5-2015

Security integrity of EKG signal monitoring under different network attack conditions

Raghava Teja Pingali
University of Texas-Pan American

SECURITY INTEGRITY OF EKG SIGNAL MONITORING UNDER DIFFERENT NETWORK ATTACK CONDITIONS

A Thesis

by

RAGHAVA TEJA PINGALI

Submitted to the Graduate School of the
University of Texas-Pan American
In partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

May 2015

Major Subject : Electrical Engineering

SECURITY INTEGRITY OF EKG SIGNAL MONITORING UNDER DIFFERENT NETWORK ATTACK CONDITIONS

A Thesis
by
RAGHAVA TEJA PINGALI

COMMITTEE MEMBERS

Dr. Sanjeev Kumar
Chair of Committee

Dr. Jaime Ramos
Committee Member

Dr. Wenjie Dong
Committee Member

May 2015

ABSTRACT

Raghava Teja Pingali, Security Integrity of EKG Signal Monitoring under Different Network Attack Conditions. Master of Science (MS), May 2015, 24 tables, 76 figures, 44 references.

This thesis focuses on issues related with monitoring of EKG signals under different network attack traffic conditions. It is becoming common for modern hospitals to monitor real time EKG signals of patients on computers that are usually connected to networks. If the network suffers with attack conditions, it can affect connected computers and alter EKG signals monitoring, hence raising false alarms. Denial of Service attacks may silently affect the real time monitoring of EKG signals. Altering of EKG signals may result in loss of integrity and it can violate CIA triad of security. In this thesis, different attack conditions were simulated for various operating systems under different loads of attack traffic to observe how the EKG signals were affected.

ACKNOWLEDGEMENTS

I am very much thankful to Dr. Sanjeev Kumar, chair of my thesis committee, for all his mentoring and advice. Thank you for believing in me and for the unconditional support you have provided throughout all this research work. I can honestly say that your encouragement and valuable suggestions helped me to finish my research. I would also like to thank my friends in the Network Research Lab at UTPA, for their support. I am also grateful to my thesis committee members: Dr. Jaime Ramos and Dr. Wenjie Dong.

Work in this thesis is based upon the grant awarded to Dr. Sanjeev Kumar by the National Science Foundation (NSF) under Grant No. 0521585

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

DDoS	: Distributed Denial of Service
EKG	: Electrocardiogram
bpm	: beats per minute
Mbps	: Megabits per second
CIA Triad	: Confidentiality, Integrity, Availability
TCP	: Transmission Control Protocol
ARP	: Address Resolution Protocol
ICMP	: Internet Control Message Protocol
SA node	: Sino- Atrial Node
AV node	: Atrio-Ventricular node
IP address	: Internet Protocol address
MAC address	: Media Access Control address
IT	: Information Technology
RAM	: Random Access Memory
SP	: Service Pack

CHAPTER I

INTRODUCTION

1.1 Statement of the problem:

Denial of Service attacks (DoS) try to diminish the network availability so the authorized users can't have access. It is a continuous severe threat to the internet. Within short period of time, DoS attacks can disable the resources of the victim computer. Effects might be overwhelming server or web site with malicious data requests. Most of the organizations profit depends on Internet infrastructure, so DoS impact could be tragic. The assaults on the most familiar web sites seems to be a wakeup call to give more priority to the importance of security in today's Internet. Even Yahoo and Amazon.com web sites were attacked by Denial of Service attacks [1].These attacks have the ability to stop communication, processing transactions, function effectively for hours or days.

Today, DoS attacks are repeatedly implemented by a network of remotely controlled, well organized, and widely distributed Zombies or Botnet computers that act together and sends a large amount of traffic and/or service packets to the destination. The target system either responds so slowly as to be unusable completely. Attacks that are performed for financial gain are frequently the most hard to stop attacks. DoS flooding attacks can be mentioned in two types based on the protocol level that is targeted. First, is Network level DDoS (Distributed Denial of Service) flooding attacks, second is Application level DDoS flooding attacks [2].

These attacks can make resources unavailable to the valid users by exhausting the resources. According to latest reports, 7000 DDoS attacks count is up on daily basis which is certainly huge loss. These attacks are obvious threat to uptime of Network, Server, Websites. In January 2015, France's chief information systems defense official announced a fine growth in online attacks against French web sites [3]. In present situation, this kind of attacks continue to menace Internet. Even though some mitigation techniques are in the market to diminish those kind of attacks, same time hackers are ahead of security professionals. According to a private organization which monitors Internet threats said that France was targeted by 1070 denial of service attacks in 24 hours[4].

Latest DDoS attacks: Belgian media group, had a distributed denial of service (DDoS) attack that led to trouble for several hours in April, 2015. Recently, New Hampshire's state government website was not in access to some users for many hours because the outside company that hosts it was handling with another "distributed denial of service" attack on its servers in April, 2015 [5].

Research is going on different DDoS attacks and their defense mechanisms to get rid of this problem. Denial of Service attacks are characterized by an explicit attempt to avoid the authorized service. Present Internet architecture focusses on the packet distribution from source to destination, there is end to end paradigm is required [6]. There are three kinds of DDoS attacks. 1) Volume Based Attacks, which are measured in bits per second. This attack wants to exhaust the bandwidth of the attacked site. 2) Protocol Based Attacks, which are measured in packets per second. This type consumes server resources. 3) Application Layer Based Attacks, which are measured in requests per second. The aim of this kind of attack is to pull down the web server. The primary challenge in preventing DDoS attack is to identify the harmful requests [7].

There are three components which are given more priority for information security in an organization called as the CIA security triad. CIA stands for Confidentiality, Integrity and Availability. These are the most important components of security.

Confidentiality:

It can be attained by avoiding unauthorized disclosure of data, system or network. The aim of this element is to avoid the vital information from reaching to unauthorized people. Moreover, this element is also responsible to make available that data to valid users. The common method to ensure confidentiality is Data encryption method. Encryption converts plain text into ciphered data, which is unreadable without authorization. Examples for different Encryptions schemes are DES (Data Encryption standard), 3 DES which is more secure, AES (Advanced Encryption Standard), Trusted Platform Modules (TPMs) can encrypt entire hard drive, S/MIME used to encrypt email. User Identification and passwords includes a standard process, even biometric identification, soft tokens and security tokens are some of the methods which ensures the element confidentiality.

Integrity :

This element includes, trustworthiness, precise and consistency of the data over its complete cycle. Integrity can be attained by protecting unauthorized modification of information. Data, which is in travel must not be modified by unauthorized people from source to destination. Steps has to be taken to make sure the precise data which is generated at the source must exactly reach the destination. Backups must be taken to get back the correct data, if data is corrupted. Hash Algorithms are used to reduce the loss of integrity. Hash is a number considered for a data set using the above algorithm. Hash number will be same as long as data is same. The common hash algorithms are Message Digest 5 - MD5, Secure Hashing Algorithm 1 (SHA-1).

Availability :

This is the last element in the CIA security triad, which delivers security for the data in its complete cycle. DDoS attack can pull down a server which is a loss of Availability for that web site. Unauthorized interruption should be avoided to achieve this availability factor. Sufficient communication bandwidth should be provided and occurrence of bottlenecks are very important. Security software's such as Firewall and proxy server can be guard against malicious activities such as Denial of Service attacks and downtime concerns. Vital information is backed up regularly and can be restored if in case we lost the original data. RAID - 1 provides mirror of two drives. If one gets disturbed, the other one contains the information. To protect a web site from loss of availability, which is due to DDoS attacks, the possible solutions are Intrusion Detection System (IDS); Intrusion Protection System. These attacks can cause loss of availability by the following reasons: Bandwidth Exhaustion, Memory exhaustion, CPU exhaustion [8].

HIPAA :

It is the Federal Health Insurance Portability and Accountability Act of 1996. The Portability section takes care of health care insurance plans. The accountability section deals with set of standards for receiving, transmitting, maintaining the health care information. The objective of this HIPAA, is to ensure confidentiality, integrity and availability for health care information [9].

The special challenges that are associated for these elements of triad are, huge volume of information must be assured, the sources are multiple and text involves various formats. These things are considered for security concern to provide reliable data transmission. Internet of things privacy is the another considered requirement to protect the information of individuals, which is publicly exposed.

Most common Denial of Service attacks are Ping attack, TCP (which stands for Transmission Control Protocol) SYN attack, ARP (which stands for Address Resolution Protocol) attack, Smurf attack. In this investigation, much attention has given to observe how these attacks effect the normal state EKG (Electrocardiogram) signal in operating systems Windows XP with SP 3,Windows Vista Ultimate, Windows 7 Enterprise, Windows 7 Ultimate with SP1, Windows 8 Enterprise, Windows 8.1 Enterprise.

1.2 Importance of the Problem

The above mentioned attacks are very common nowadays. These attacks can exhaust the resources in networks or victim computer. Authorized users can't access the network, sometimes applications may take longer time to open. In case, network attacks are operated on the computer, which is used to monitor EKG signals, the EKG information can be modified. Then, wrong diagnosis can happen. From the results of this research, EKG signal which is captured at rest position turned out to an abnormal EKG signal because of these attacks. The health care information must meet the standards of HIPAA and must not compromise with the CIA security triad.

1.3 Assumptions and Limitations

The EKG arrangement under rest position for any individual is not same as EKG pattern with work out state. In this research, the EKG signal at normal rest condition was considered, where bpm (beats per minute) are between 60-100. The subject's age is 28, whose EKG signal is captured for these experiments. The focus of investigation is to know how the attacked EKG signal varies from the normal EKG signal.

1.4 Outline

The main objective is to observe the effects of the above mentioned attacks on the data collection of EKG signals which are monitored. This thesis is classified in

Chapter I: Introduction to provide the details on how Denial of Service attacks (DoS) influencing today's internet and the significance of CIA security triad and HIPAA standards as well.

Chapter II : Electrocardiogram (EKG) signals and their abnormalities **,** description of some abnormalities that are associated with heartbeat. When attack was introduced to the computer, which monitors EKG signal, what are the possible effects on the data collection of EKG signals can be discussed in this chapter.

Chapter III : Background study of DDoS (which stands for Distributed Denial of Service) attacks, it covers an overview of different kind of Denial of Service .

Chapter IV : Effects of different network attacks on the data collection of EKG signals, this chapter includes the results of the attacked EKG signals which turned out abnormal with some abnormalities under different attacks.

Chapter V : Conclusions we present some conclusions.

CHAPTER II

EKG AND THEIR ABNORMALITIES

The method of monitoring the electrical activity of the heart over a period of time by keeping electrodes on the individual body is Electrocardiography. Placed electrodes captures the electrical activity on the skin that occurs from heart muscle depolarizing on heartbeat. The sensor from Vernier company called EKG - BTA is an educational purpose sensor, which has three electrodes to place on subject's body.

