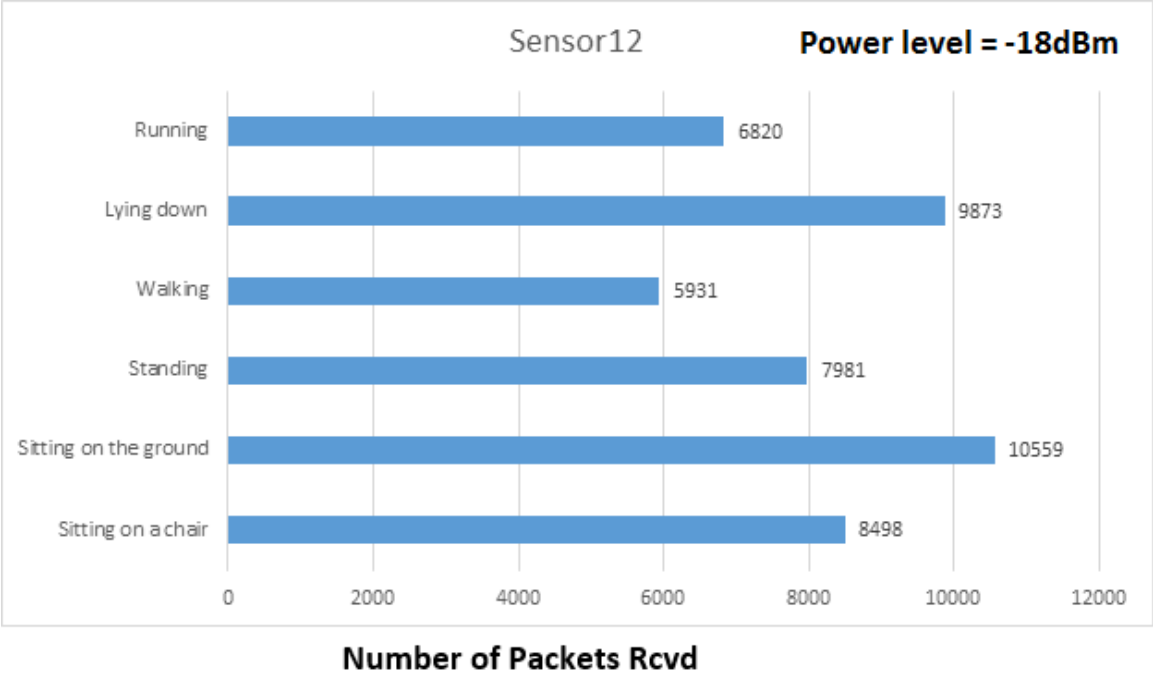


Figure 6.24: Packets received by Sensor12 at Power Level1

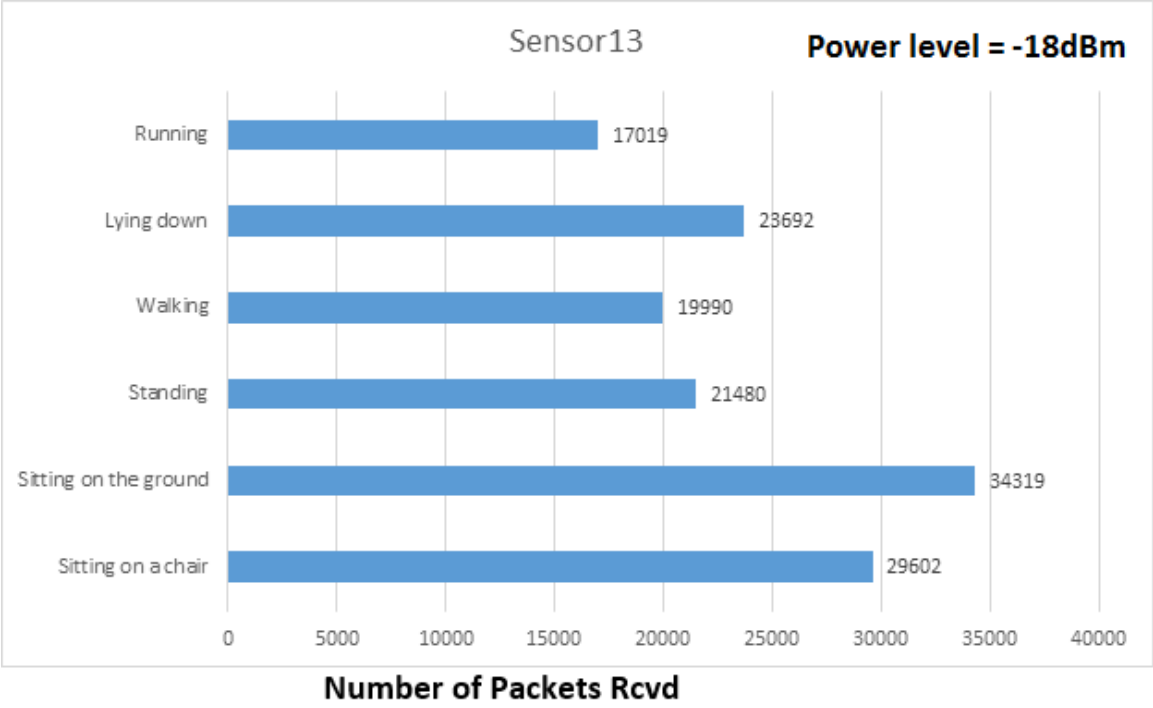


Figure 6.25: Packets received by Sensor13 at Power Level1

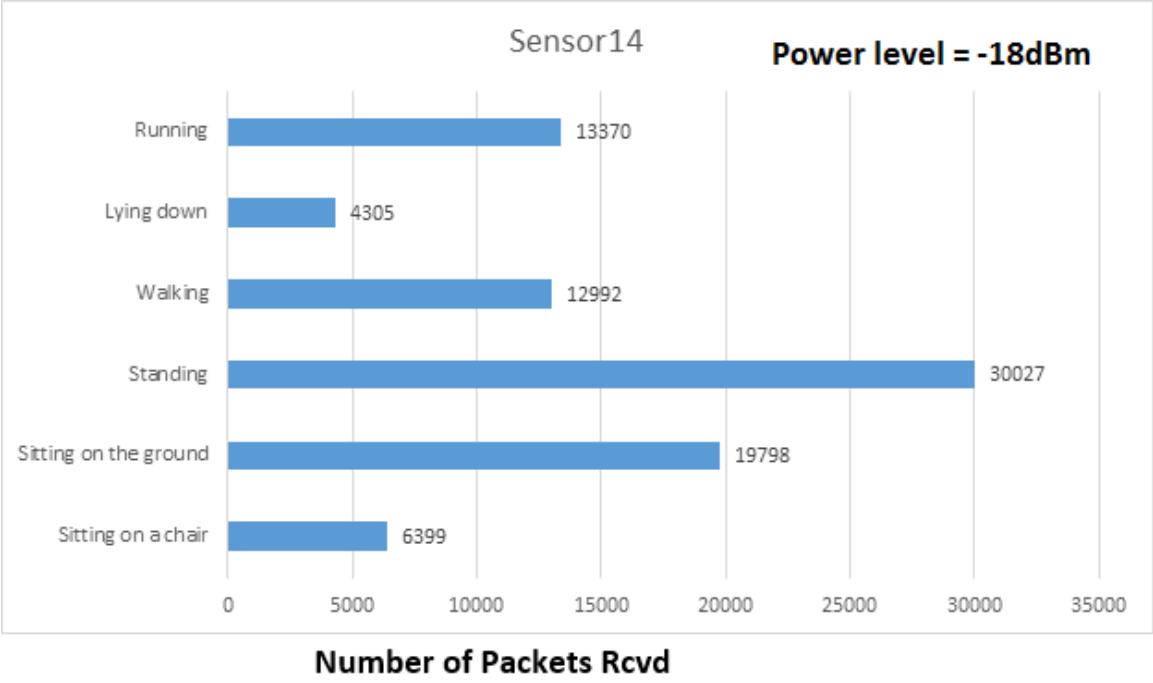


Figure 6.26: Packets received by Sensor14 at Power Level1

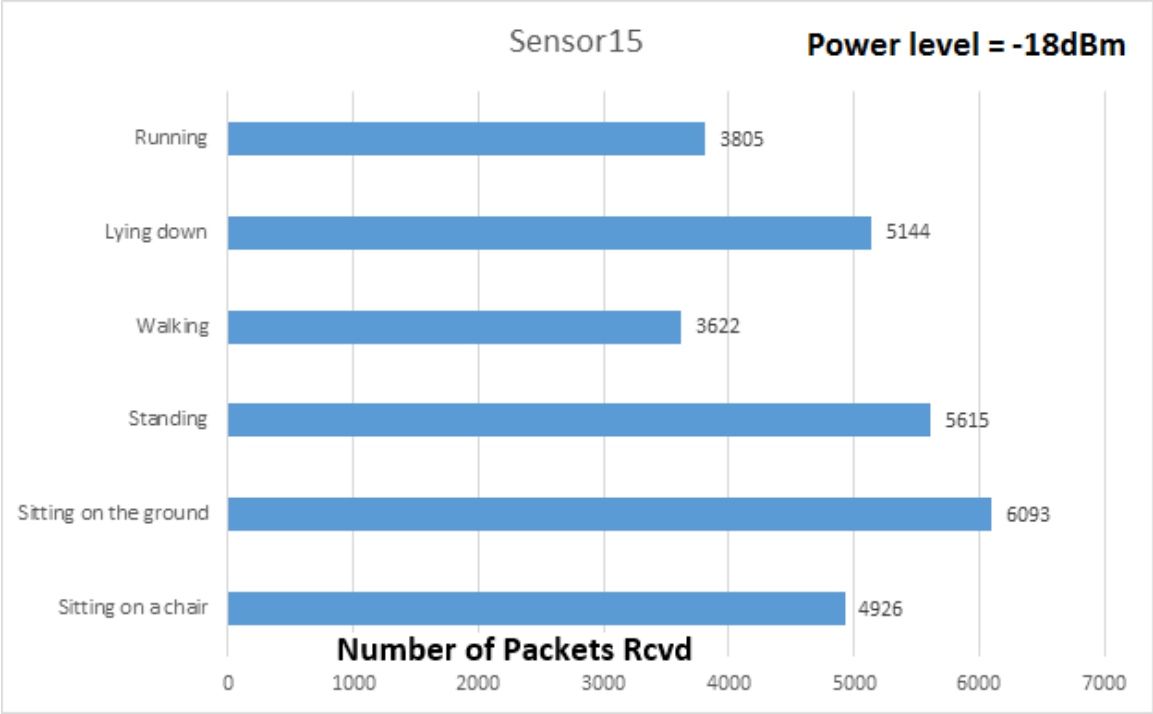


Figure 6.27: Packets received by Sensor15 at Power Level1

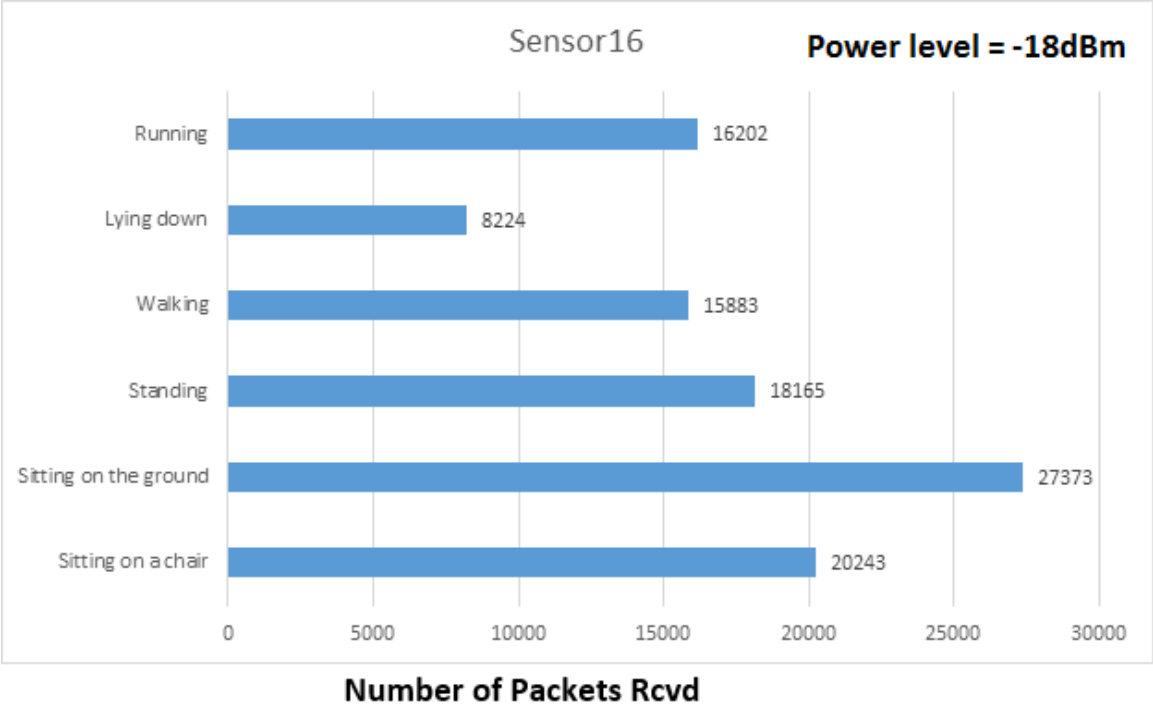


Figure 6.28: Packets received by Sensor16 at Power Level1

But these results might be misleading as we also have to take in consideration the spread of these packets among all the sensor nodes.

6.4.4 Markov Chain Model

