VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JNANA SANGAMA", BELAGAVI-590018

2020–2021

B.L.D.E. ASSOCIATION'S

VACHANA PITAMAHA DR. P.G. HALAKATTI COLLEGE OF ENGINEERING & TECHNOLOGY

VIJAYAPUR – 586103

Project
Report

On

"AN INTRUSION DETECTION SYSTEM FOR IOT BASED APPLICATION"

Submitted in partial fulfilment for the award of the degree of

BACHELOR OF ENGINEERING

In

ELECRONICS AND COMMUNICATION ENGINEERING

UNDER THE GUIDANCE OF
Prof.ABID.H.SYED

Submitted By

Mohummad Gous Sadiq Ahmed Killedar **[2BL16EC053]**

Mohammed Shahabuddin Chatterki **[2BL18EC411]**

B.L.D.E. ASSOCIATION'S

VACHANA PITAMAHA DR. P.G. HALAKATTI COLLEGE OF ENGINEERING & TECHNOLOGY

VIJAYAPUR - 586103

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that the project work entitled **"**An Intrusion Detection System For Iot Based Application**"** carried out by Mohummad.G.Sadiq Ahmed Killedar [2BL16EC053],Mohammad Shahabuddin Chatterki [2BL18EC411], Vishwanath Jagadev Benakanahalli [2BL18EC421],Sunlikumar

N Dodamni [2BL17EC088] are bonafide students of BLDEA's V. P. Dr. P. G. Halakatti College of Engineering and Technology in partial fulfilment for the award of "BACHELOR OF ENGINEERING" in ELECTRONICS

AND COMMUNICATION as prescribed by VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI during the academic year 2020-2021. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the Report deposited in the Departmental library. The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said Degree.

GUIDE	H.O.D	PRINCIPAL
Prof.Abid.H.Syed	Dr. Umesh. D. Dixit	Dr. Atul. Ayare

ACKNOWLEDGEMENT

We express our gratitude to **Dr. Atul. Ayare**, Principal, BLDEA's V. P. Dr. P. G. Halakatti College of Engineering and Technology, for providing us an excellent facilities and academic ambience.

We extend our sincere thanks to **Dr. Umesh. D. Dixit**, Head of the Department, ECE; for providing all the facilities and fostering a congenial academic environment in the department.

We feel deeply indebted to our esteemed guide **Prof.Abid.H.Syed,** for the help, right from the conception and visualization to the very presentation of the project. He has been our guiding light throughout.

We would like to take this opportunity to thank all the faculty members and supporting staff for helping to complete this project.

Last but not the least we would like to thank our parents, friends and well wishers who have helped us directly or indirectly.

Mohummad Gous Sadiq Ahmed Killedar

Mohammed Shahabuddin Chatterki

ABSTRACT

We are currently living in an era where smart devices and other wireless handheld devices are changing our environment, making it more interactive, adaptive and informative, forming "Internet of Things (IOT)" which is an emerging technology that has revolutionized, the network in the global world.

Since IOT innovation is advancing and providing diverse smart solutions and applications, from E-transport to E-health, smart living, to E-manufacturing and many other E-solutions related to industries. As anything connected to the internet, IOT & IIOT devices are subject to cyber threats. These include attacks on industrial control systems such as distributed control systems (DCS), programmable logic controllers (PLC), supervisory control and data acquisition (SCADA) systems etc. Security threats like vulnerabilities, data manipulation, stealing, device manipulation, hacking and these risks are exponentially greater. Therefore, we present a Cybersecurity Solution based on Intrusion Detection System to detect malicious activity occurring in the networks of IOT based applications. In this paper we present a novel method based ON vulnerability assessment and attack model in different layer, with feature and learning from parsed protocol with additional data including malware samples. Moreover, we developed a cyber-attack model and algorithm that included a classification and visualization process. Finally, the results of the experimental implementation show that our proposed Cybersecurity Solution based on IDS was able to detect and prevent attacks in real time in an IoT-based Application

CONTENTS

CHAPTER-1
INTRODUCTION

Internet is among the most important inventions of the century which has affected our lives. Today internet has crossed every barrier and have changed the way we use to talk, work, manage business and industrial reforms. The technology have reached to an extent that we don't even require a computer for using internet. Now we have internet enabled smartphone and palmtops etc , but this advancement of technology also brings a exponentially greater concern for security and privacy of industries, organizations and individuals. As a large number of data is collected by various devices and transmitted from one device to another, and as these large numbers of devices are connected with each other and to the world network and the number is increasing every day, there is a major risk of security threat, vulnerabilities, data manipulation, stealing, identity, device manipulation, and hacking. Therefore it is very crucial address these security risks, which is diligently handle by Cyber security.

When we talk about cyber security / security it involves these key features:

• Confidentiality: Confidentiality Assurance that information is shared only among authorized persons or organizations.

• Integrity: Integrity In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

• Availability: Availability of information refers to ensuring that authorized parties are able to access the information when needed

1.1.1 WHAT IS CYBER SECURITY?

Cybersecurity encompasses methods used to restrict unauthorized access to devices, networks, and data; it protects tools and technologies used to store data.

1.1.2 Types of Cyber Security :

• Information security: Information security protects your information from unauthorized access, identity theft and protects the privacy of information and hardware that use, store and transmit data. Examples of Information security: Authorization of user and Cryptography.

• Network security: Network security protects the usability, integrity and safety of a network and protects network traffic by controlling incoming and outgoing connections to prevent threats from entering or spreading on the network.

• Application security: Application security protects applications from threats that occur due to the flaws in application design, development, installation, upgrade or maintenance phases.

• Date Loss Prevention (DLP): Protects data by focusing on the location, classification and monitoring of information at rest, in use and in motion.

• Cloud security: Provides protection for data used in cloud-based services and applications.

• Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS): work to identify potentially hostile cyber activity.

General Classification of Security Attacks:

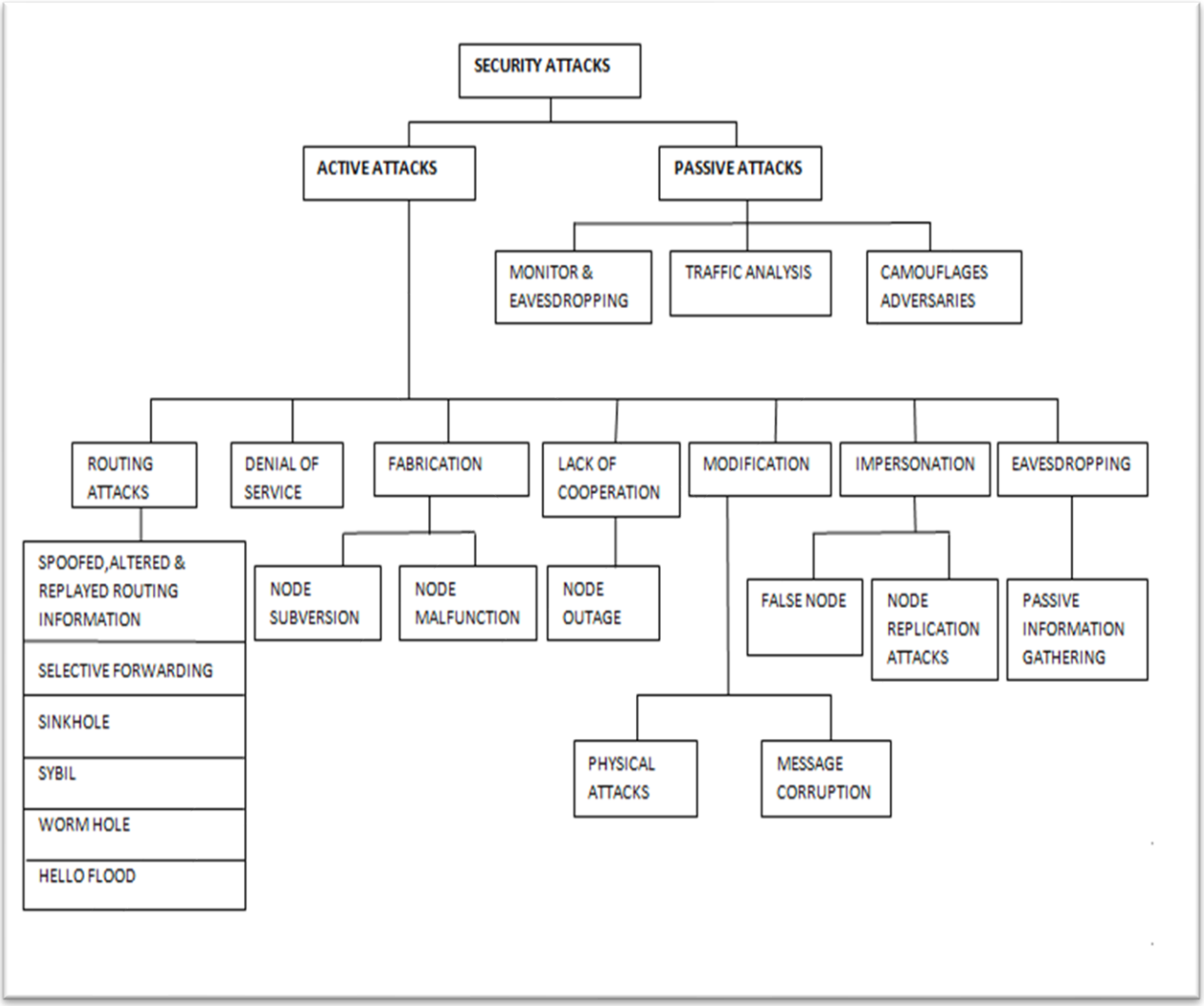


Fig 1.1

The active and passive attacks both fall in the family of security attacks, with a few underlying points that differentiate them. Security attacks are typically computer attacks that jeopardize the security of the system. These security attacks are further classified into active attacks and passive attacks

1.1.3 Active attacks : Active attacks are attacks in which the hacker attempts to change or transform the content of messages or information. These attacks are a threat to the integrity and availability of the system. Due to these attacks, systems get damaged, and information can be altered. The prevention of these attacks is difficult due to their high range of physical and software vulnerabilities. The damage that is done with these attacks can be very harmful to the system and its resources.