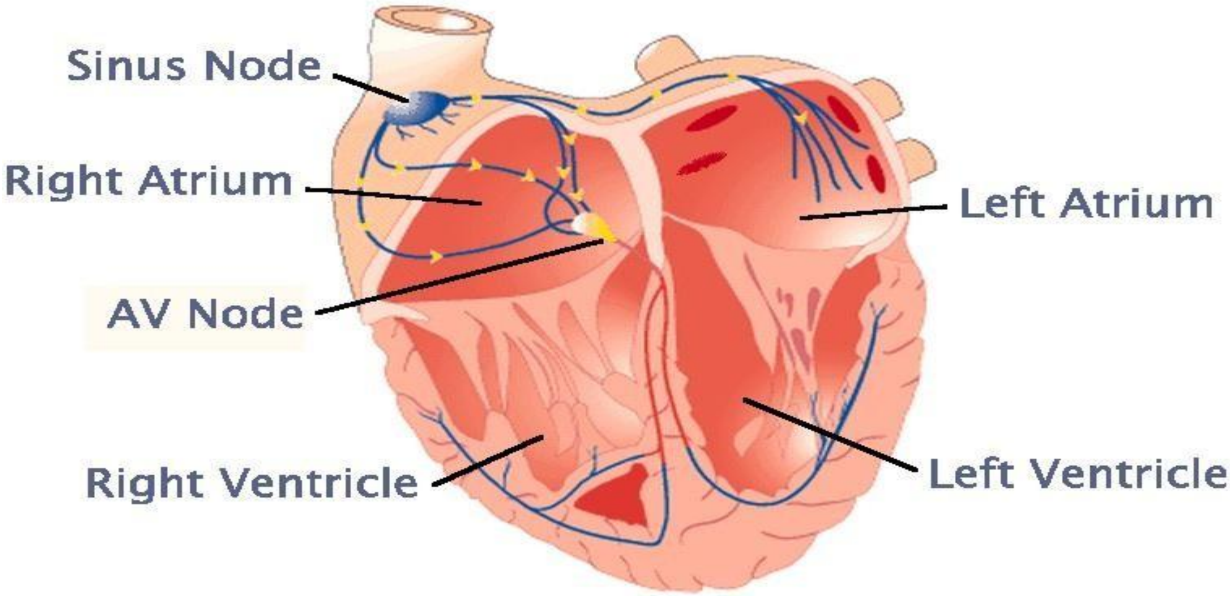


Fig 2.1 . Heart of the human body [10]

The heart has four chambers - two at the top (the atria) and two at the bottom (the ventricles). The obvious trigger for the heart to contract occurs from the heart's natural pacemaker, the SA (which stands for Sinoatrial) node, which is in the top chamber. The SA node pushes out regular electrical impulses causing the atrium to contract and for pumping blood into the bottom chamber (the ventricle). The electrical impulse then passes to the ventricles through a form of 'junction box' called the AV node (Atrio-Ventricular node). This electrical impulse spreads into the ventricles, causing the muscle to contract and then pump blood to the lungs and the body [10].

The SA node automatically depolarizes at a rate of about 70 bpm. Each segment of the conduction system immediately depolarizes at a progressively lower rate. If the SA node stopped having action potentials, or if each portion of the heart was divided and try to understand separately, the atrial muscle cells would depolarize approximately by 60 bpm. In the absence of SA node, or atrial muscle initiation of depolarization in the heart the AV node could take over as the pacemaker [11].

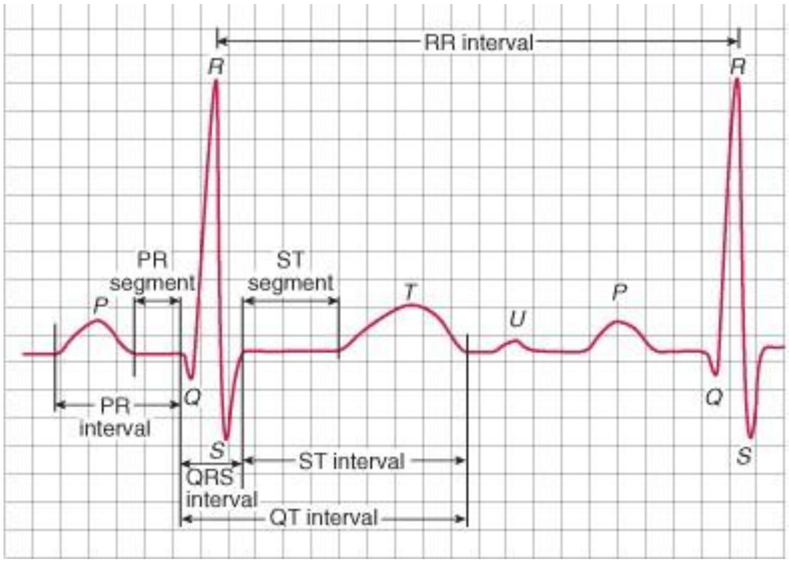


Fig 2.2. EKG signal [12]

2.1 Details of EKG waves and their intervals

P wave: It represents the sequential activation of the right and left atria. Depolarization goes continuously from right to left, where we can see the right atrium deflection first and then left atrium. It is the first visible positive deviation in EKG signal.

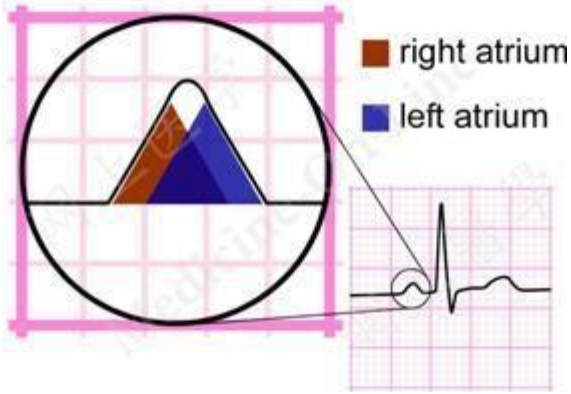


Fig 2.3 . Normal P wave in EKG [13]

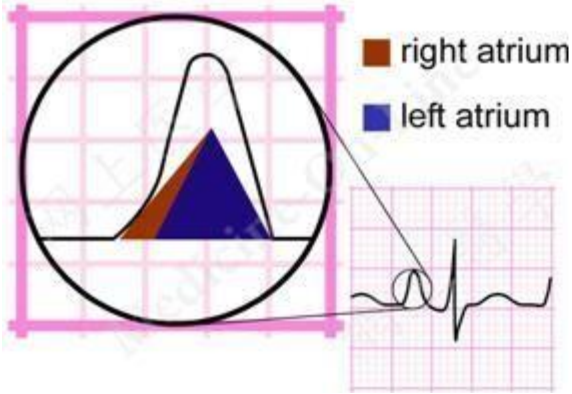


Fig 2.4. Right Atrial Enlargement [13]

The abnormalities related with P wave are Left Atrial enlargement, Right Atrial enlargement. Left Atrial Enlargement is due to pressure overload of the left atrium. Right Atrial Enlargement produces peaked P waves.

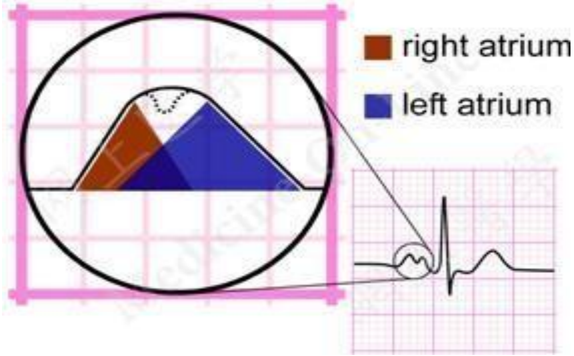


Fig 2.5. Left Atrial Enlargement [13]

Inverted P waves :

When the PR interval is less than 120ms, the origin of the heartbeat signal is from the AV junction.

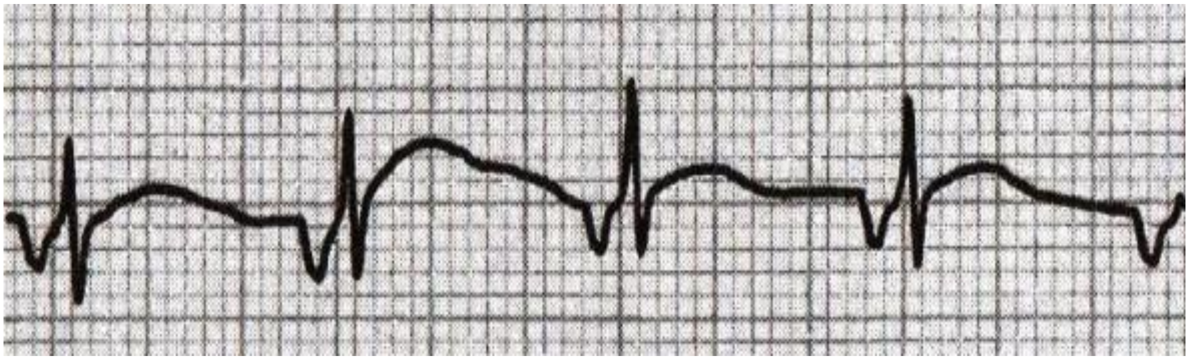


Fig 2.6 . Accelerated Junctional Rhythm [13]

When the PR interval is less than 120ms, the origin of the heartbeat signal is from the atria.

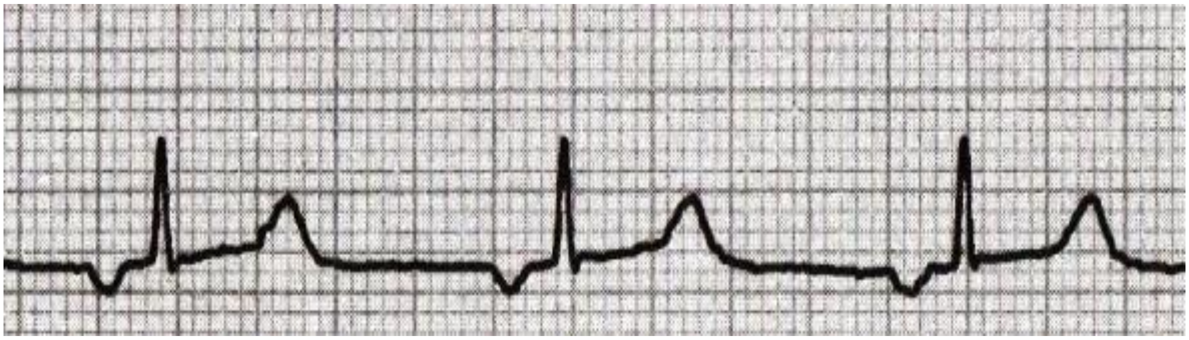


Fig 2.7. Ectopic Atrial Rhythm [13]

If more than three different P wave morphologies are observed, then multifocal atrial rhythm is considered.