We can use Markov Chain Discrete event model to define the discrete state of the human test subject. The mobility of a human test subject can be modeled as shown in Figure 6.31 with the give probability to move from posture to next one. Now we can assume this to be our initial model. Assuming this does not stay constant forever, we have to update the model dynamically depending on the location or mobility level of the test subject which can be a statistically learned value from our knowledge database.

Packets Received	Sitting on a chair	Sitting on the ground	Standing	Walking	Lying down	Running	Average
Sensor1	15120	5255	15438	10716	8948	9172	10775
Sensor2	8442	8716	5134	8490	9043	6699	7754
Sensor3	7491	336	10577	8140	4333	6813	6282
Sensor4	8753	4573	10484	7606	3277	6637	6888
Sensor5	11443	15125	11199	10414	9559	10203	11324
Sensor6	10164	5490	13700	10166	12743	9334	10266
Sensor7	30265	17956	24936	19692	23252	20094	22699
Sensor8	13683	14788	17647	12472	3819	39647	17009
Sensor9	11543	11582	9859	6954	10575	8870	9897
Sensor10	8643	12549	9076	6035	10568	8202	9179
Sensor11	10878	14223	11950	7488	9244	7966	10292
Sensor12	8498	10559	7981	5931	9873	6820	8277
Sensor13	29602	34319	21480	19990	23692	17019	24350
Sensor14	6399	19798	30027	12992	4305	13370	14482
Sensor15	4926	6093	5615	3622	5144	3805	4868
Sensor16	20243	27373	18165	15883	8224	16202	17682