The good thing about this type of attack is that the victim is notified about the attack. So, instead of prevention, the paramount importance is laid on detecting the attack and restoration of the system from the attack. An active attack typically requires more effort and generally have more difficult implication.

1.1.4 Passive attacks: Passive attacks are the ones in which the attacker observes all the messages and copy the content of messages or information. They focus on monitoring all the transmission and gaining the data. The attacker does not try to change any data or information he gathered. Although there is no potential harm to the system due to these attacks, they can be a significant danger to your data's confidentiality.

Unlike the Active attacks, these are difficult to detect as it does not involve alteration in data or information. Thus, the victim doesn't get any idea about the attack. Although it can be prevented using some encryption techniques. In this way, at any time of transmission, the message is in indecipherable form, so that hacker could not understand it. So this is the reason why more emphasis is given to prevention than detection.

Difference between active and passive attacks in network security are listed down below:

- In active attacks, modification of messages is done, but on the other hand, in passive attacks, the information remains unchanged.
- The active attack causes damage to the integrity and availability of the system, but passive attacks cause damage to data confidentiality.
- In active attacks, attention is given to detection, while in the other one, attention is given to prevention.
- The resources can be changed in active attacks, but passive attacks have no impact on the resources.
- The active attack influences the system services, but the information or data is acquired in passive attacks.
- Inactive attacks, information is gathered through passive attacks to attack the system, while passive attacks are achieved by collecting confidential information such as private chats and passwords.

CHAPTER -2

LITERATURE SURVEY

This section describes the work:

• In this paper [1] we aim to evaluate the newest techniques of operation in abnormality-based IDS in Intrusion Detection and security achievement in AMI against signature-based IDS operation with the use of standard criteria in equal situations experimentally. According to the results from this research we can see that the signature-based methods are not useful in IDS systems applied in AMI network. The measurement on anomaly-based IDS which is using data mining techniques showed very hopeful results. However these methods need some improvements in order to achieve their best place.

• In this paper[2] the author describes about Cyber Security in IOT Application and Service Domains , IOT is advancing and provides diverse smart solutions or application ,from e- transport to e-health ;smart living to e-manufacturing and many other e-solutions. In this environment the rising cyber attacks on system infrastructure coupled system inherent vulnerabilities presents a source of concern need to be addressed in order to ensure user confidence so as to promote wide acceptance and reap the potentials of paper looks at some of the major IOT application and service domains, and analyse the cyber security challenges which are likely to drive IOT research in the future.

• Yang et al. [3] proposed a security scheme in IOT-based healthcare systems. In this research, they proposed a self-adaptive access control together with a privacy-preserving smart IOT-based healthcare big data storage system. Further security approaches have been developed for IOT systems.

• In this paper[4], the impact of three different possible cyber events on physical power grid have been analysed using an integrated cyber-power modelling and simulation testbed. Real-time modelling of end-to-end cyber power systems have been developed with hardware-in-the-loop capabilities. Real-Time Digital Simulator (RTDS), synchro phasor devices, DeterLab, and Network Simulator-3 (NS-3) are utilized in this developed testbed. DeterLab can be used to model real-life cyber events in the developed cyber-physical testbed. Man-in-the-middle and denial-of-service attacks have been modelled as specific cases for IEEE standard test cases. Additionally, communication failure impact on the power grid has been analysed using the tested.

• In this paper[5], we will first present our analysis of Duqu, an information-collecting malware sharing striking similarities with Stuxnet. We describe our contributions in the investigation ranging from the original detection of Duquvia finding the dropper file to the design of a Duqu detector toolkit. We then continue with the analysis of the Flame advanced information-gathering malware.

• In this paper[6], we survey the various types of buffer overflow vulnerabilities and attacks, and survey the various defensive measures that mitigate buffer overflow vulnerabilities, including our own StackGuard method. We then consider which combinations of techniques can eliminate the problem of buffer overflow vulnerabilities, while preserving the functionality and performance of existing systems.

• This paper[7] proposed a software buffer overflow vulnerability prediction method by using software metrics and a *decision tree* algorithm. First, the software metrics were extracted from the software source code, and data from the dynamic data stream at the functional level was extracted by a data mining method. Second, a model based on a *decision tree* algorithm was constructed to measure multiple types of buffer overflow vulnerabilities at the functional level.

Finally, the experimental results showed that our method ran in less time than *SVM, Bayes, adaboost, and random forest* algorithms and achieved 82.53% and 87.51% accuracy in twodifferent data sets. The method presented in this paper achieved the effect of accurately predicting software buffer overflow vulnerabilities in C/C++ and Java programs.

• This paper[7] include vast idea and information regarding the buffer overflow as history of Vulnerabilities, buffers, stack, registers, Buffer Overflow Vulnerabilities and Attacks, current buffer over flow, Shell code, Buffer Overflow Issues, the Source of the Problem, prevention/detection of Buffer Overflow attacks and Finally how to react towards Buffer Overflows. The objective of this study is to take one inside the buffer overflow attack and bridge the gap between the "descriptive account" and the "technically intensive account".

• In this paper[8] the author said Supervisory Control and Data Acquisition (SCADA) systems are deeply ingrained in the fabric of critical infrastructure sectors. These computerized real-time process control systems, over geographically dispersed continuous distribution operations, are increasingly subject to serious damage and disruption by cyber means due to their standardization and connectivity to other networks. However, SCADA systems generally have little protection from the escalating cyber threats. In this paper [9] explain the technological challenges for the SCADA security and overview the approaches which address these challenges. Then we focus on the security protocol which has been proposed in the SCADA cyber security initiatives and implementation issues when the both security function and the communication function are implemented on the embedded system devices in future power grid including the SCADA network.

• In this paper [10]authors DNP Users Group [Volume 2]Distributed Network Protocol 3 (DNP3) is a set of communication protocol used between components in process automation systems. Its main use is in utilities such as electric and water companies. Usage in other industries is not common. It was developed for communications between various types of data acquisition and control equipment. It plays a crucial role in SCADA systems, where it is used by SCADA Master Stations Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). It is primarily used for communications between a master station and RTUs or IEDs. ICCP, the Inter-Control Center Communications Protocol), is used for inter-master station communications.

• This paper[11] presents a distributed intrusion detection system (DIDS) for supervisory control and data acquisition (SCADA) industrial control systems, which was developed for the CockpitCI project. Its architecture was designed to address the specific characteristics and requirements for SCADA cybersecurity that cannot be adequately fulfilled by techniques from the information technology world, thus requiring a domain-specific approach.

• In this paper authors Musa, S. Aborujilah.[12] study In the initial structure of SCADA there is no security mechanism that prevents or detects the attacks in SCADA communication network. SCADA technology is not new but was deployed in limited networks; currently these systems have been deployed and accessible by many networks such as LAN/WAN, Mobile networks, Web Browsers and GPRS through internet technology. Using Modern communication facilities SCADA systems are vulnerable from different types of internet attacks that create major security problems for SCADA communication.

• In this paper[13] authors Chen, X.; Li, A.; Zeng, X.; Guo, W.; Huang, G[2] we study about The internet of things (IoT) attracts great interest in many application domains concerned with monitoring and control of physical phenomena. However, application development is still one of the main hurdles to a wide adoption of IoT technology. Application development is done at a low level, very close to the operating system and requires programmers to focus on low-level system issues.

• In this page[14] consider a potential gray hole attack against SCADA substation to control centre communications using DNP3. We propose a support vector machine-based traffic analysis algorithm that relies on message direction and timing information only, and we use trace-based simulations to show that even if SCADA traffic is sent through an encrypted tunnel, as often done in practice, the gray hole attack can be effectively performed based on the timing and direction of three consecutive messages.

• In this paper[15] authors DNP Users Group [1-2]Distributed Network Protocol (DNP3) is the predominant SCADA protocol in the energy sector – more than 75% of North American electric utilities currently use DNP3 for industrial control applications. This paper presents a taxonomy of attacks on the protocol. The attacks are classified based on targets (control center, outstation devices and network/communication paths) and threat categories (interception, interruption, modification and fabrication).

• In this paper[16] author Fu-Hau Hsu [1-6] Buffer overflow attack is the main attack method that most if not all existing malicious worms use to propagate themselves from machine to machine. Although a great deal of research has been invested in defense mechanisms against buffer overflow attack, most of them require modifications to the network applications and/or the platforms that host them.

Being an extension work of CTCP, this paper presents a network-based low performance overhead buffer overflow attack detection system called Nebula, which can detect both known and zero-day buffer overflow attacks based solely on the packets observed without requiring any modifications to the end hosts.

• In this paper[17] ,the author present an Intrusion Detection System (IDS) [1-3], by applying genetic algorithm (GA) to efficiently detect various types of network intrusions. Parameters and evolution processes for GA are discussed in details and implemented. This approach uses evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity. To implement the author used KDD99 benchmark dataset and obtained reasonable detection rate.