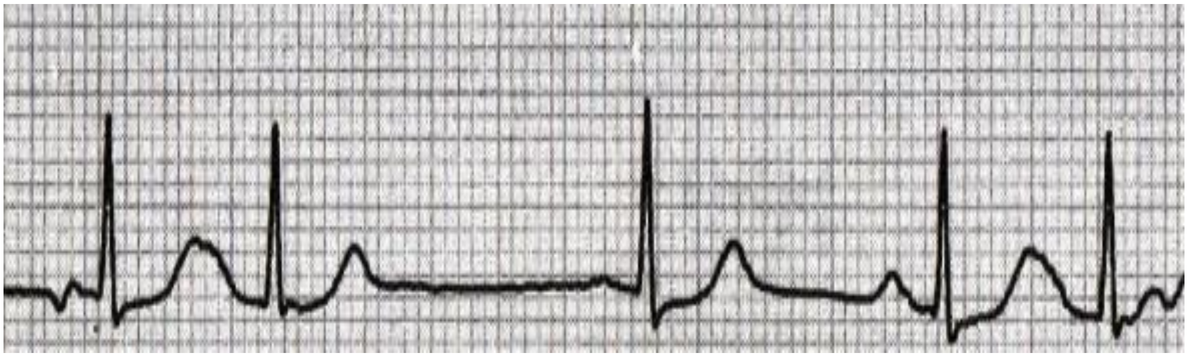


Fig 2.8 . Multifocal Atrial Rhythm [13]

If more than three different P wave morphologies are seen and the heartbeat rate is greater than 100(bpm), then multifocal atrial tachycardia (MAT) is considered.

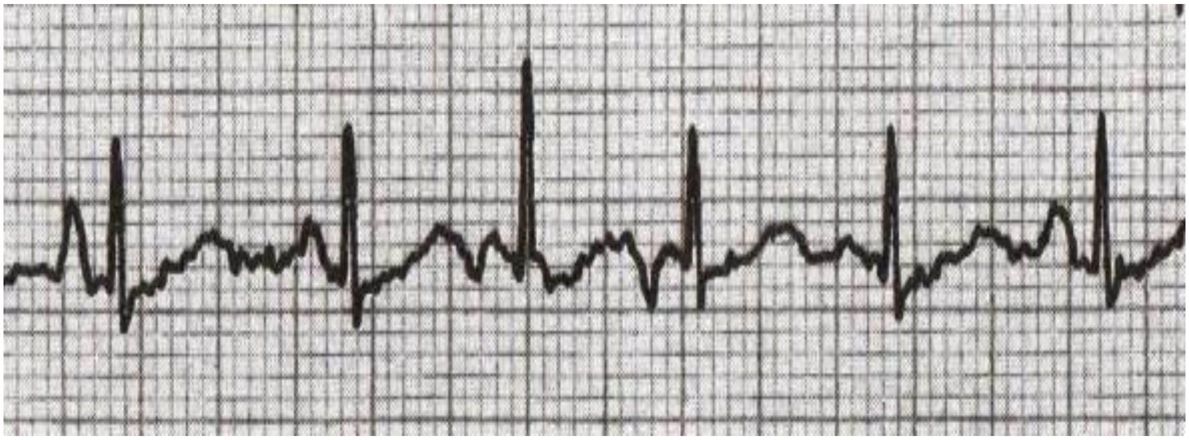


Fig 2.9 . Multifocal Atrial Tachycardia [13]

QRS complex: It represents the simultaneous activation of the right and left ventricles, although most of the QRS waveform is derived from the larger left ventricular musculature. It is present in both narrow and broad complexes [7]. Narrow QRS complex (QRS < 100ms) are from supraventricular origin. Broad complexes are because of either ventricular in origin or equal conduction of supraventricular complexes. Narrow QRS complexes comes in three cases :

Case I : Each QRS complex is preceded by normal P wave.

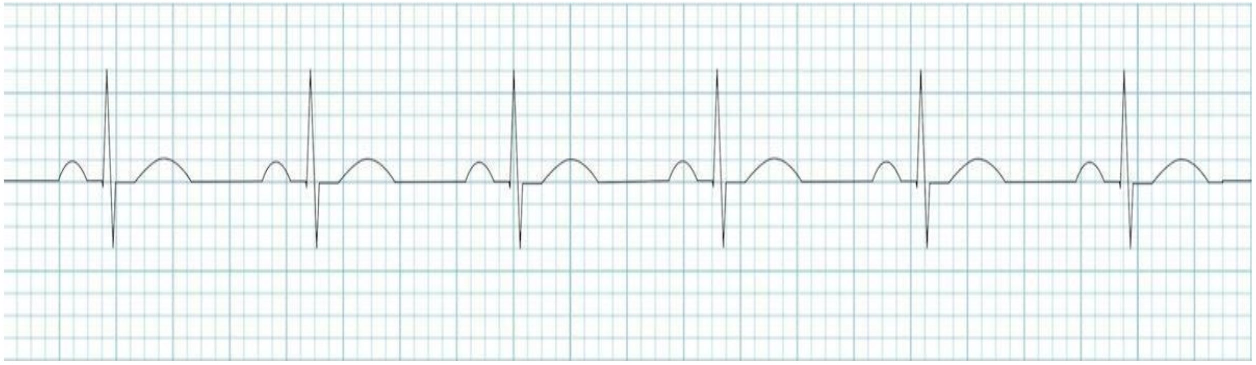


Fig 2.10 . Case I in Narrow QRS complexes [13]

Case II : QRS complexes with flicker regular waves.

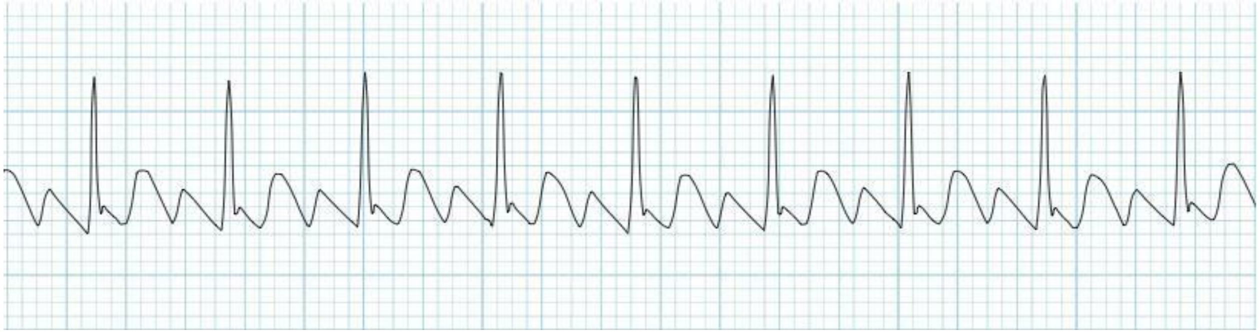


Fig 2.11. Case II in Narrow QRS complexes [13]

Case III : There will be no P waves, just narrow QRS complexes.

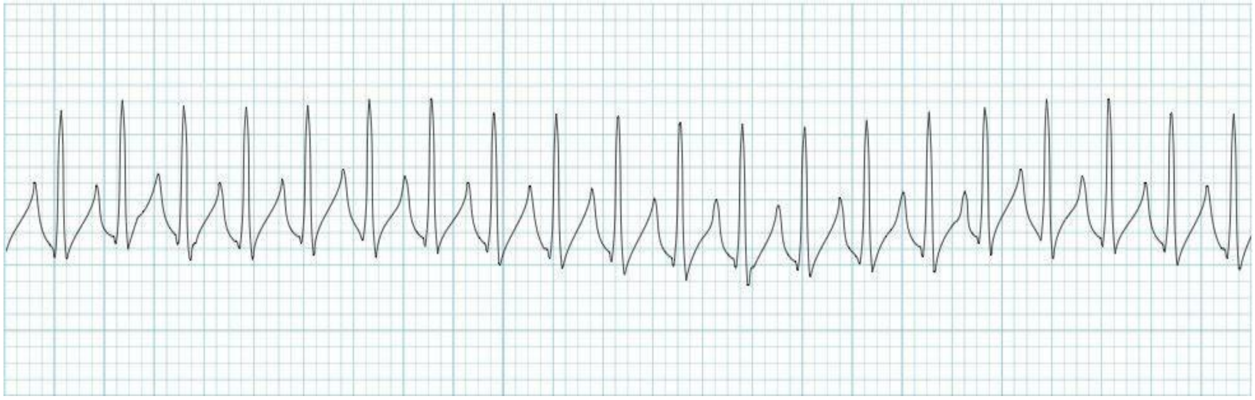


Fig 2.12 . Case III in Narrow QRS complexes [13]

Broad Complexes occurs in some cases where P waves are invisible. This abnormality is called Ventricular Tachycardia.

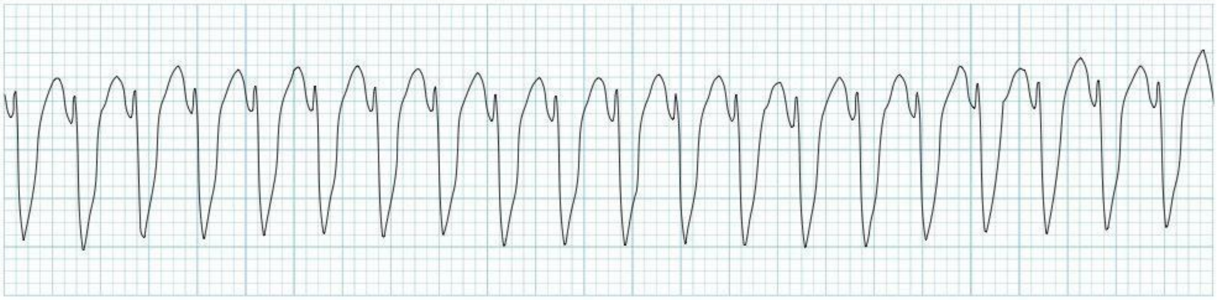


Fig 2.13 . Broad QRS complexes [13]

T- wave : It represents ventricular repolarization. It is the immediate positive deviation after QRS complex. The abnormalities in T wave are:

Peaked T waves : Tall T waves are seen in the case of the abnormality hyperkalaemia. Treatment of life-threatening hyperkalaemia focuses on blocking the effects on myocyte transmembrane potential and cardiac conduction, as well as decreasing extracellular potassium levels.