Figure 6.29: Packets received by 16 sensors at Power Level1

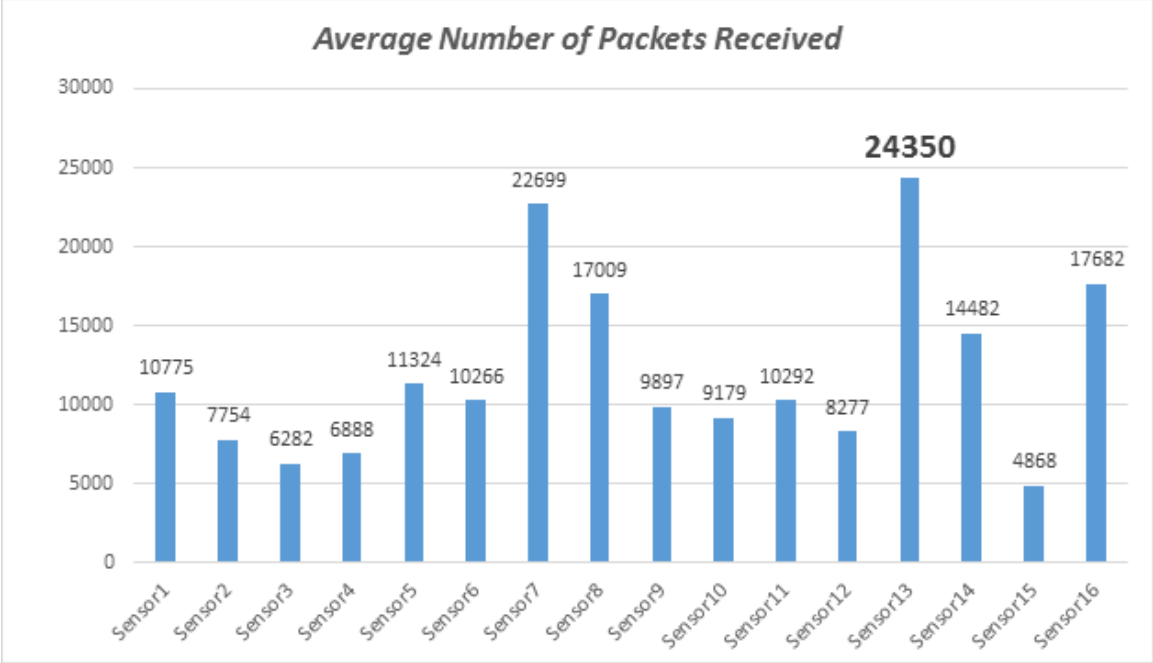


Figure 6.30: Number of packets received when taking an average over all 6 postures

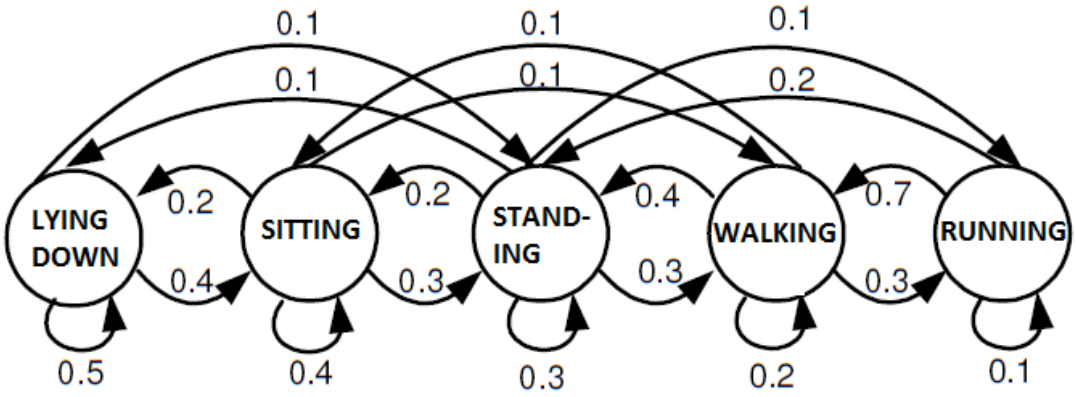


Figure 6.31: Markov Model for Body Posture

Chapter 7

Conclusions and Future Work

7.1 Network Trust Performance:

The trust value score was observed and recorded at various nodes in our network during the simulation. Attacker vs Normal behavior has been induced synthetically using already tagged packet injection at varying levels. Specifically 10, 50 and 100 percent levels. Figure 7.1 shows how the trust values converge over time. These results show our trust network scheme is very efficient in identifying malicious behavior and converges to expected values rapidly proportional to rate of observed malicious behavior. This Security and Trust performance was observed under the simulated Threat Model at 10,50 and 100 percent levels. Malicious and attacker traffic in a real life scenario will vary greatly. These threat traffic levels are used just to come up with a discrete model of malicious behavior for our simulation purposes.