• In this paper[18], the author use RST (Rough Set Theory) and SVM (Support Vector Machine) to detect intrusions at pg[1-6]. First, RST is used to preprocess the data and reduce the dimensions. Next, the features were selected by RST will be sent to SVM model to learn and test respectively. The method is effective to decrease the space density of data. The experiments will compare the results with different methods and show RST and SVM schema could improve the false positive rate and accuracy.

• In this paper[19] author propose a hierarchical architectural design based intrusion detection system that fits the current demands and restrictions of wireless ad hoc sensor network. In this proposed intrusion detection system architecture followed clustering mechanism to build a four level hierarchical network which enhances network scalability to large geographical area and use both anomaly and misuse detection techniques for intrusion detection. This introduce policy based detection mechanism as well as intrusion response together with GSM cell concept for intrusion detection architecture.

• This paper [20] proposes a design of multi stage filter which is an efficient and effective approach in dealing with various categories of attacks in networks. The first stage of the filter is designed using Enhanced Adaboost with Decision tree algorithm to detect the frequent attacks occurs in the network and the second stage of the filter is designed using enhanced Adaboost with Naïve Byes algorithm to detect the moderate attacks occurs in the network. The final stage of the filter is used to detect the infrequent attack which is designed using the enhanced Adaboost algorithm with Naïve Bayes as a base learner. Performance of this design is tested with the KDDCup99 dataset and is shown to have high detection rate with low false alarm rates

• In the study paper [21] of network intrusion, much attention has been drawn to on-time detection of intrusion to safeguard public and private interest and to capture the law-breakers. This approach helps detect the intrusion and has a greater potential to apprehend the law-breaker. The purpose of this article is to formulate a method to this effect that is based on the statistical quality control techniques widely used in the manufacturing and production processes.

• In the proposed system in paper [22], designed fuzzy logic-based system for effectively identifying the intrusion activities within a network. The proposed fuzzy logic-based system can be able to detect an intrusion behavior of the networks since the rule base contains a better set of rules. Here, we have used automated strategy for generation of fuzzy rules, which are obtained from the definite rules using frequent items. The experiments and evaluations of the proposed intrusion detection system are performed with the KDD Cup 99 intrusion detection dataset. The experimental results clearly show that the proposed system achieved higher precision in identifying whether the records are normal or attack one

• In this paper [23], they built a model for intrusion detection system using random forest classifier. Random Forest (RF) is an ensemble classifier and performs well compared to other traditional classifiers for effective classification of attacks. To evaluate the performance of our model, we conducted experiments on NSL-KDD data set. Empirical result show that proposed model is efficient with low false alarm rate and high detection rate.

• In this research[24], a hierarchical off-line anomaly network intrusion detection system based on Distributed Time-Delay Artificial Neural Network is introduced. This research aims to solve a hierarchical multi class problem in which the type of attack (DoS, U2R, R2L and Probe attack) detected by dynamic neural network. The results indicate that dynamic neural nets (Distributed Time-Delay Artificial Neural Network) can achieve a high detection rate, where the overall accuracy classification rate average is equal to 97.24%.

• In the paper proposed algorithm[25], the detection metrics, such as number of packets transmitted and received, are used to compute the intrusion ratio (IR) by the IDS agent. The computed numeric or nonnumeric value represents the normal or malicious activity. As and when the sinkhole attack is captured, the IDS agent alerts the network to stop the data transmission. Thus, it can be a resilient to the vulnerable attack of sinkhole. Above all, the simulation result is shown for the proposed algorithm which is proven to be efficient compared with the existing work, namely, MS-LEACH, in terms of minimum computational complexity and low energy consumption. Moreover, the algorithm was numerically analysed using TETCOS NETSIM.

• In this paper[26], report the progress in developing intrusion detection (ID) capabilities for MANET. Building on our prior work on anomaly detection, we investigate how to improve the anomaly detection approach to provide more details on attack types and sources. For several well-known attacks, we can apply a simple rule to identify the attack type when an anomaly is reported. In some cases, these rules can also help identify the attackers. We address the run-time resource constraint problem using a cluster-based detection scheme where periodically a node is elected as the ID agent for a cluster. Compared with the scheme where each node is its own ID agent, this scheme is much more efficient while maintaining the same level of effectiveness. We have conducted extensive experiments using the ns-2 and MobiEmu environments to validate our research.

• In this paper[27], the author Snehal Deshmukh-Bhosale describes. In this context, capacity optimization goes beyond the traditional aim of capacity maximization, contributing also for organization's profitability and value. Indeed, lean management and continuous improvement approaches suggest capacity optimization instead of maximization. The study of capacity optimization and costing models is an important research topic that deserves contributions from both the practical and theoretical perspectives. This paper presents and discusses a mathematical

CHAPTER-3

INTERNET OF THINGS

The Internet of Things (IoT) is the network of physical objects ,devices, instruments, vehicles, buildings and other items embedded with electronics, circuits ,software, sensors and network connectivity that enables these objects to collect and exchange data.

The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency and accuracy

3.1.1 Definition of IOT: **"The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."**

3.1.2 Fundamental Characteristics Of Iot:

• **Interconnectivity**: With regard to the IOT, anything can be interconnected with the global information and communication infrastructure.

•**Things-related services:** The IOT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change

•**Heterogeneity:** The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

•**Dynamic changes:** The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

• **Enormous scale:** The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

• **Safety:** As we gain benefits from the IoT, we must not forget about safety. As both the creators and recipients of the IoT, we must design for safety. This includes the safety of our personal data and the safety of our physical well-being. Securing the endpoints, the networks, and the data moving across all of it means creating a security paradigm that will scale.

• **Connectivity:** Connectivity enables network accessibility and compatibility. Accessibility is getting on a network while compatibility provides the common ability to consume and produce data.

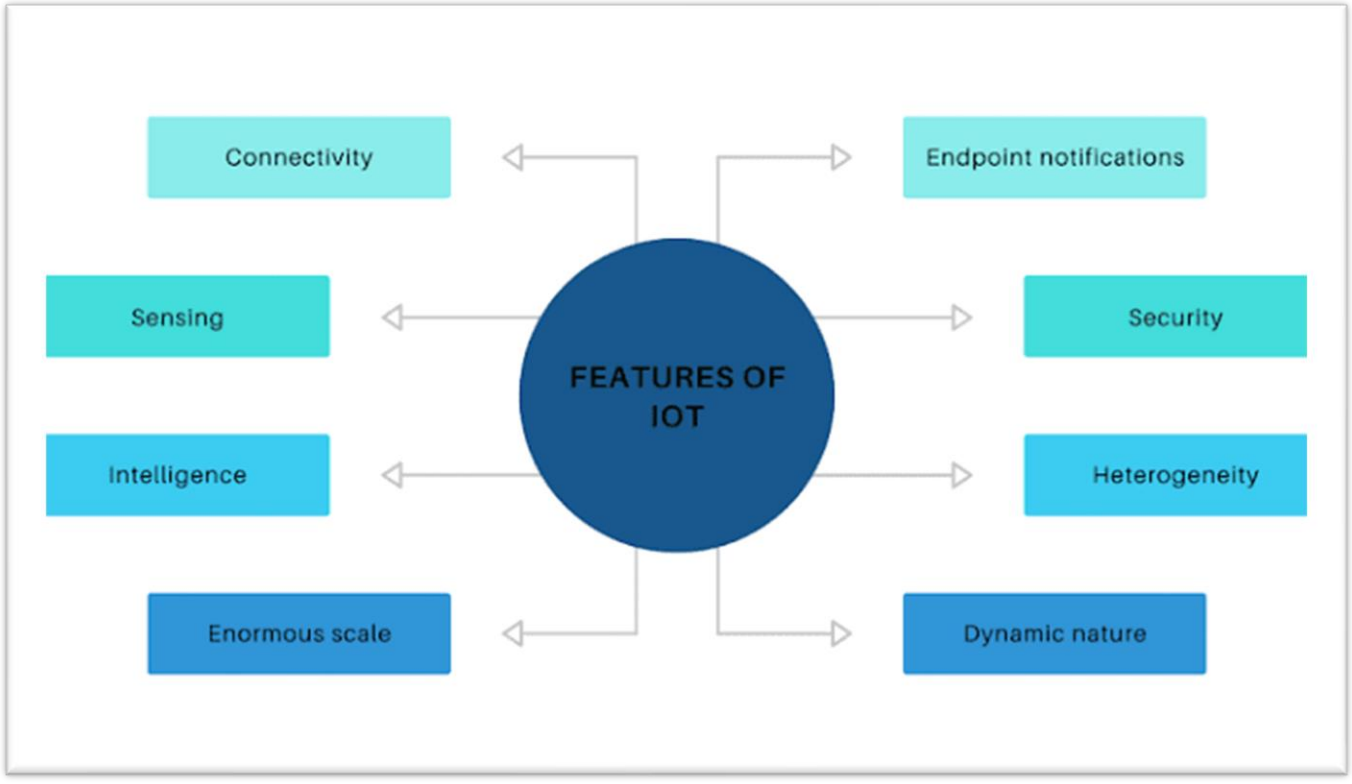


Fig 3.1

3.2.1 Industrial IOT: The Industrial Internet of Things (IIoT) refers to interconnected sensors, instruments, and other devices networked together with computers dedicate for industrial applications, including manufacturing and energy management. This connectivity allows for data collection, exchange, and analysis, potentially facilitating improvements in productivity and efficiency as well as other economic benefits.