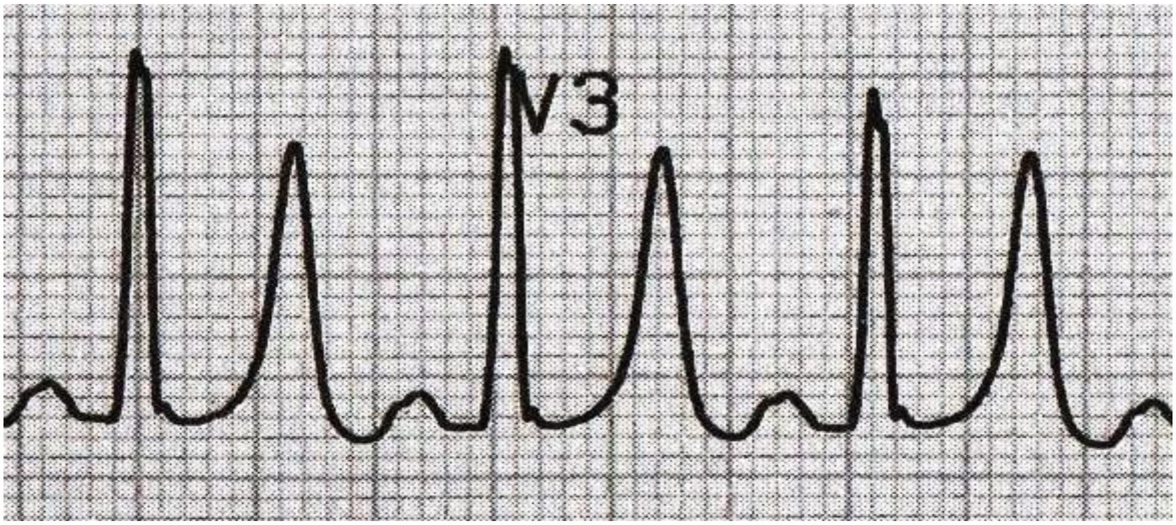


Fig 2.14 . Abnormality Hyperkalaemia [13]

Hyperacute T waves : They can be seen in initial points of ST elevation MI (STEMI)

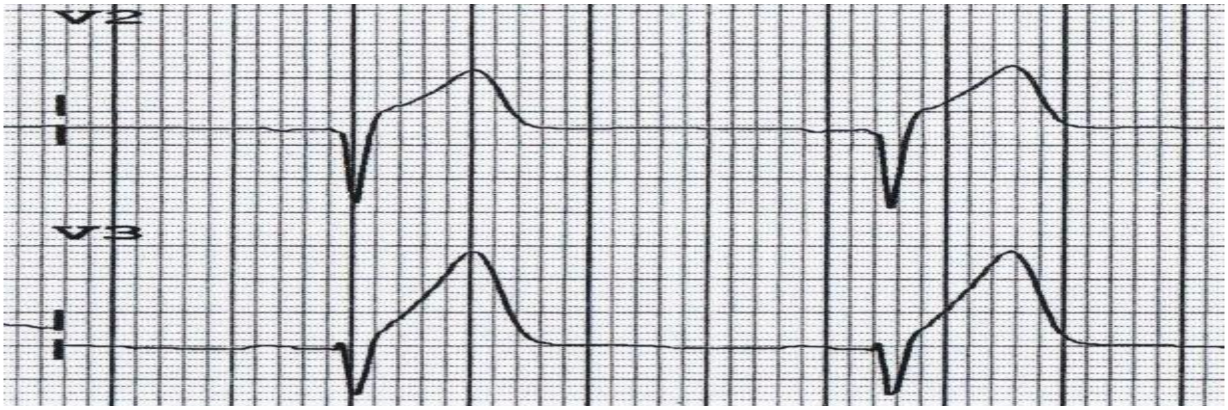


Fig 2.15 . Hyperacute T waves [13]

Biphasic T waves : The two causes of biphasic T waves are Myocardial Ischaemia and Hypokalemia.

1) Myocardial Ischemia

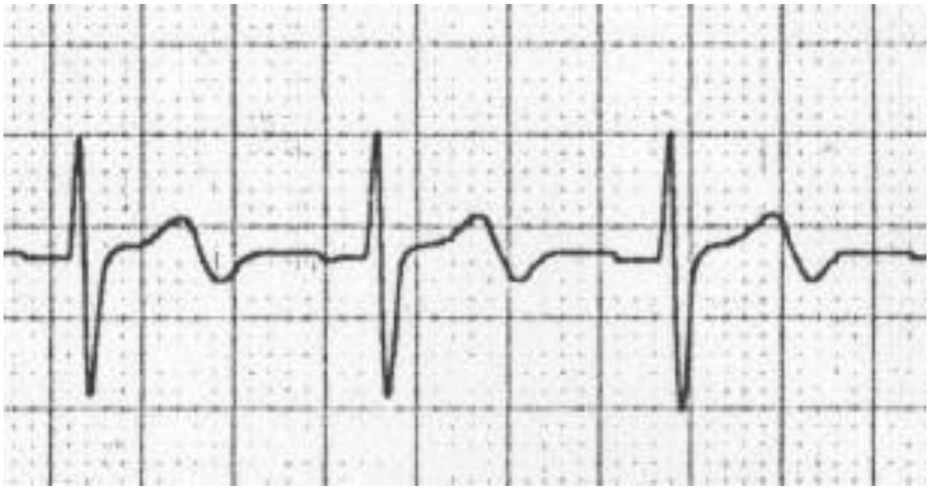


Fig 2.16 . Biphasic T waves which goes up and down [13]

Here, T waves goes up and down.

2) Hypokalaemia

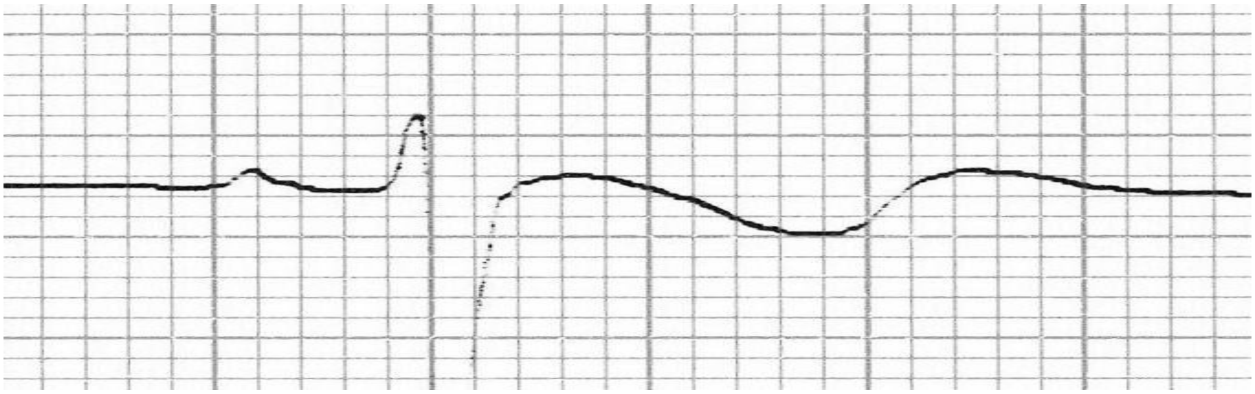


Fig 2.17 . Biphasic T waves which goes down and up [13]

Here, T waves go down and up.

Camel - hump T waves :

One cause for this kind of abnormality is bulging U waves at the end of T wave. This can happen in hypokalaemia.

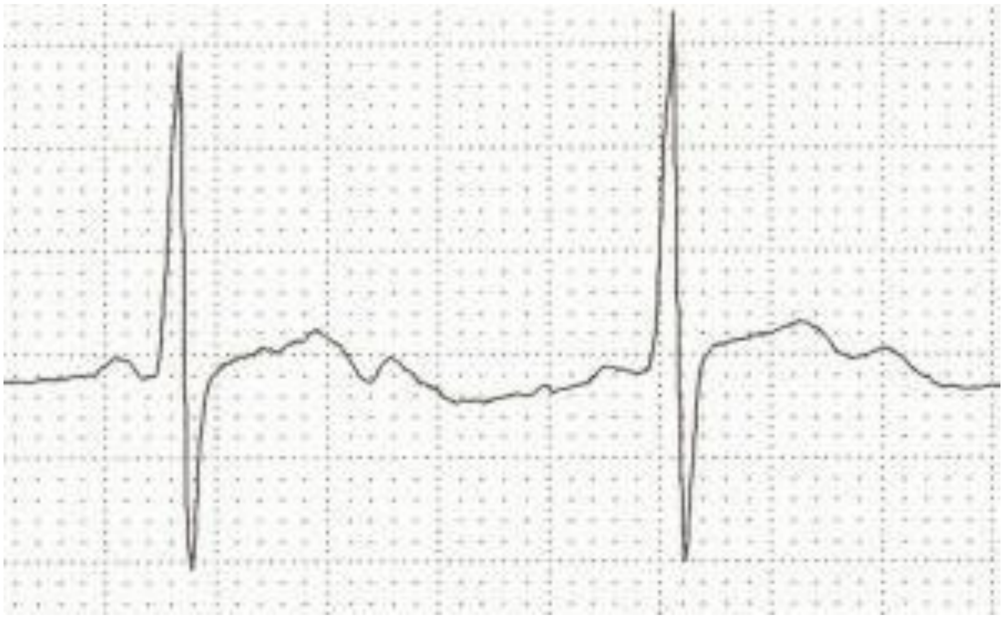


Fig 2.18 . Camel hump T waves [13]

Another cause is covered p waves, in case of heart block or sinus tachycardia.