Along the course of my studies at UC, this has been an incremental ongoing work which has shaped into a large endeavor accomplished in several independent units as reflected in individual chapters in this document. I have investigated multiple application specific networks independently and their border conditions with varying topologies. Namely, I have simulated a Body Area Network at one power level and six different postures. Further extended this to a complete mobility model with varying power levels. This was a foundation of an energy efficient smart body area network protocol.

Further, I have extended this similar approach for a VANET providing reliable, efficient and secure protocol. After I have designed all the modules individually for BAN, VANET and CLOUD, I have defined the

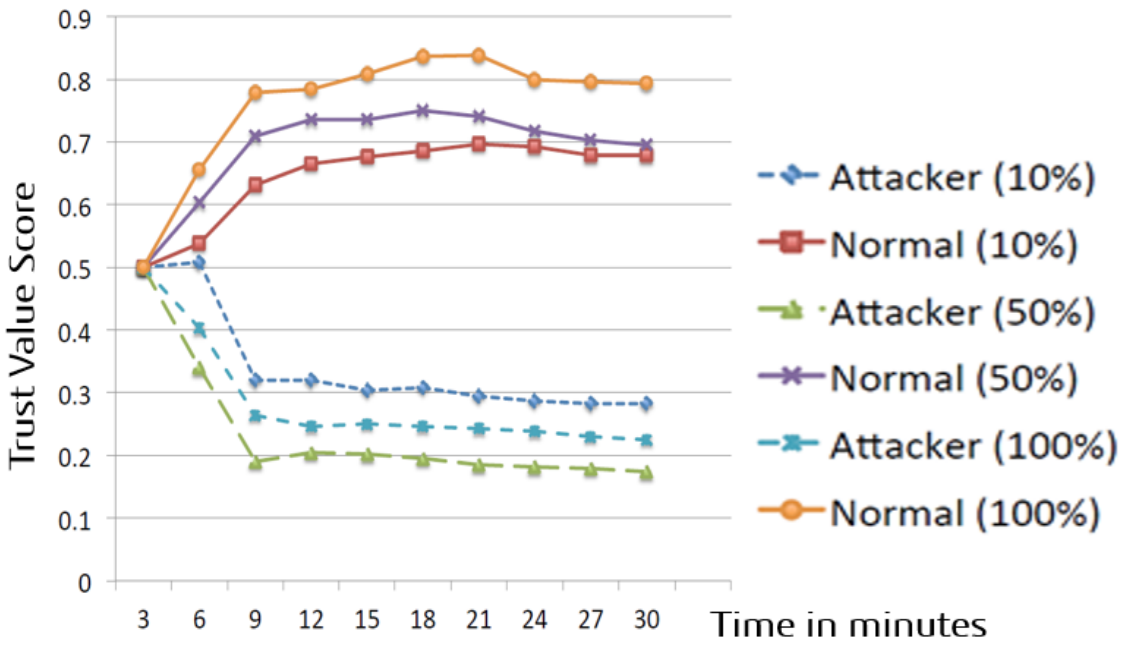


Figure 7.1: Network Trust Performance

Security and Privacy components of it. Once all the modules were designed and ready they were integrated together to generate the hybrid wireless mesh network that is efficient and secure to serve any kind of device be it IoT, BAN, VANET or a Cloud service client.

We have proposed a secure framework for a unified platform rendering seamless connectivity.

When such a secure ubiquitous network is established, we can develop various WPAN and VANET applications on top of such an infrastructure. Our framework also enforces an active security policy, addressing all eight domains defined under a standard comprehensive security policy.

Future work:

1. Security and Privacy concerns are dynamic.
2. Accurate Threat modeling.
3. Precise quantification of Security.
4. Specifically working on access control and packet filtering using firewalls.
5. Blockchain implementation for trust establishment in the network based on the bitcoin model.

Chapter 8

Bibliography

[1] J. Bae, H. Cho, K. Song, H. Lee, and H.-J. Yoo, "The signal transmission mechanism on the surface of human body for body channel communication," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 60, pp. 582–593, March 2012.

[2] Z.-y. Li, Y. Pang, J. Lin, J. Liu, S. Liu, and C.-y. Li, "Sar computation and channel modeling of body area networks," in *The 15th International Conference on Biomedical Engineering* (J. Goh, ed.), vol. 43 of *IFMBE Proceedings*, pp. 72–75, Springer International Publishing, 2014.

[3] P. Grifoni, F. Ferri, A. DAndrea, T. Guzzo, and A. Passarella, "Special issue on pervasive social computing," *Pervasive and Mobile Computing*, vol. 36, pp. 1 – 2, 2017. Special Issue on Pervasive Social Computing.

[4] V. Arnaboldi, M. G. Campana, F. Delmastro, and E. Pagani, "A personalized recommender system for pervasive social networks," *Pervasive and Mobile Computing*, vol. 36, pp. 3 – 24, 2017. Special Issue on Pervasive Social Computing.