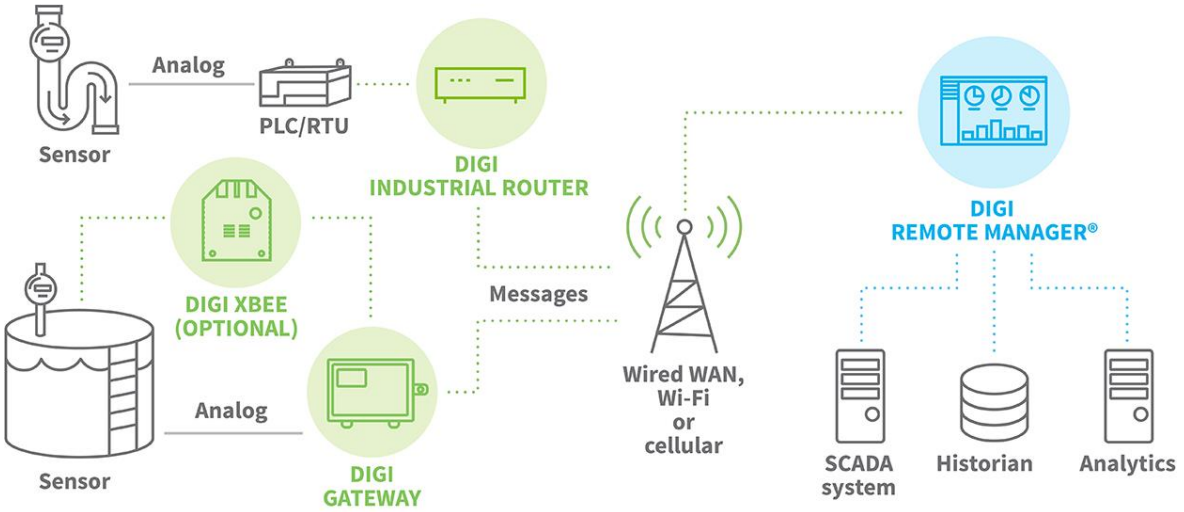


Fig 3.2

The IIoT is an evolution of a distributed control system (DCS) that allows for a higher degree of automation by using cloud computing to refine and optimize the process controls that are managed by industrial control systems.

Industrial Control Systems are organized into several classes by reference to their control action's relative complexity of the overall functions of the ICS. Common types of these control systems include:

- Programmable Logic Controllers (PLCs)
- Distributed Control Systems (DCS)
- Intelligent Electronic Devices (IEDs)
- Supervisory control and Data Acquisition (SCADA)
- Programmable Automation Controllers (PACs)
- Industrial Automation and Control Systems (IACS)
- Remote Terminal Units (RTUs)

CHAPTER-4

SECURITY THREATS IN IOT

4.1.1 Security Threats, Attacks, and Vulnerabilities: Before addressing security threats, the system assets (system components) that make up the IoT must first be identified. It is important to understand the asset inventory, including all IoT components, devices and services.An asset is an economic resource, something valuable and sensitive owned by an entity. The principal assets of any IoT system are the system hardware (include buildings, machinery, etc.) software, services and data offered by the services .

4.1.2 Vulnerabilities:

Vulnerabilities are weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks . Vulnerabilities can be found in variety of areas in the IoT systems. In particular, they can be weaknesses in system hardware or software, weaknesses in policies and procedures used in the systems and weaknesses of the system users themselves .

IoT systems are based on two main components; system hardware and system software, and both have design flaws quite often. Hardware vulnerabilities are very difficult to identify and also difficult to fix even if the vulnerability were identified due to hardware compatibility and interoperability and also the effort it take to be fixed. Software vulnerabilities can be found in operating systems, application software, and control software like communication protocols and devices drives. There are a number of factors that lead to software design flaws, including human factors and software complexity. Technical vulnerabilities usually happen due to human weaknesses. Results of not understanding the requirements comprise starting the project without a plan, poor communication between developers and users, a lack of resources, skills, and knowledge, and failing to manage and control the system .

4.1.3 Exposure: Exposure is a problem or mistake in the system configuration that allows an attacker to conduct information gathering activities. One of the most challenging issues in IoT is resiliency against exposure to physical attacks. In the most of IoT applications, devices may be left unattended and likely to be placed in location

easily accessible to attackers. Such exposure raises the possibility that an attacker might capture the device, extract cryptographic secrets, modify their programming, or replace them with malicious device under the control of the attacker

4.1.4 Threat: A threat is an action that takes advantage of security weaknesses in a system and has a negative impact on it . Threats can originate from two primary sources: humans and nature. Natural threats, such as earthquakes, hurricanes, floods, and fire could cause severe damage to computer systems. Few safeguards can be implemented against natural disasters, and nobody can prevent them from happening. Disaster recovery plans like backup and contingency plans are the best approaches to secure systems against natural threats. Human threats are those caused by people, such as malicious threats consisting of internal (someone has authorized access) or external threats (individuals or organizations working outside the network) looking to harm and disrupt a system. Human threats are categorized into the following:

- Unstructured threats consisting of mostly inexperienced individuals who use easily available hacking tools.
- Structured threats as people know system vulnerabilities and can understand, develop and exploit codes and scripts. An example of a structured threat is Advanced Persistent Threats (APT) . APT is a sophisticated network attack targeted at high-value information in business and government organizations, such as manufacturing, financial industries and national defence , to steal data .

As IoT become a reality, a growing number of ubiquitous devices has raise the number of the security threats with implication for the general public. Unfortunately, IoT comes with new set of security threat. There are a growing awareness that the new generation of smart-phone, computers and other devices could be targeted with malware and vulnerable to attack

4.2.1 Attacks: Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools. Attackers launch attacks to achieve goals either for personal satisfaction or recompense. The measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources and motivation is called attack cost . Attack actors are people who are a threat to the digital world . They could be hackers, criminals, or even governments. An attack itself may come in many forms, including active network attacks to monitor unencrypted traffic in search of sensitive information; passive attacks such as

monitoring unprotected network communications to decrypt weakly encrypted traffic and getting authentication information; close-in attacks; exploitation by insiders, and so on.

4.2.2 Common cyber-attack types are:

Physical attacks: This sort of attack tampers with hardware components. Due to the unattended and distributed nature of the IoT, most devices typically operate in outdoor environments, which are highly susceptible to physical attacks.

Reconnaissance attacks: Unauthorized discovery and mapping of systems, services, or vulnerabilities. Examples of reconnaissance attacks are scanning network ports, packet sniffers, traffic analysis, and sending queries about IP address information.

Denial-of-service (DoS): This kind of attack is an attempt to make a machine or network resource unavailable to its intended users. Due to low memory capabilities and limited computation resources, the majority of devices in IoT are vulnerable to resource enervation attacks.

Access attacks: Unauthorized persons gain access to networks or devices to which they have no right to access. There are two different types of access attack: the first is physical access, whereby the intruder can gain access to a physical device. The second is remote access, which is done to IP-connected devices.

Attacks on privacy: Privacy protection in IoT has become increasingly challenging due to large volumes of information easily available through remote access mechanisms. The most common attacks on user privacy are:

Data mining: enables attackers to discover information that is not anticipated in certain databases.

Cyber espionage: using cracking techniques and malicious software to spy or obtain secret information of individuals, organizations or the government.

Eavesdropping: listening to a conversation between two parties

Tracking: a users movements can be tracked by the devices unique identification number (UID). Tracking a users location facilitates identifying them in situations in which they wish to remain anonymous.

Password-based attacks: attempts are made by intruders to duplicate a valid user password. This attempt can be made in two different ways: 1) dictionary attack – trying possible combinations of letters and numbers to guess user passwords; 2) brute force attacks – using cracking tools to try all possible combinations of passwords to uncover valid passwords.