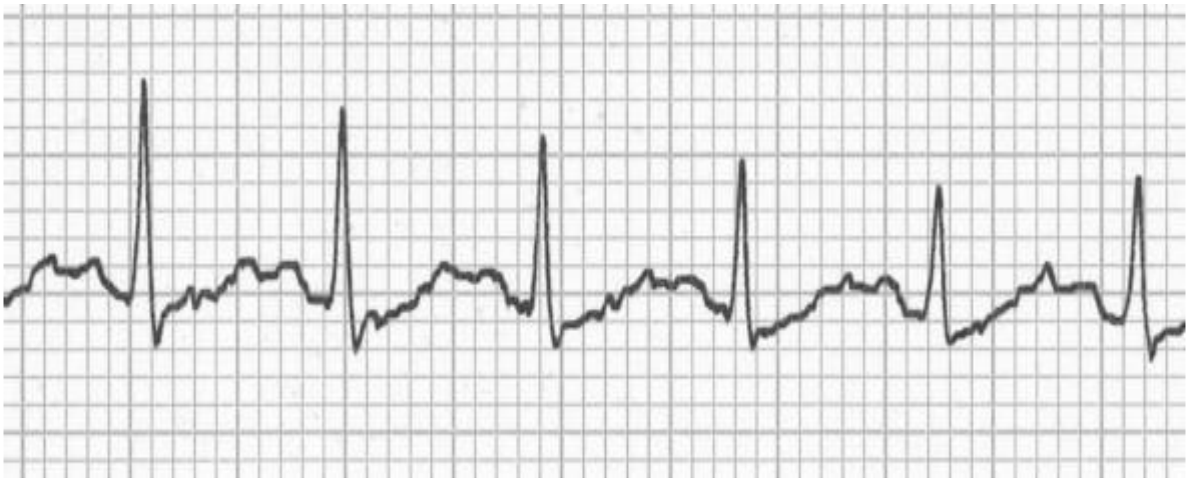


Fig 2.19 . Covered P waves in Sinus Tachycardia [13]

Wellen's Syndrome : There are two arrangements of T wave abnormality Type I includes deeply inverted ones.

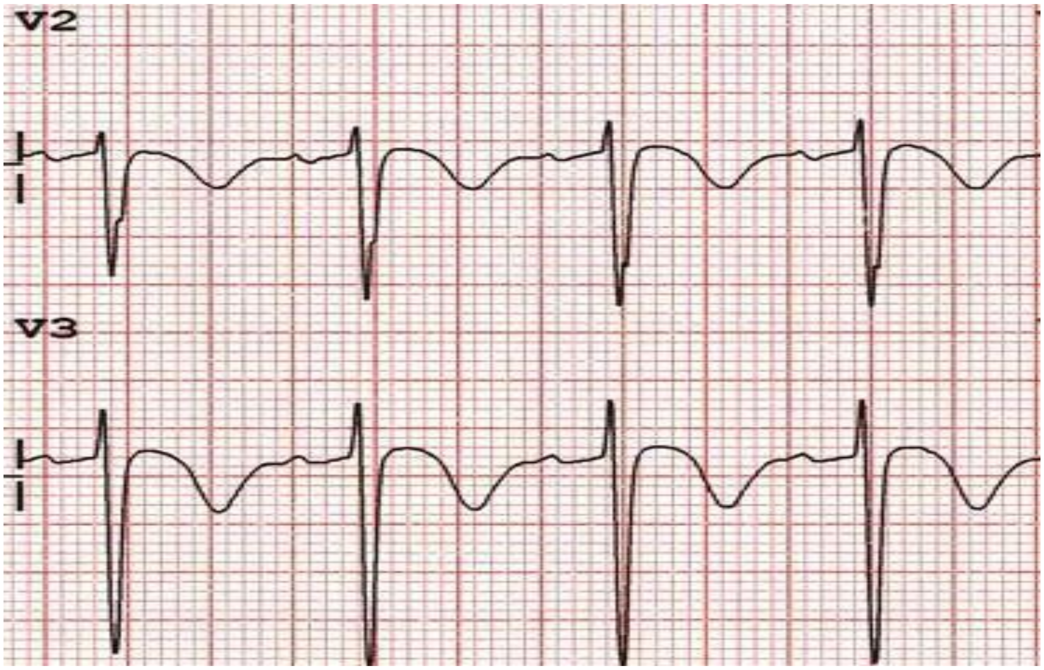


Fig 2.20 . Wellen's Syndrome Type I [13]

Type II includes byphasic which has both positive and negative deflections.

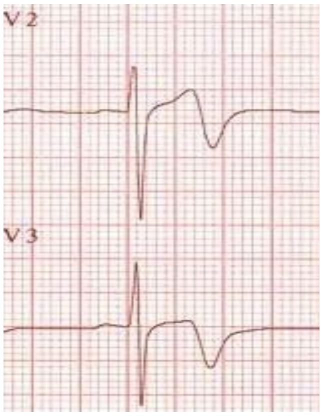


Fig 2.21 . Wellen's Syndrome Type II [13]

U wave: It is the small deviation which is next to the T wave. It normally follows T wave direction. It occurs because of delayed repolarization of Purkinje fibers. It is visible if the heartbeat count is less than 65 (bpm< 65) .

Abnormalities of U wave :

Bulging U waves can be seen in severe hypokalemia and sinus bradycardia.

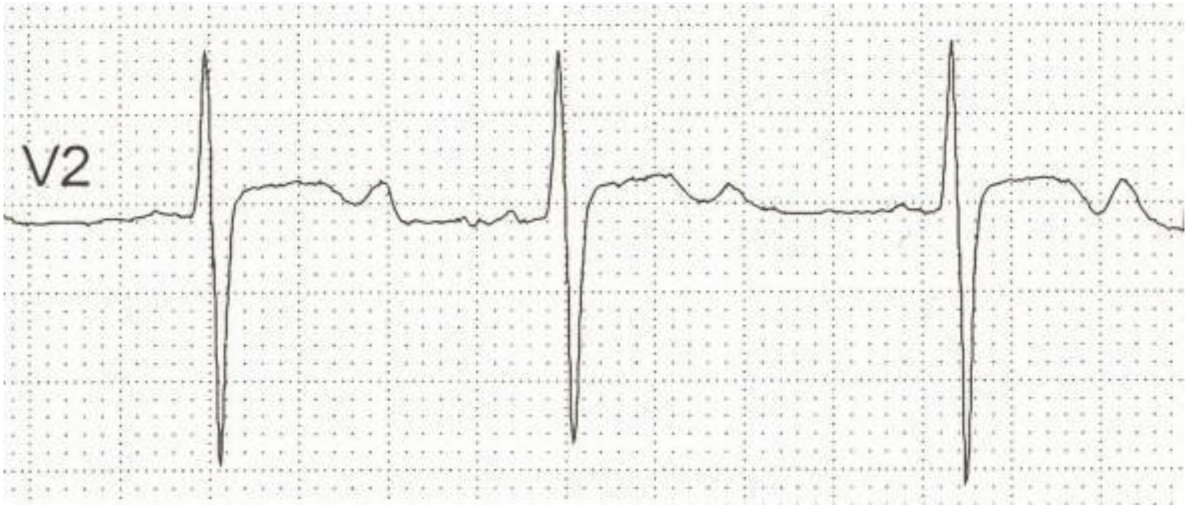


Fig 2.22 . Bulging U waves in some abnormalities [13]

Inverted U waves occurs because of Coronary artery disease, hypertension, Hyperthyroidism.

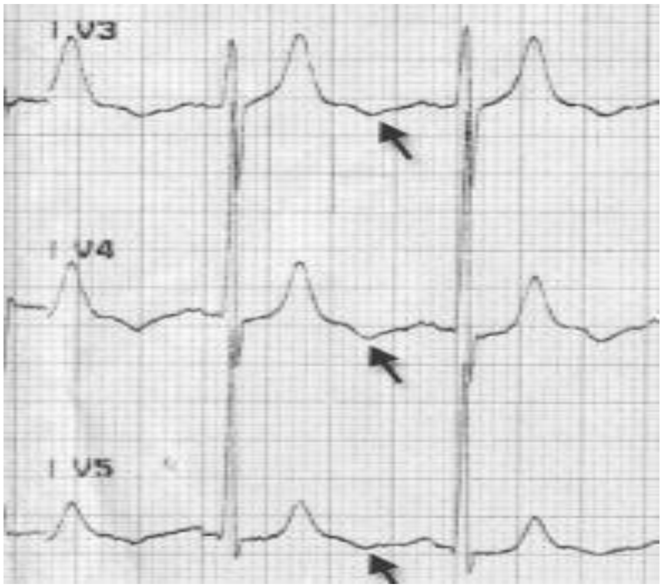


Fig 2.23 . Inverted U waves in some abnormalities [13]

PR Interval : This interval starts with P wave and ends with origin of QRS complex. It indicates conduction through the AV node. Normally it lies between 120ms - 200ms interval. If the PR interval is more than 200 ms, then the first degree heart block abnormality is noticed. If the interval time is less than 120ms, then AV Nodal (junctional) rhythm is considered.

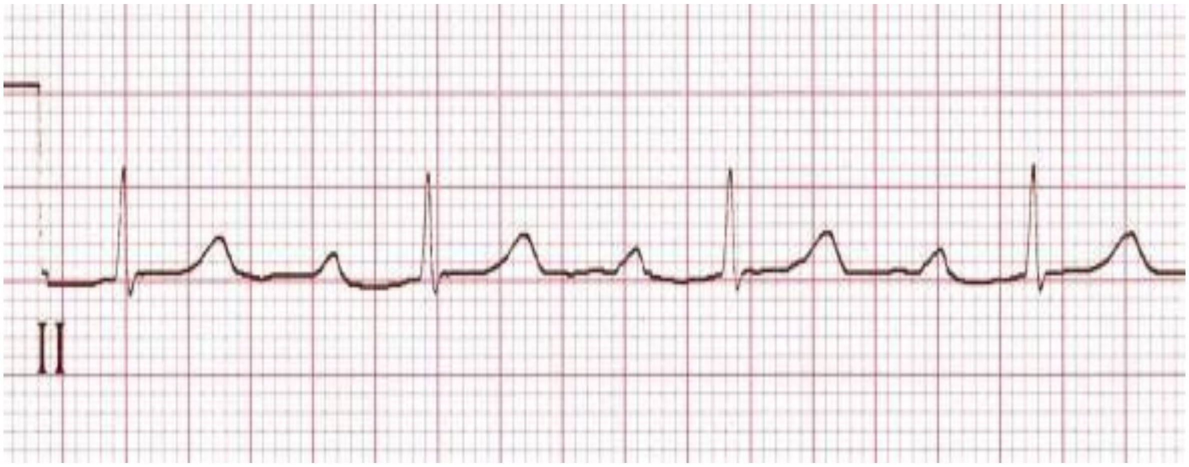


Fig 2.24 . First Degree Heart Block, PR interval > 200ms [13]