[5] H. Flores, R. Sharma, D. Ferreira, V. Kostakos, J. Manner, S. Tarkoma, P. Hui, and Y. Li, "Social-aware hybrid mobile offloading," *Pervasive and Mobile Computing*, vol. 36, pp. 25 – 43, 2017. Special Issue on Pervasive Social Computing.

[6] D. Marr, "Artificial intelligencea personal view," *Artificial Intelligence*, vol. 9, no. 1, pp. 37 – 48, 1977.

[7] D. M. Mckeown, "The role of artificial intelligence in the integration of remotely sensed data with geographic information systems," *IEEE Transactions on Geoscience and Remote Sensing*, vol. GE-25, pp. 330–348, May 1987.

[8] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, MCC '12, (New York, NY, USA), pp. 13–16, ACM, 2012.

[9] T. G. Dietterich, "Ensemble methods in machine learning," in *Proceedings of the First International Workshop on Multiple Classifier Systems*, MCS '00, (London, UK, UK), pp. 1–15, Springer-Verlag, 2000.

[10] A. Mannini and A. M. Sabatini, "Machine learning methods for classifying human physical activity from on-body accelerometers," *Sensors*, vol. 10, no. 2, pp. 1154–1175, 2010.

[11] K. Kirkpatrick, "Software-defined networking," *Commun. ACM*, vol. 56, pp. 16–19, Sept. 2013.

[12] R. Weist, E. Eils, and D. Rosenbaum, "The influence of muscle fatigue on electromyogram and plantar pressure patterns as an explanation for the incidence of metatarsal stress fractures," *The American Journal of Sports Medicine*, vol. 32, no. 8, pp. 1893–1898, 2004.

[13] L. Lee and W. Grimson, "Gait analysis for recognition and classification," in *Automatic Face and Gesture Recognition, 2002. Proceedings. Fifth IEEE International Conference on*, pp. 148–155, May 2002.

[14] J. Jun and M. Sichitiu, "The nominal capacity of wireless mesh networks," *Wireless Communications, IEEE*, vol. 10, pp. 8–14, Oct 2003.

[15] S.-M. Cheng, P. Lin, D.-W. Huang, and S.-R. Yang, "A study on distributed/centralized scheduling for wireless mesh network," in *Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing*, IWCMC '06, (New York, NY, USA), pp. 599–604, ACM, 2006.

[16] J. Xie and X. Wang, "A survey of mobility management in hybrid wireless mesh networks," *Network, IEEE*, vol. 22, pp. 34–40, November 2008.

[17] M. Bahr, "Update on the hybrid wireless mesh protocol of ieee 802.11s," in *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE International Conference on*, pp. 1–6, Oct 2007.

[18] H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, pp. 164–171, June 2008.

[19] T. Zimmerman, "Personal area networks: Near-field intrabody communication," *IBM Systems Journal*, vol. 35, no. 3.4, pp. 609–617, 1996.

[20] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop, 2008. GCE '08*, pp. 1–10, Nov 2008.

[21] "Internet of things global standards initiative." `http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx`.

[22] L. Tan and N. Wang, "Future internet: The internet of things," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 5, pp. V5–376–V5–380, Aug 2010.

[23] D. Guinard, V. Trifa, and E. Wilde, "A resource oriented architecture for the web of things," in *Internet of Things (IOT), 2010*, pp. 1–8, Nov 2010.

[24] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless- and mobility-related view," *Wireless Communications, IEEE*, vol. 17, pp. 44–51, December 2010.

[25] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *Communications Surveys Tutorials, IEEE*, vol. 16, pp. 414–454, First 2014.

[26] Y. Yang, S. Zhu, G. Cao, and T. LaPorta, "An active global attack model for sensor source location privacy: Analysis and countermeasures," in *Security and Privacy in Communication Networks* (Y. Chen, T. Dimitriou, and J. Zhou, eds.), vol. 19 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 373–393, Springer Berlin Heidelberg, 2009.

[27] D. P. A. Abhinav Prakash, *Chapter 1: Data Security in Wired and Wireless Systems in Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. IGI Global, 1st ed., 2016.

[28] M. Nabi, M. Geilen, and T. Basten, "Moban: A configurable mobility model for wireless body area networks," in *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*, SIMUTools '11, (ICST, Brussels, Belgium, Belgium), pp. 168–177, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011.

[29] C. Kaufman, R. Perlman, and M. Speciner, *Network security : private communication in a public world*. Prentice Hall series in computer networking and distributed systems, Upper Saddle River (N. J.): Prentice Hall, 2002.

[30] Edney and W. A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11I*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2003.

[31] A. Bittau, M. Handley, and J. Lackey, "The final nail in wep's coffin," in *Security and Privacy, 2006 IEEE Symposium on*, pp. 15 pp.–400, May 2006.

[32] H. Hamed and E. Al-Shaer, "Taxonomy of conflicts in network security policies," *Communications Magazine, IEEE*, vol. 44, pp. 134–141, March 2006.

[33] J. Scambray, S. McClure, and G. Kurtz, *Hacking Exposed*. McGraw-Hill Professional, 2nd ed., 2000.