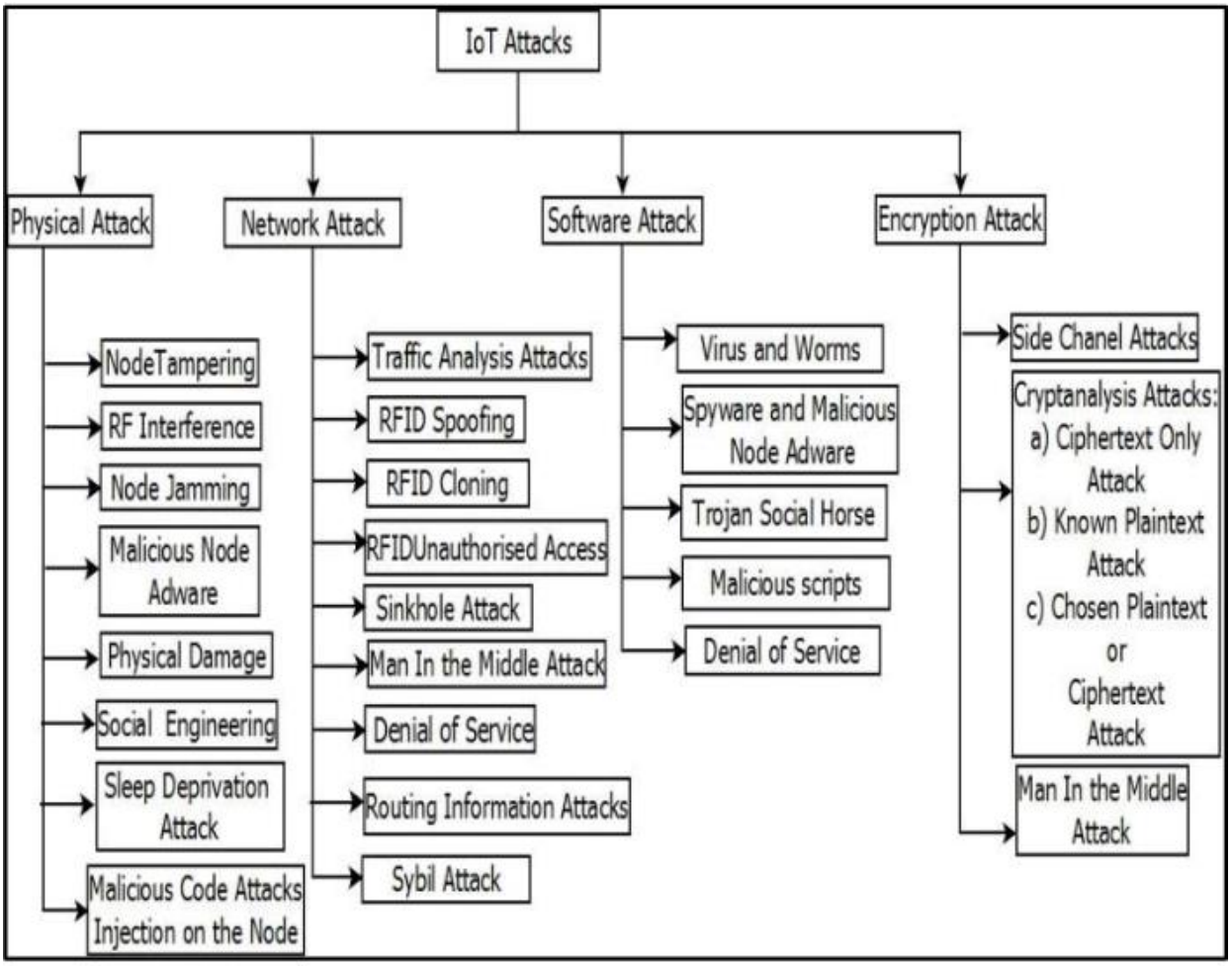


Fig 4.1

Cyber-crimes: The Internet and smart objects are used to exploit users and data for materialistic gain, such as intellectual property theft, identity theft, brand theft, and fraud

Destructive attacks: Space is used to create large-scale disruption and destruction of life and property. Examples of destructive attacks are terrorism and revenge attacks.

Supervisory Control and Data Acquisition (SCADA) Attacks: As any other TCP/IP systems, the SCADA system is vulnerable to many cyber attacks . The system can be attacked in any of the following ways:

Using denial-of-service to shut down the system.

Using Trojans or viruses to take control of the system. For instance, in 2008 an attack launched on an Iranian nuclear facility in Natanz using a virus named Stuxnet

CHAPTER-5

NETWORK CODING

5.1.1 An Overview On Computer Networks & Coding:

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes. The interconnections between nodes are formed from a broad spectrum of telecommunication network technologies, based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of network topologies, simply speaking Computer Network is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network. The aim of the computer network is **the sharing of resources among various devices**.

The nodes of a computer network may include personal computers, servers, networking hardware, or other speclized or general-purpose hosts. They are identified by hostnames and network addresses. Hostnames serve as memorable labels for the nodes, rarely changed after initial assignment. Network addresses serve for locating and identifying the nodes by communication protocols such as the Internet Protocol. Computer networks may be classified by many criteria, including the transmission medium used to carry signals, bandwidth, communications protocols to organize network traffic, the network size, the topology, traffic control mechanism, and organizational intent.

Computer networks support many applications and services, such as access to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications .A computer network extends interpersonal communications by electronic means with various technologies, such as email, instant messaging, online chat, voice and video telephone calls, and video conferencing.

A network allows sharing of network and computing resources. Users may access and use resources provided by devices on the network, such as printing a document on a shared network printer or use of a shared storage device. A network allows sharing of files, data, and other types of information giving authorized users the ability to access information stored on other computers on the network. Distributed computing uses computing resources across a network to accomplish tasks.

5.2.1INTRODUCTION TO NETWORK CODING :

NETWORK CODING has emerged as an alternative and powerful solution in communication networks because of its potential for achieving huge throughput gains . The core idea behind network coding is the combination of packets of various flows via algebraic operations in the relay nodes or routers. Network-coded packets can be decoded in their destinations by jointly processing information flows from different paths and/or exploiting some prior knowledge. This breakthrough coding method may achieve the maximum-flow capacity bound in multicasting applications, thereby meeting the stringent requirements and demand of high-speed multimedia traffics, such as IPTV. In wireless networks, network coding can substantially improve the energy and spectrum efficiency in unicast flow transmissions because of the broadcasting nature of the physical layer. As such, wireless network coding has attracted significant attention recently. Network coding was first proposed to achieve the maximum-flow multicasting of wired networks . Two unified frameworks, a linear-space-based and an algebra-based , were then proposed to solve the single-source multicasting problem and perform global code construction for multicasting over a general graph model. In wireless networks, network coding can be easily applied to achieve throughput gains for unicast flows. It can be applied locally into some typical wireless subnetworks, such as bidirectional or X-relaying topologies, without knowing the global topology information. The work in [5] first demonstrated the application of network coding in bidirectional relaying, where the relay XORs the packets from two sources and broadcasts the XORed output packet. A destination node will then decode the received packet by simply XORing it again with its own packet. This idea can save a total of 50% power and bandwidth for the relay transmission. Motivated by this great potential, [6] and [7] studied a modified scheme, namely the

physical-layer network coding, where the relay amplifies and broadcasts the received signal, which then becomes a noisy version of the summation of the two source signals. More practical issues, such as constellation and channel coding, were investigated in [8] and [9]. A generalized and unified method for signal level network coding was proposed in [10], which can be applied into arbitrary wireless relay networks. To broaden the applications, [11] investigated network coding for X and wheel topologies with multiple bidirectional flows via a common relay.

A platform along with a prototype protocol, COPE, was developed and evaluated. In these topologies, opportunistic combination was found to be a useful means to maximize the goodput [12]. Our previous work [13] studied multiway relaying, where nodes exchange their packets via a common relay using a wireless switching network model. Network coding was generalized by a cross-layer approach, referred to as joint physical-network coding, which can significantly improve the throughput of multiway relaying. The bidirectional relaying topology was also extended to the multirelay case, where network coding was combined with distributed space-time coding [14], relay selection [15], and beamforming [16] to combat fading. In addition, the global analysis of network coding gains in large-scale wireless networks was considered in [17]–[19]. The above works were mainly aimed at utilizing network coding to improve the throughput. Among them, [11] and [12] have particularly noticed the random packet arrival process, which yields an opportunistic coding/scheduling. With random packet arrivals, one should also carefully optimize the higher-layer performance, such as queueing delay or stability.

This has motivated some cross-layer design of wireless network coding in random access or unreliable networks [20]–[23]. In contrast to existing works, this paper jointly optimizes the quality-of-service (QoS) parameters, namely delay and packet loss rate, as well as the power efficiency of wireless network coding. An intuitive motivation of this work relies on the observation that with an asynchronous and random arrival process, a packet has to wait to be network-coded with other packets if they do not arrive simultaneously. Therefore, packet delay will be induced by network coding as a cost to be paid for the energy or power saving. For the relay node with finite buffer capacity, the number of backlogged packets to be network-coded can exceed the buffer capacity, which will result in packet loss and retransmission. This may greatly reduce the overall QoS, especially for real-time traffic. To overcome this limitation, a proper design of wireless network coding must balance the saving of power due to the combination of packets and the increase of delay due to the packet waiting times. An intuitive and straightforward solution is to

allow opportunistic transmission of some packets without network coding. Although the transmission without network coding may lose some power efficiency, it can efficiently reduce the average queue length in the relay buffer as well as the queueing delay. As a result, a novel method that can take advantage of both the network-coded and uncoded transmission is desired to achieve the optimal tradeoff between the power efficiency and the packet delay. Our aim is to understand its fundamental performance limit and the optimal design.

5.1.2 Communication Protocols & Data exchange :

The TCP/IP model and its relation to common protocols used at different layers of the model. A communication protocol is a set of rules for exchanging information over a network. Communication protocols have various characteristics. They may be connection-oriented or connectionless, they may use circuit mode or packet switching, and they may use hierarchical addressing or flat addressing. In a protocol stack, often constructed per the OSI model, communications functions are divided up into protocol layers, where each layer leverages the services of the layer below it until the lowest layer controls the hardware that sends information across the media.