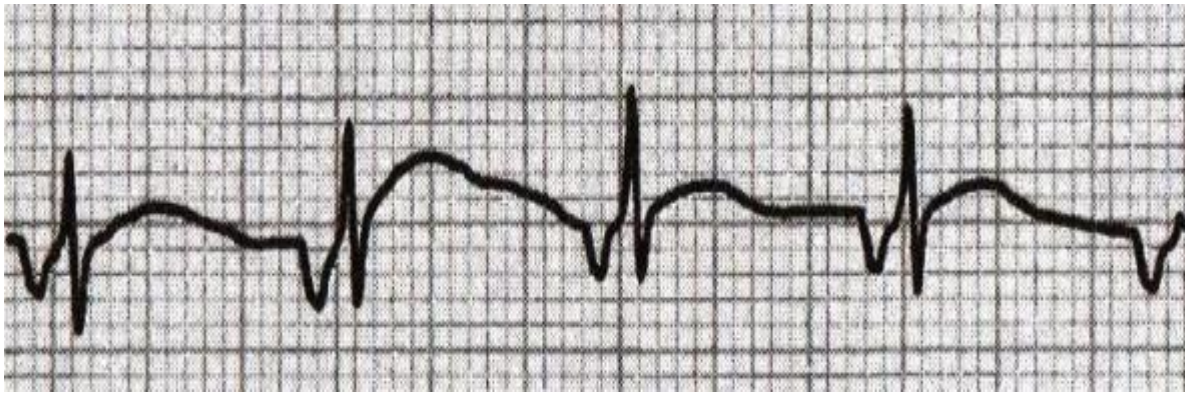


Fig 2.25. Accelerated Junctional Rhythm which has PR interval < 120ms [13]

There are another special kind of abnormalities which comes under PR interval < 120ms. It happens because of Pre-excitation syndromes. They are Wolff - Parkinson - White (WPW) and Lown - Ganong - Levine (LGL) syndromes. Characteristics of Wolff - Parkinson - White (WPW) syndrome are short PR intervals and broad QRS complexes. In Lown - Ganong - Levine syndrome we can notice short PR intervals and QRS complexes will be invisible.

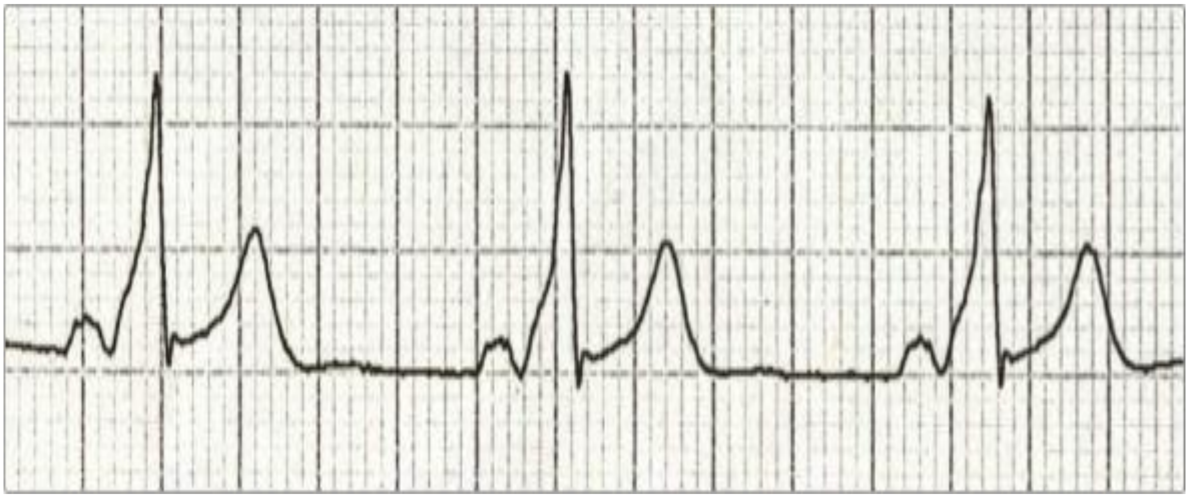


Fig 2.26 . Wolff - Parkinson - White (WPW) syndrome [13]

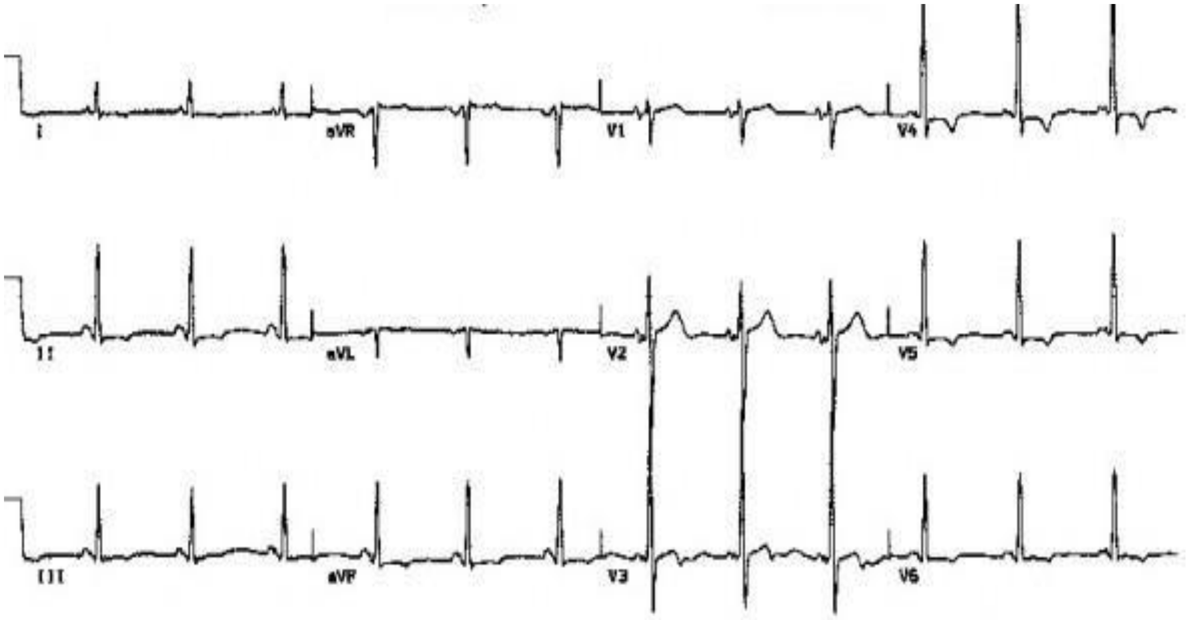


Fig 2.27 . Lown - Ganong - Levine (LGL) syndrome [13]

QT Interval : It is the time from origin of Q wave and end of T wave. It indicates Ventricular depolarisation and repolarization. There is a relation with heart rate for this QT interval. The interval is short in case of fast heart beat and it extends when the heart beat is slow. Presently research confirms that short QT syndrome leads to increase in risk of paroxysmal atrial , ventricular fibrillation and abrupt cardiac attack.

ST segment : The critical cause of this segment is myocardial infarction. Pericarditis, Benign early repolarization, left ventricular hypertrophy are some other causes of ST segment elevation. ST segment represents the end of ventricular conduction and the start of ventricular repolarization. Changes in this segment gives myocardial harm.

Table 2.1 . Details of PQRST intervals in EKG signal and their significance [14]

Name of the wave/segment	Importance	Location	Duration (sec)
P wave	It is the first component of a normal ECG signal	Precedes the QRS complex	0.06 to 0.12
PR interval	It tracks the atrial impulse from the atria through AV node, bundle of His, and right and left bundle branches	Beginning of P wave to beginning of QRS	0.12 to 0.20
QRS wave	It represents depolarization of ventricles, intraventricular conduction time.	Follows PR interval	0.06 to 10
ST segment	It represents the end of ventricular depolarization and start of ventricular repolarization.	Extends from S wave to origin of T wave	
T wave	It represents the Ventricular	Follows S wave	

	repolarization.		
QT segment	It shows the time needed for ventricular depolarization-repolarization cycle. Any problems here leads to myocardial issues.	Beginning of QRS to end of T wave	0.36 to 0.44
U wave	It represents the recovery period of ventricular conduction fibers.	Follows T wave	

2.2 Abnormalities in Electrocardiogram (EKG)

Normal Sinus Rhythm:

This rhythm is regular. Sinus rhythm is obvious if its frequency stays between 60-100/ min. P-QRS-T follows the same order and they are differentiable. Here, QRS complex is preceded by actual P wave. We get same value for PR interval for every heartbeat. Normal heartbeat rates :

For Newborn :	110 - 150 bpm
2 years old :	85 - 125 bpm
4 years old :	75 - 115 bpm
6 years old + :	60 - 100 bpm

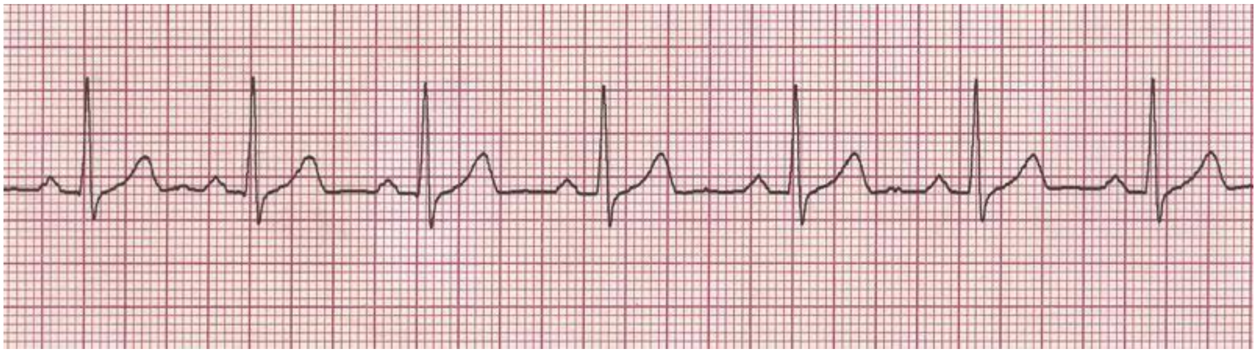


Fig 2.28 . Normal Sinus Rhythm [15]

Sinus bradycardia:

Sinus Rhythms are named due to locus of stimulation being at SA (sinoatrial) node. Sinus rhythm, if its frequency stays less than 60/min, then it is said to be sinus bradycardia. This one is caused because of increased vagal, fainting attacks. Sinus bradycardia can happen during sleep due to decreased metabolic demands. Non cardiac diseases , like hyperkalemia, hypothyroidism, hypothermia are the causes of Sinus bradycardia.