[34] M. E. Manley, C. A. McEntee, A. M. Molet, and J. S. Park, "Wireless security policy development for sensitive organizations," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, pp. 150–157, June 2005.

[35] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Upper Saddle River, NJ, USA: Prentice Hall Press, 5th ed., 2010.

[36] L. L. Peterson and B. S. Davie, *Computer Networks, Fifth Edition: A Systems Approach*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 5th ed., 2011.

[37] S. A. Hoseini-Tabatabaei, A. Gluhak, and R. Tafazolli, "A survey on smartphone-based systems for opportunistic user context recognition," *ACM Comput. Surv.*, vol. 45, pp. 27:1–27:51, July 2013.

[38] M. Robshaw and O. Billet, eds., *New Stream Cipher Designs: The eSTREAM Finalists*. Berlin, Heidelberg: Springer-Verlag, 2008.

[39] C. P. Pfleeger, "The fundamentals of information security," *IEEE Softw.*, vol. 14, pp. 15–16,60, Jan. 1997.

[40] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, Oct 1949.

[41] H. C. v. Tilborg, *Encyclopedia of Cryptography and Security*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005.

[42] D. Dolev, C. Dwork, and M. Naor, "Nonmalleable cryptography," *SIAM Review*, vol. 45, no. 4, pp. 727–784, 2003.

[43] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, pp. 2–21. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991.

[44] A. Biryukov, C. De Cannière, and M. Quisquater, *On Multiple Linear Approximations*, pp. 1–22. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004.

[45] J. Daemen and V. Rijmen, *The Design of Rijndael*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2002.

[46] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer Publishing Company, Incorporated, 1st ed., 2009.

[47] S. R. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of rc4," in *Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, SAC '01, (London, UK, UK), pp. 1–24, Springer-Verlag, 2001.

[48] O. Goldreich, *Foundations of Cryptography: Basic Tools*. New York, NY, USA: Cambridge University Press, 2000.

[49] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*. New York, NY, USA: Springer-Verlag New York, Inc., 2001.

[50] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (wep, wpa and wpa2/802.11i)," in *2009 2nd IEEE International Conference on Computer Science and Information Technology*, pp. 48–52, Aug 2009.

[51] B. Preneel, V. Rijmen, and A. Bosselaers, "Recent developments in the design of conventional cryptographic algorithms," in *State of the Art in Applied Cryptography, Course on Computer Security and Industrial Cryptography - Revised Lectures*, (London, UK, UK), pp. 105–130, Springer-Verlag, 1998.

[52] G. Z. Gurkas, A. H. Zaim, and M. A. Aydin, "Security mechanisms and their performance impacts on wireless local area networks," in *2006 International Symposium on Computer Networks*, pp. 1–5, 2006.

[53] K. G. Paterson and G. J. Watson, "Immunising cbc mode against padding oracle attacks: A formal security treatment," in *Proceedings of the 6th International Conference on Security and Cryptography for Networks*, SCN '08, (Berlin, Heidelberg), pp. 340–357, Springer-Verlag, 2008.

[54] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory (2Nd Edition)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2005.

[55] J. Katz and Y. Lindell, *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007.

[56] X. Huang, P. G. Shah, and D. Sharma, "Protecting from attacking the man-in-middle in wireless sensor networks with elliptic curve cryptography key exchange," in *2010 Fourth International Conference on Network and System Security*, pp. 588–593, Sept 2010.

[57] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine*, vol. 43, pp. S23–S30, Sept 2005.

[58] A. Ghosh, D. R. Wolter, J. G. Andrews, and R. Chen, "Broadband wireless access with wimax/802.16: current performance benchmarks and future potential," *IEEE Communications Magazine*, vol. 43, pp. 129–136, Feb 2005.

[59] Q. F. Hassan, A. M. Riad, and A. E. Hassan, "Understanding cloud computing," *Software Reuse in the Emerging Cloud Computing Era*, pp. 204–227, 2012.

[60] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Media, Inc., 2009.

[61] B. A. Sullivan, "Securing the cloud: Cloud computer security techniques and tactics," *Security Journal*, vol. 27, no. 3, pp. 338–340, 2014.

[62] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *2010 Proceedings IEEE INFOCOM*, pp. 1–9, March 2010.

[63] G. Jakimoski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, pp. 163–169, Feb 2001.

[64] P. F. Syverson, D. M. Goldschlag, and M. G. Reed, "Anonymous connections and onion routing," in *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)*, pp. 44–54, May 1997.

[65] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, Nov 1994.

[66] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, pp. 54–62, Oct 2002.

[67] J. Kong, Z. Petros, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," in *Proceedings Ninth International Conference on Network Protocols. ICNP 2001*, pp. 251–260, Nov 2001.

[68] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless- and mobility-related view," *IEEE Wireless Communications*, vol. 17, pp. 44–51, December 2010.

[69] A. Smailagic and D. Kogan, "Location sensing and privacy in a context-aware computing environment," *IEEE Wireless Communications*, vol. 9, pp. 10–17, Oct 2002.