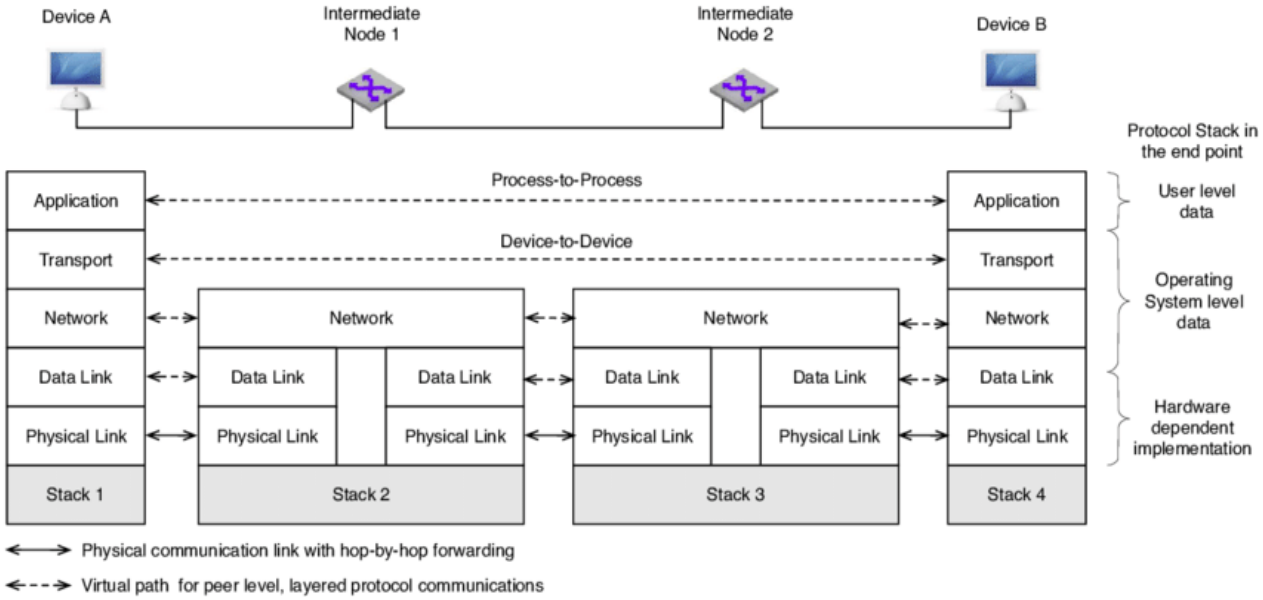
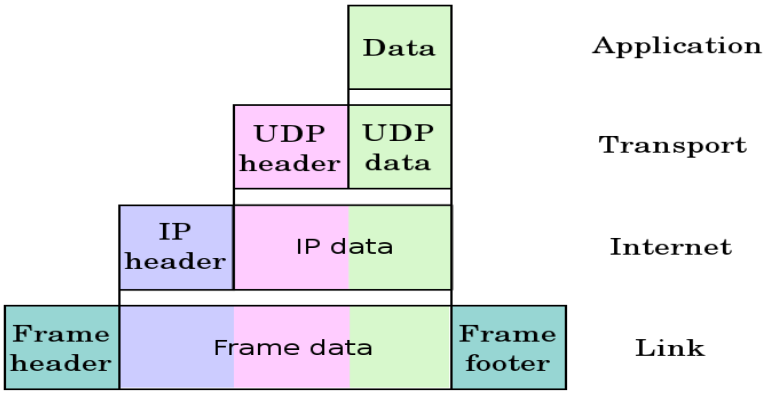


Fig 5.1

The use of protocol layering is ubiquitous across the field of computer networking Conceptual data flow in a simple network topology of two hosts (A and B) connected by a link between their respective routers. The application on each host executes read and write operations as if the processes were directly connected to each other by some kind of data pipe.

After establishment of this pipe, most details of the communication are hidden from each process, as the underlying principles of communication are implemented in the lower protocol layers. In analogy, at the transport layer the communication appears as host-to-host, without knowledge of the application data structures and the connecting routers, while at the internetworking layer, individual network boundaries are traversed at each router

The end-to-end principle has evolved over time. Its original expression put the maintenance of state and overall intelligence at the edges, and assumed the Internet that connected the edges retained no state and concentrated on speed and simplicity. Real-world needs for firewalls, network address translators, web content caches and the like have forced changes in this principle.



Encapsulation of application data descending through the layers described in RFC 1122

Fig 5.2

The robustness principle states: “In general, an implementation must be conservative in its sending behaviour, and liberal in its receiving behaviour. That is, it must be careful to send well formed datagrams, but must accept any datagram that it can interpret (e.g., not object to technical errors where the meaning is still clear).The second part of the principle is almost as important: software on other hosts may contain deficiencies that make it unwise to exploit legal but obscure protocol features. Encapsulation is used to provide abstraction of protocols and services.

Encapsulation is usually aligned with the division of the protocol suite into layers of general functionality. In general, an application (the highest level of the model) uses a set of protocols to send its data down the layers. The data is further encapsulated at each level

5.2.2 Buffer-Aware Network Coding:

Buffer-Aware Network Coding, also referred to as BANC, to merge network-coded and uncoded transmissions. The two key performance metrics, namely the power efficiency in the physical layer and the average packet delay in the higher layer, will be coupled by this cross-layer framework. In particular, we shall consider the bidirectional relaying topology and X-topology, where network coding can be performed in the relay node with random packet arrivals. A random mapping-based method will be presented to characterize any buffer aware networking coding in a unified way. Based on this, a Markov model of the buffer state is formulated to obtain analytical results regarding the average packet delay, packet loss rate, and power consumption. To understand the cross-layer performance limit of BANC, we shall consider an optimization problem, where the weighted sum packet delay is minimized given the average power constraint. The optimal solution of this problem will yield the minimum delay pair, as well as the achievable delay region of queues. Moreover, we shall propose the delay-optimal BANC, which can achieve the bound of the delay region. It is very interesting to see that the delay-optimal BANC allows transmission without network coding only when the queue length exceeds a given threshold. This can result in very low implementation complexity. Intuitively, with a higher uncoded transmission threshold, more packets will be combined via network coding. Therefore, increasing this threshold will increase the packet delay but decrease the power consumption. This motivates us to investigate the optimal delay–power tradeoff as the performance limits of BANC. In addition, some asymptotic performance of the optimal BANC will be studied to give more insights.

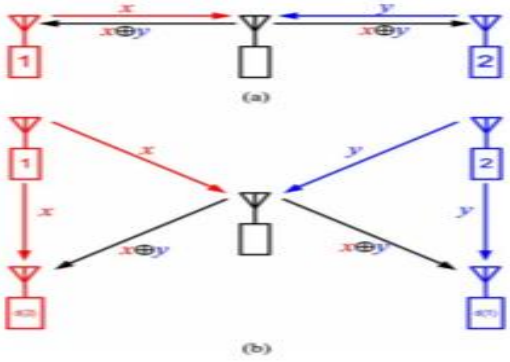


Fig. 1. Wireless networks with network coding. (a) Bidirectional relay network. (b) X-topology relay network.

The remainder of this paper is organized as follows. Section II presents the system model. In Section III, a unified framework for wireless network coding with random packets arrival is presented. Section IV will obtain the analytical results on the average packet delay and relay power consumption by formulating Markov models for the buffer states. Based on these results, we shall investigate the achievable delay region, as well as the delay-optimal BANC strategy by solving a weighted delay minimization problem in Section V. Finally, simulation results and concluding remarks are presented in Sections VI and VII, respectively.

CHAPTER-6

PROPOSED WORK & METHODOLOGY

6.1 Proposed Work :

- Create a wireless network of n number of nodes in a network simulator tool
- Create threat issues such that system resources in the network are compromised which could be from the following "Bandwidth, Power, Latency etc"
- Introduce network coding into the network to solve the arising problem encounterd in point number two
- Finally obtain the Output via visual animation through network simulator tools
- Obtain the Graph Plot

6.2 Methodology :

- To fulfil the following above mentioned objectives the Paraphernalia and tools set up is a network simulator tool called Ns-2 and XGraph, xgraph is a general purpose x-y data plotter

- Ns is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. All are discrete-event computer network simulators, primarily used in research and teaching.

❖ **The simulation invovels the methodology as follows :**

- We have created the network coding is a reasonable way to increase network efficiency in response to an increase of sensed data in the wireless sensor network.

- Our proposed network coding, intermediate nodes combine packets received from neighbouring nodes, transform, and transmit encoded packets that can be decoded at the destination. Our Proposed wireless sensor network prepared with a number of nodes.

- The concept covered the system resources with Bandwidth , Power and Latency.

- The network coding is prepared for getting parameters.

- This scheme is based on trust among nodes.

- If any malicious node joins the network, it can act as an intermediate node that could fabricate encoded packets.

- It might be more difficult to identify the authenticity of such encoded packets since packets that are received at the destination might not originate from a single source,

- Be combined with several other packets originating from multiple sources

RESULTS

6.3 Xgraph Plots:

PLOT I:

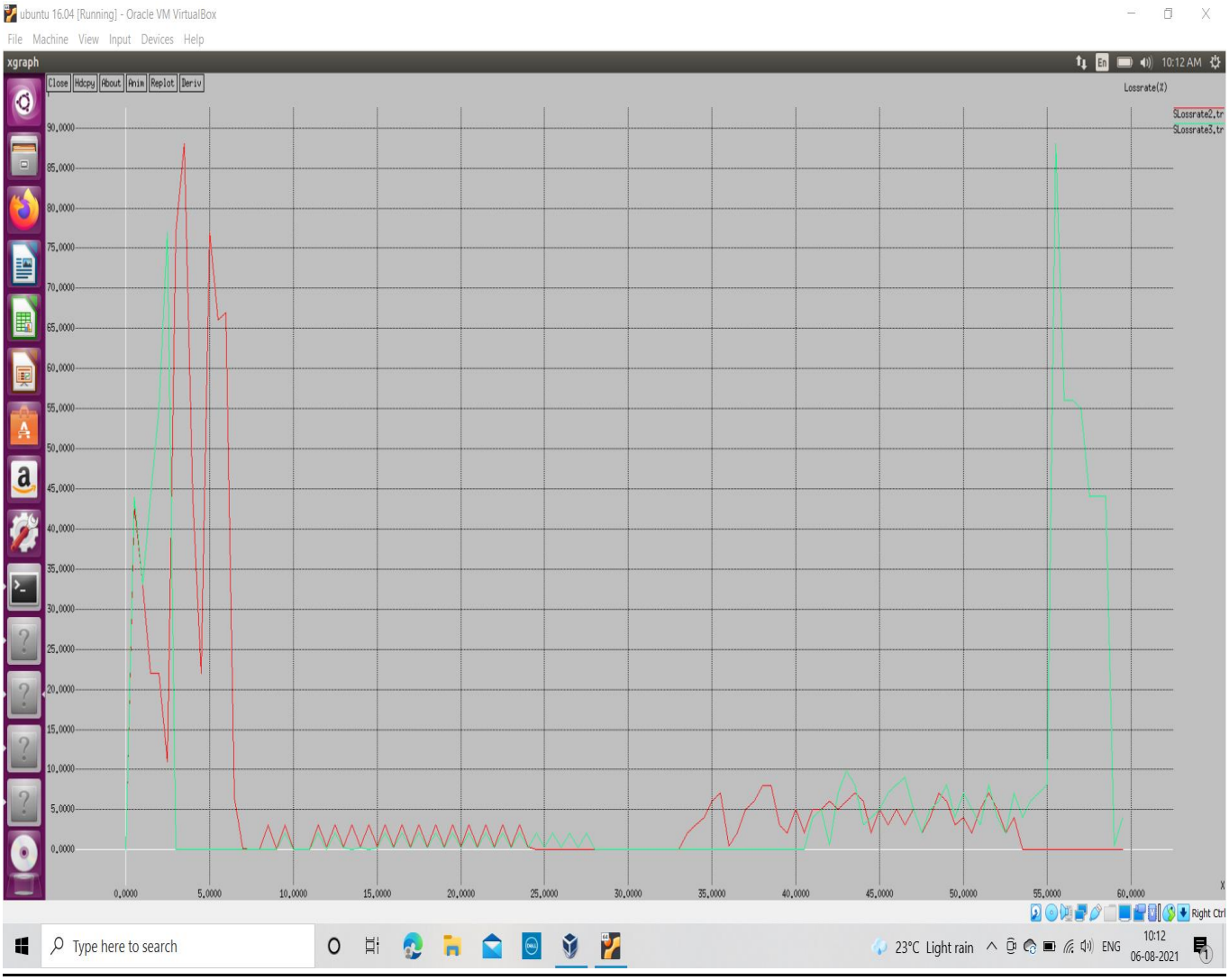


Fig 6.1

The graphs shows the various data packets routing from one node to another node the peaks indicates the malicious nodes are attacking during the routing as the peak reduced the routing is efficient. The plot further describes the loss rate of the packets that have been dropped during the activity of the malicious node

PLOT II :

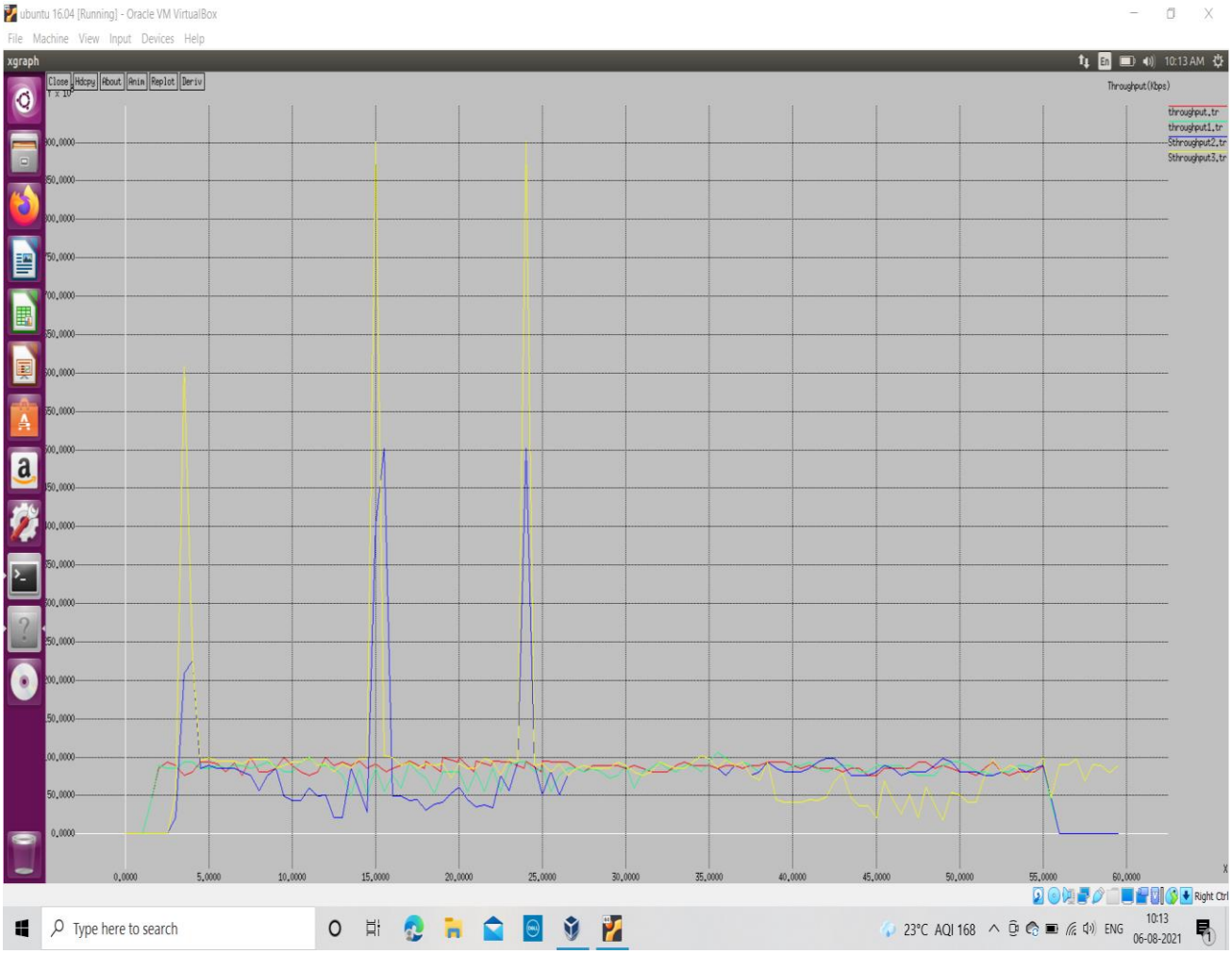


Fig 6.2

The graphs shows the scenario of data packets routing from one node to another node the peaks indicates the malicious nodes are attacking during the routing, as the peak is achieved the efficiency of the network decrease and as the peak is reduced the routing is efficient which is been shown as throughput count in the above plot

Throughput:

In general terms, throughput is the rate of production or the rate at which something is processed. Throughput or network throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link, or it can pass through a certain network node.

PLOT III:

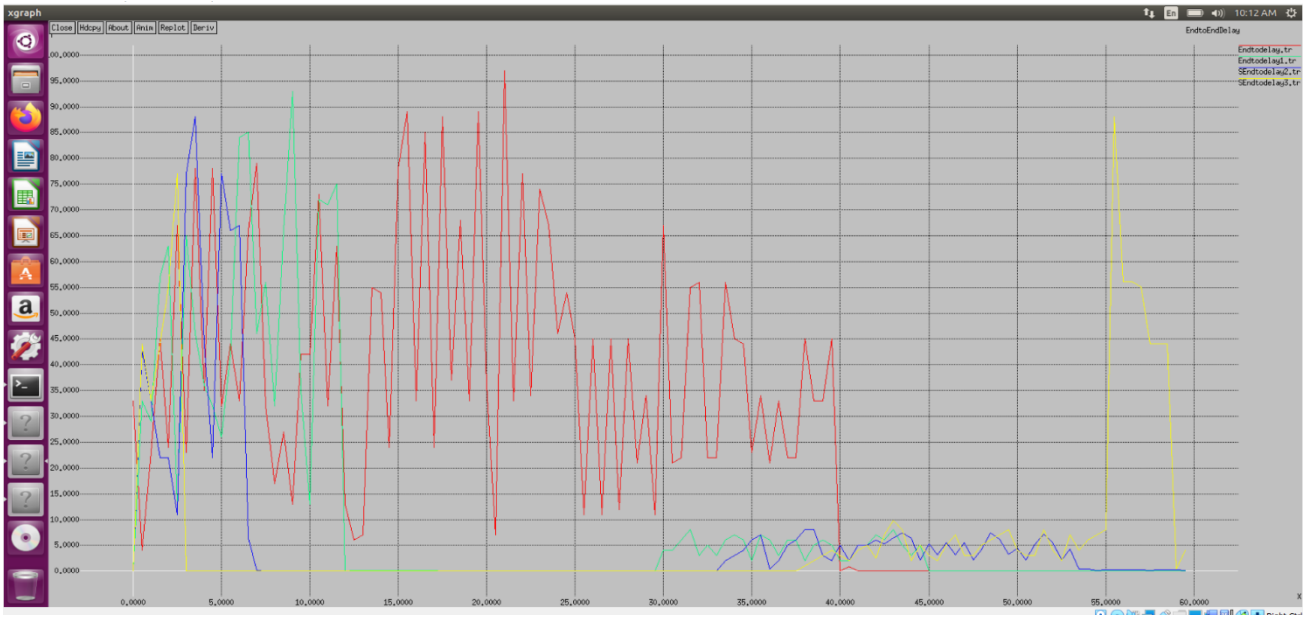


Fig 6.3

The above plot shows the network performance during the malicious activity of the node and after in terms of End to End delay parameter i.e End-to-end delay or one-way delay (OWD) refers to the time taken for a packet to be transmitted across a network from source to destination.