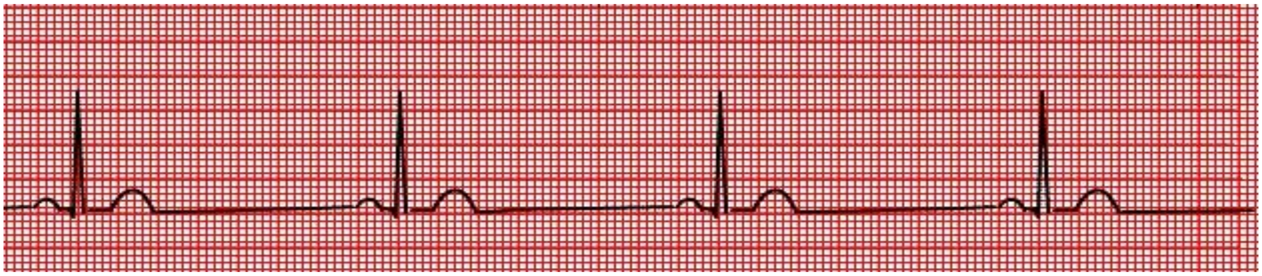


Fig 2.29 . Sinus bradycardia [15]

Sinus tachycardia:

Sinus rhythm, if its frequency stays more than 100/min, then it is said to be sinus tachycardia. This one is caused because of physiological response, pain, fear. At higher heartbeat rates, myocardial demands for oxygen are increased. In that case, tachycardia can trouble the heart and produces severe pain. The QT interval normally shortens and P wave may combined with preceding T wave, and it may be difficult to identify, QRS complex may increase its amplitude , with tachycardia.

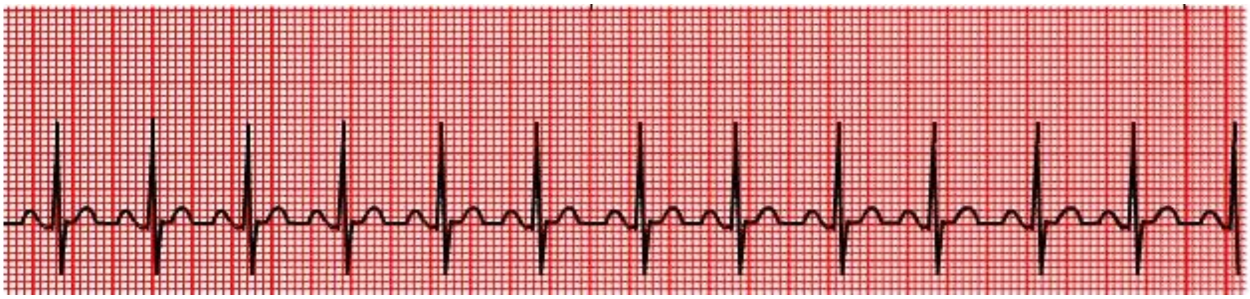


Fig 2.30 . Abnormality Sinus Tachycardia [15]

Sinus arrhythmia:

In this case, the PP or RR interval exceeds the shortest interval by 0.16 s. This one is common in all age groups. It occurs normally because of vagus nerve which mediates respiration as well as heart rhythm. The important change happens at the time interval between T wave and the next P wave.

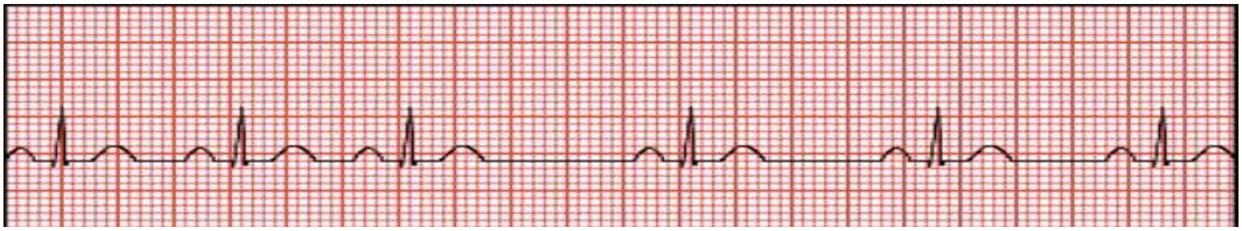


Fig 2.31 . Abnormality Sinus Arrhythmia [15]

Atrial Flutter:

The interval between end of T and origin of P wave disappears, when the heartbeat rate is increased. This abnormality is called Atrial flutter, a supraventricular tachycardia . Saw tooth P waves are present. P waves lose their distinction due to increased atrial rate. QRS complex is normal, however, may be widened if the flutter waves are hidden in the complex. T wave is not visible in this abnormality. QT interval cannot be measured as we don't see T wave.

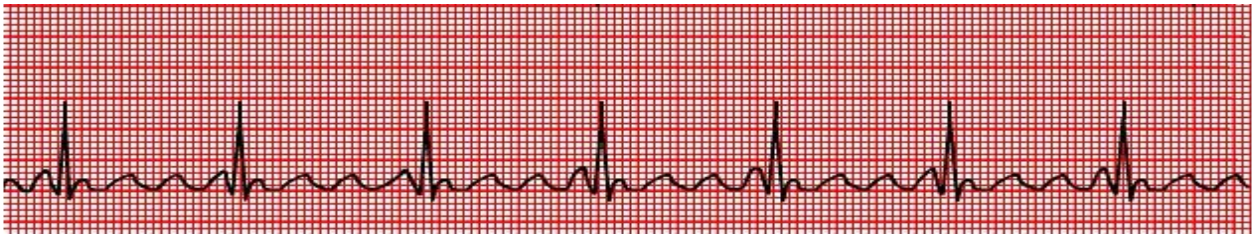


Fig 2.32 . Abnormality Atrial Flutter [16]

Atrial fibrillation:

The activation in the atria may also be fully irregular and chaotic, producing irregular fluctuations in the baseline .The QRS wave will be normal and rest follows the irregular fluctuations in the baseline. T wave occurs because of hyperthyroidism and pericarditis. The ventricles respond to those pulses coming through the AV node. In this case, P wave doesn't represent atrial activity, but fibrillation waves represent it. R waves are irregular in Atrial fibrillation. We can't measure QT interval in the EKG signal at this abnormality. T wave and PR interval are vague.

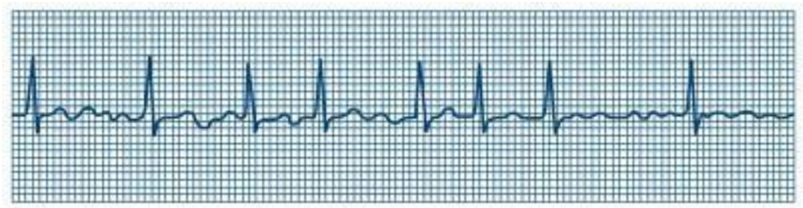


Fig 2.33 . Abnormality Atrial Fibrillation [16]

Junctional Escape Rhythm:

Junctional escape rhythm happens after the conduction delay from the atria. It can be caused by conditions that disturbs SA node. P waves are inverted , QRS complexes are typically normal. This occurs somewhere at AV junction. This rhythm has heartbeat rate of 40 - 60 bpm.

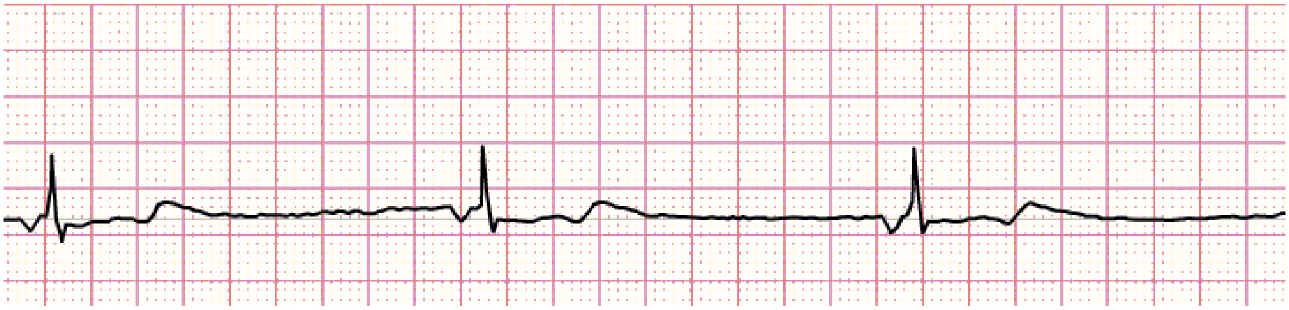


Fig 2.34 . Junctional Escape Rhythm [17]

Premature Ventricular Contraction:

The immature heartbeat originating from an ectopic focus in the ventricles. Basically these immature contractions are classified based on their origins, like atrial (PACs), junctional (PJCs), and ventricular (PVCs). The EKG signal features for this abnormality are broad QRS complex, different ST segment and changes in T wave. Discordance happens when ST segment with upright T waves in leads with strong S wave. The normal direction of septal depolarization is inverted as impulse advances to Right ventricles (RV) and then Left Ventricles (LV) via the septum. As ventricles are activated in the process from right to left, but not simultaneously this could give the broad QRS complex.

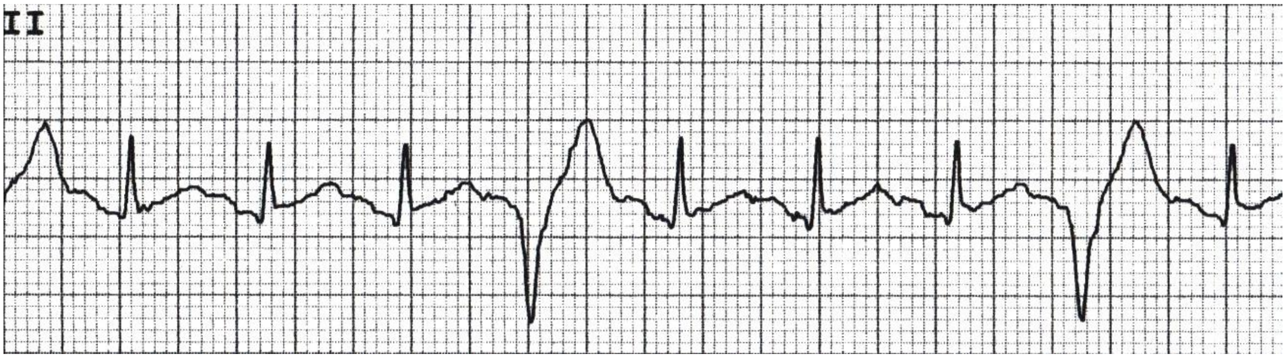


Fig 2.35 . Premature Ventricular Contraction [17]

Ventricular Fibrillation:

In this case, we can observe disorder in ventricular depolarization. This can be seen in the ECG comes without QRS complexes. In this arrhythmia the contraction of ventricular muscle is not proper and also inefficient at pumping blood.