[70] Y. C. Abhinav Prakash, Dharma P. Agrawal, "Network coding combined with onion routing for anonymous and secure communication in a wireless mesh network," *International Journal of Computer Networks and Communications*, vol. 6, pp. 1–14, November 2014.

[71] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. Agrawal, "Wireless mesh networks: Current challenges and future directions of web-in-the-sky," *Wireless Communications, IEEE*, vol. 14, pp. 79 –89, august 2007.

[72] Y. Zhou and Y. Fang, "Security of ieee 802.16 in mesh mode," in *Military Communications Conference, 2006. MILCOM 2006. IEEE*, pp. 1 –6, oct. 2006.

[73] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02, (New York, NY, USA), pp. 41–47, ACM, 2002.

[74] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pp. 197 – 213, may 2003.

[75] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques*, (New York, NY, USA), pp. 335–338, Springer-Verlag New York, Inc., 1985.

[76] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *CRYPTO*, pp. 471–486, 1992.

[77] Y. Cheng and D. Agrawal, "Efficient pairwise key establishment and management in static wireless sensor networks," in *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*, pp. 7 pp. –550, nov. 2005.

[78] A. Gaur, A. Prakash, S. Joshi, and D. P. Agrawal, "Polynomial based scheme (pbs) for establishing authentic associations in wireless mesh networks," *Journal of Parallel and Distributed Computing*, vol. 70, no. 4, pp. 338 – 343, 2010.

[79] Y. Cheng, M. Malik, B. Xie, and D. P. Agrawal, "Enhanced approach for random key pre-distribution in wireless sensor networks," in *Proceedings of International Conference on Communication, Networking and Information Technology*, 2008.

[80] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Onion routing network for securely moving data through communication networks," 07 2001.

[81] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 7, pp. 1302–1311, 2012.

[82] Z. Wan, K. Ren, B. Zhu, B. Preneel, and M. Gu, "Anonymous user communication for privacy protection in wireless metropolitan mesh networks," *Vehicular Technology, IEEE Transactions on*, vol. 59, pp. 519–532, Feb 2010.

[83] K. Vu, R. Zheng, and J. Gao, "Efficient algorithms for k-anonymous location privacy in participatory sensing," in *INFOCOM, 2012 Proceedings IEEE*, pp. 2399–2407, March 2012.

[84] X. Wu and N. Li, "Achieving privacy in mesh networks," in *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, SASN '06, (New York, NY, USA), pp. 13–22, ACM, 2006.

[85] R. Li, L. Pang, Q. Pei, and G. Xiao, "Anonymous communication in wireless mesh network," in *Computational Intelligence and Security, 2009. CIS '09. International Conference on*, vol. 2, pp. 416 –420, dec. 2009.

[86] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *Information Theory, IEEE Transactions on*, vol. 52, pp. 4413–4430, Oct 2006.

[87] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "Xors in the air: Practical wireless network coding," *Networking, IEEE/ACM Transactions on*, vol. 16, pp. 497–510, June 2008.

[88] P. Zhang, C. Lin, Y. Jiang, P. P. C. Lee, and J. C. S. Lui, "Anoc: Anonymous network-coding-based communication with efficient cooperation," *IEEE Journal on Selected Areas in Communications*, pp. 1738–1745, 2012.

[89] L. Chen, S. L. Ng, and G. Wang, "Threshold anonymous announcement in vanets," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 605–615, March 2011.

[90] T. Cui, L. Chen, and T. Ho, "Energy efficient opportunistic network coding for wireless networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, April 2008.

[91] J. C. Corena, A. Basu, S. Kiyomoto, Y. Miyake, and T. Ohtsuki, "Xor network coding pollution prevention without homomorphic functions," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, pp. 293–300, Jan 2014.

[92] A. Prakash, A. Gaur, and D. P. Agrawal, "Multilevel onion tree routing for anonymous and secure communication in a wireless mesh," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 3, January 2013.

[93] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on*, pp. 599 –608, june 2005.

[94] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," *Mobile Computing, IEEE Transactions on*, vol. 11, pp. 320 –336, feb. 2012.

[95] Y. Wang and D. P. Agrawal, "Optimizing sensor networks for autonomous unmanned ground vehicles," 2008.

[96] D. Agrawal, A. Prakash, S. Chakraborty, A. Jamthe, and S. Ghosh, "System and method for real-time personnel fatigue level monitoring," Dec. 1 2016. US Patent App. 14/846,851.

[97] "Frequency of injury among college athletes." http://www.livestrong.com/article/513231-frequency-of-injury-among-college-athletes/.

[98] "Barefoot running: Avoid injury by changing our way of running." http://www.buenaforma.org/2014/03/13/barefoot-running/.

[99] G. Gobbi, D. Galli, C. Carubbi, A. Pelosi, M. Lillia, R. Gatti, V. Queirolo, C. Costantino, M. Vitale, M. Saccavini, M. Vaccarezza, and P. Mirandola, "Assessment of body plantar pressure in elite athletes: an observational study," *Sport Sciences for Health*, vol. 9, no. 1, pp. 13–18, 2013.