PLOT IV :

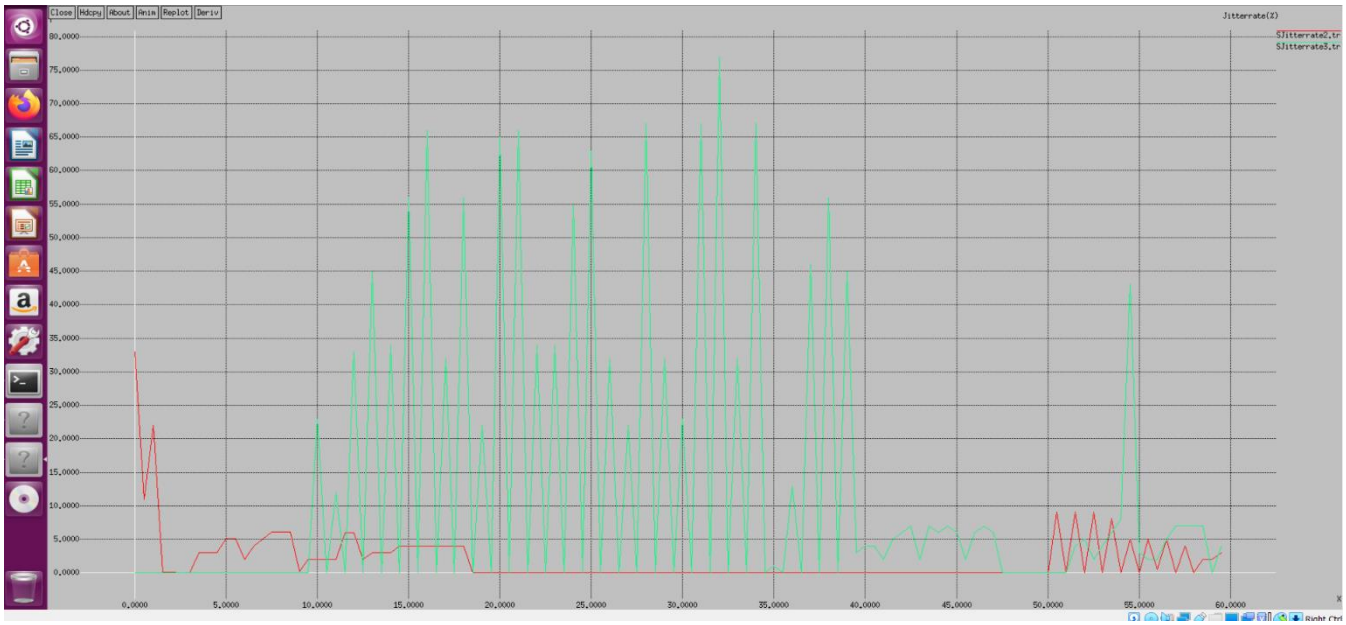


Fig 6.4

The plot iv similar to the others show the network performance but after the malicious node's route path been removed it shows the proper fuctionin parameter in terms of bit rate and latency of the network

CHAPTER -7

CONCLUSION & DISCUSSION

Internet of Things is an important part of the future, and the security of IoT will relate to many important scenarios of the future and has become the core requirement of the network development. However, as the resources of IoT devices are constrained, many security mechanisms are hard to be implemented to protect the security of IoT networks. In this article, based on the , we proposed a uniform intrusion detection method for the vast heterogeneous IoT networks. Our method uses an extension of Labelled Transition Systems to propose a uniform description of IoT systems and can detect the intrusions by comparing the abstracted actions flows. We designed the intrusion detection approach, The result of the proposed IDS detects the malicious activity which is compromising a node's parameter . and produce appropriate graph plots.

For the future work, we plan to continue enrich date types in our Standard Protocol Library and to improve the fuzzy method to make the creating of Normal Action Library become more efficient and accurate. Another line of our future research is to develop the suitable method to describe and evaluate the contents of the translating packets.

REFERENCE

[1] IDLP: An Efficient Intrusion Detection and Location-Aware Prevention Mechanism for Network Coding-Enabled Mobile Small Cells ,Received January 24, 2020, accepted February 7, 2020, date of publication March 2, 2020, date of current version March 12, 2020.Digital Object Identifier 10.1109/ACCESS.2020.2977428

[2] Enhanced AODV Protocol for Detection and Prevention of Blackhole Attack in Mobile Ad Hoc Network I S S N 2 2 7 7 – 3061 volume 1 international journal of technology

[3] Blackhole attack implementation in AODV Protocol , international Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 402 ISSN 2229-5518

[4] Zhu, B.; Joseph, A.; Sastry, S. A Taxonomy of Cyber Attacks on SCADA Systems. In Proceedings of the 2011International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Washington, DC, USA, 19 October 2011;

[5] DNP Users Group. DNP3 Application Layer Specification; Version 2.00; DNP Organization: Washington, WA,USA, 2005; Volume 2.

[6] Byungho, M.; Vijay, V. Design and Analysis of Security Attacks against Critical Smart Grid Infrastructures. IN Proceedings of the IEEE 2014 19th International Conference on Engineering of Complex Computer Systems, Washington, DC, USA, 4–7 August 2014

[7] Cyber Security Threats to IoT Applications and Service Domains Wireless Pers Commun DOI 10.1007/s11277-017-4434-6

[8] P. Popovski and H. Yomo, “Wireless network coding by amplify-andforward for bi-directional traffic flows,” IEEE Commun. Lett., vol. 11, no. 1, pp. 16–18, Jan. 2007.

[9] T. Koike-Akino, P. Popovski, and V. Tarokh, “Optimized constellations for two-way wireless relaying with physical network coding,” IEEE J. Sel. Areas Commun., vol. 27, no. 5, pp. 773–787, Jun. 2009.

[10] S. L. Zhang and S. C. Liew, "Channel coding and decoding in a relay system operated with physical-layer network coding," IEEE J. Sel. Areas Commun., vol. 27, no. 5, pp. 788–796, Jun. 2009.

[11] S. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow: A deterministic approach," IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.

[12] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the air: Practical wireless network coding," IEEE/ACM Trans. Netw., vol. 16, no. 3, pp. 497–510, Jun. 2008.

[13] H. Yomo and P. Popovski, "Opportunistic scheduling for wireless network coding," IEEE Trans. Wireless Commun., vol. 8, no. 6, pp. 2766–2770, Jun. 2009.

[14] P. Sanders, S. Egner, and L. Tolhuizen, "Polynomial time algorithms for network information flow," in Proc. 15th ACM Symp. Parallel Algorithms and Architectures, San Diego, CA, 2003, pp. 286–294.

[15] S. D. Servetto and G. Barrenechea, "Constrained random walks on random graphs: Routing algorithms for large scale wireless sensor networks," in Proce. 1st ACM Int. Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, 2002, pp. 12–21.

[16] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," IEEE Trans. Inf. Theory, vol. IT-19, no. 4, pp. 471–480, Jul. 1973. [29] Y. Zhu, B. Li, and J. Guo, "Multicast with network coding in application-layer overlay networks," IEEE J. Sel. Areas Commun., vol. 22, no. 1, pp. 107–120, Jan. 2004

[17] Virendra Singh Kushwah "Implementation of New Routing Protocol for NodeSecurity in a Mobile Ad Hoc Network" (IJCSIS) International Journal of Computer Science and Information Security,Vol. 8, No. 9, December 2010

[18] Tamilselvan, L.; and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. AusWireless, 21-21.

[19] C. Perkins, E. B. Royer, and S. Das, "Ad hoc on-demand distance vector(aodv) routing," RFC: 3561, Nokia Research Center

[20] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, ''Network information flow,'' IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[21] T. Ho and D. Lun, Network Coding: An Introduction. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[22] A. Esfahani, G. Mantas, and J. Rodriguez, ‘‘An efficient null space-based homomorphic MAC scheme against tag pollution attacks in RLNC,’’ IEEE Commun. Lett., vol. 20, no. 5, pp. 918–921, May 2016.

[23] R. Parsamehr, G. Mantas, A. Radwan, J. Rodriguez, and J.-F. Martínez, ‘‘Security threats in network coding-enabled mobile small cells,’’ in Proc. Int. Conf. Broadband Commun., Netw. Syst. Cham, Switzerland: Springer, Sep. 2018, pp. 337–346.

[24] S. Agrawal and D. Boneh, ‘‘Homomorphic MACs: MAC-based integrity for network coding,’’ in Proc. Int. Conf. Appl. Cryptography Netw. Secur. Berlin, Germany: Springer, 2009, pp. 292–305.

[25] A. Fiandrotti, R. Gaeta, and M. Grangetto, ‘‘Securing network coding architectures against pollution attacks with band codes,’’ IEEE Trans. Inf. Forensics Secur., vol. 14, no. 3, pp. 730–742, Mar. 2019.

[26] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, ‘‘Resilient network coding in the presence of byzantine adversaries,’’ in Proc. 26th IEEE Int. Conf. Comput. Commun. (INFOCOM), May 2007, pp. 616–624.

[27] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger, ‘‘Byzantine modification detection in multicast networks with random network coding,’’ IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2798–2803, Jun. 2008.

[28] M. Kim, L. Lima, F. Zhao, J. Barros, M. Medard, R. Koetter, T. Kalker, and K. J. Han, ‘‘On counteracting byzantine attacks in network coded peer-to-peer networks,’’ IEEE J. Sel. Areas Commun., vol. 28, no. 5, pp. 692–702, Jun. 2010.

**********END**********