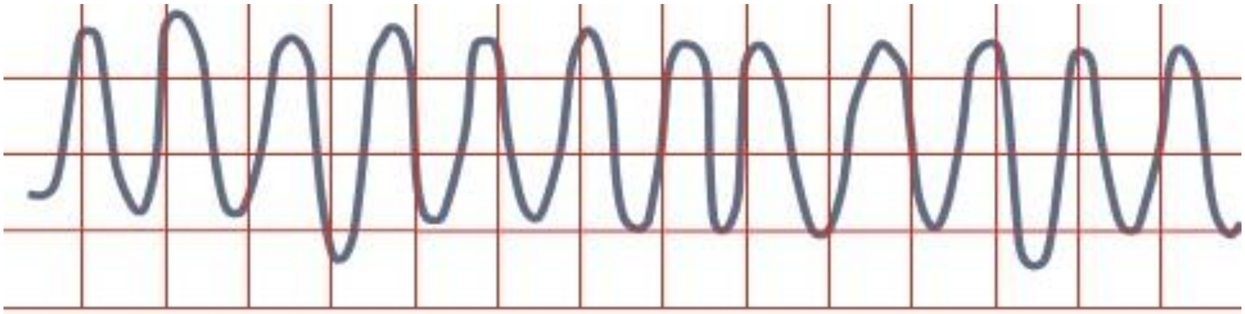


Fig 2.36 . Ventricular Fibrillation [17]

Pericarditis :

Infection of the pericardium generates chest pain and tachycardia. Involvement of underlying epicardium occurs which is indicated by widespread ST segment. We recognize Pericarditis in EKG with ST elevation and PR depression occurs in the same level. Moreover, ST depression and PR elevation coincides [18].

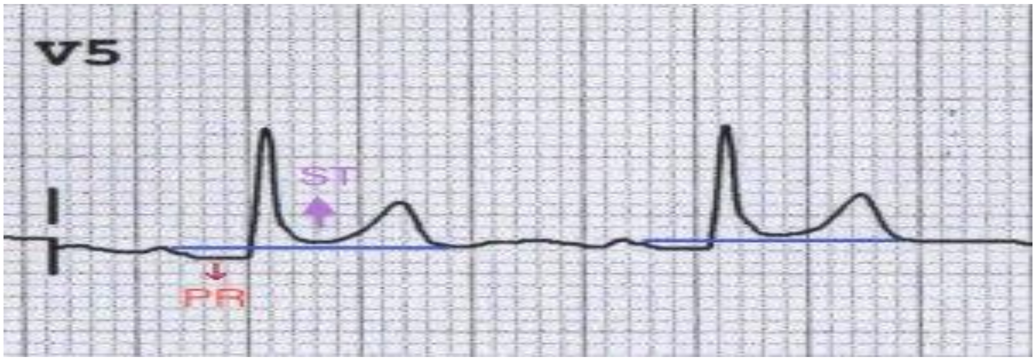


Fig 2.37 . PR depression and ST elevation in Pericarditis [18]

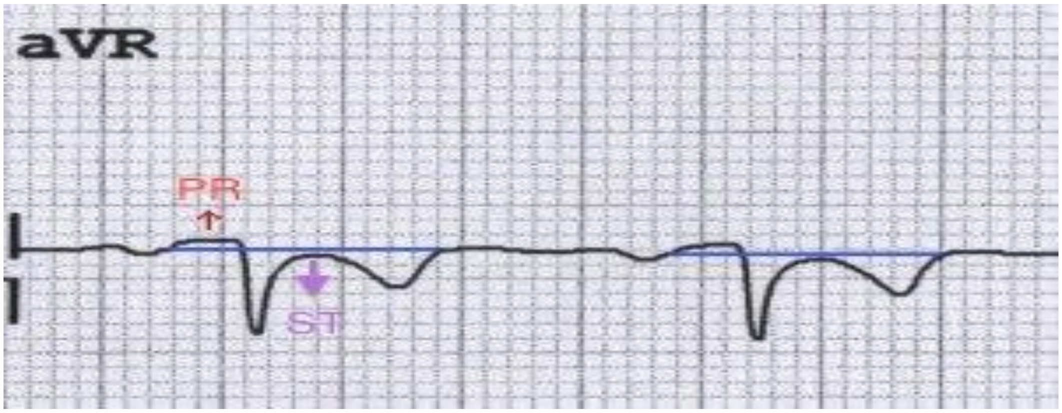


Fig 2.38. PR elavation and ST depression in Pericarditis [18]

Hyperkalaemia: Tall T waves or peaked T waves are visible in this type of abnormality. The electrolyte Potassium (k^+) level in the blood increases and peaked T waves and shortened QT interval appear. To avoid risk, temporary treatment will be given, however removal of unwanted potassium level can be done by stimulating urine or dialysis.

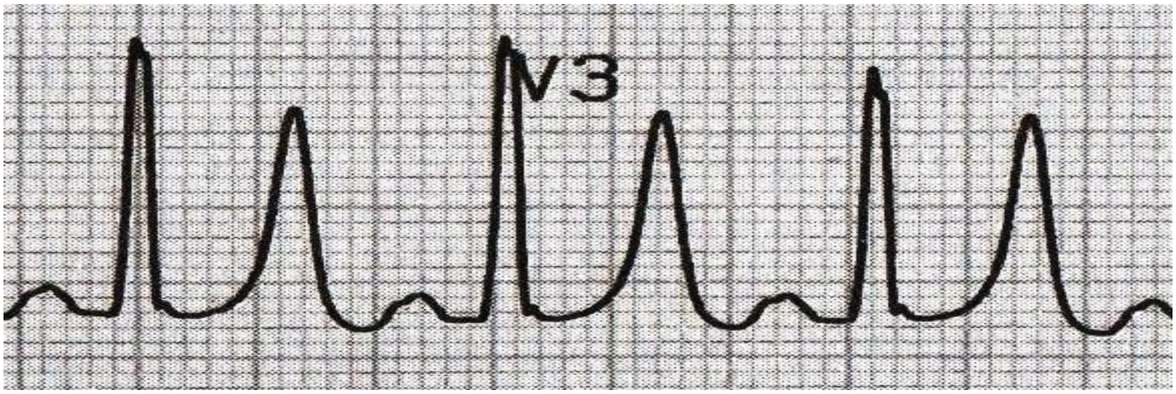


Fig 2.39 . Hyperkalaemia representing Peaked T waves [19]

Hypothermia :

When the core body temperature is less than 35 degree centigrade, it is called as Hypothermia. If the body temperature is between 32-35 degrees, then it is said to be mild Hypothermia. If the body temperature is between 29-32 degrees, then it is called moderate Hypothermia. If the body temperature is less than 29 degrees, then it is severe Hypothermia.

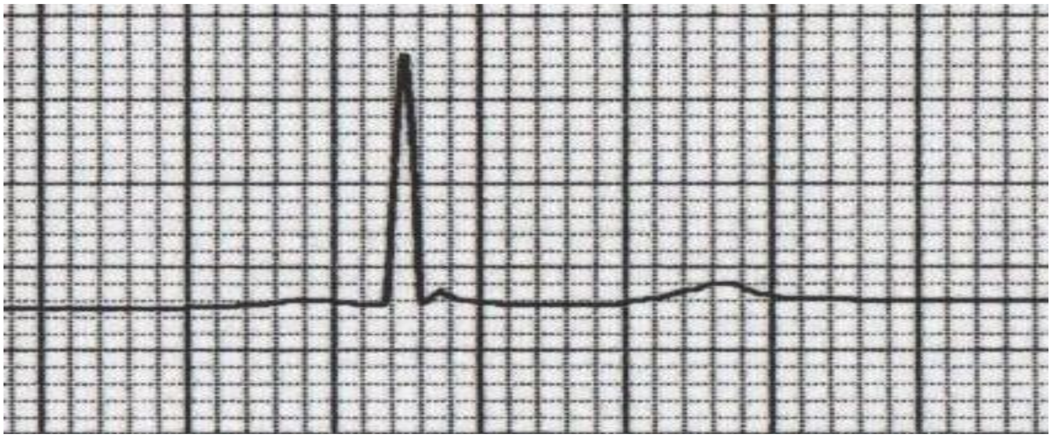


Fig 2.40 . Subtle Osborn waves in mild hypothermia (temp 32.5 degrees C) [13]

We can see J wave deviation in moderate Hypothermia, and in our research results we can notice that this kind of abnormality is observed in attacked EKG signals under different network attacks.

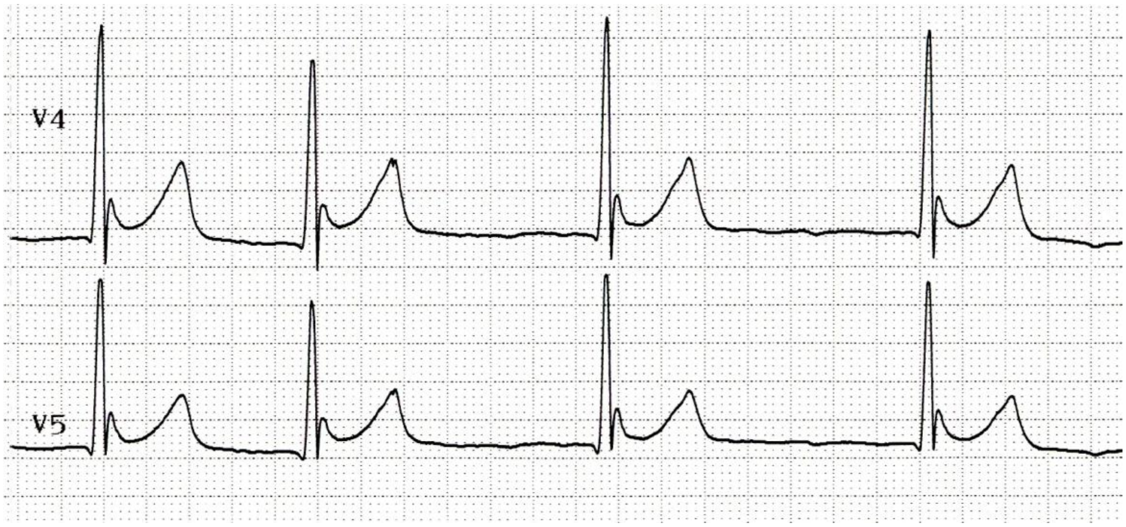


Fig 2.41 . J waves in moderate hypothermia (30 degrees C) [13]

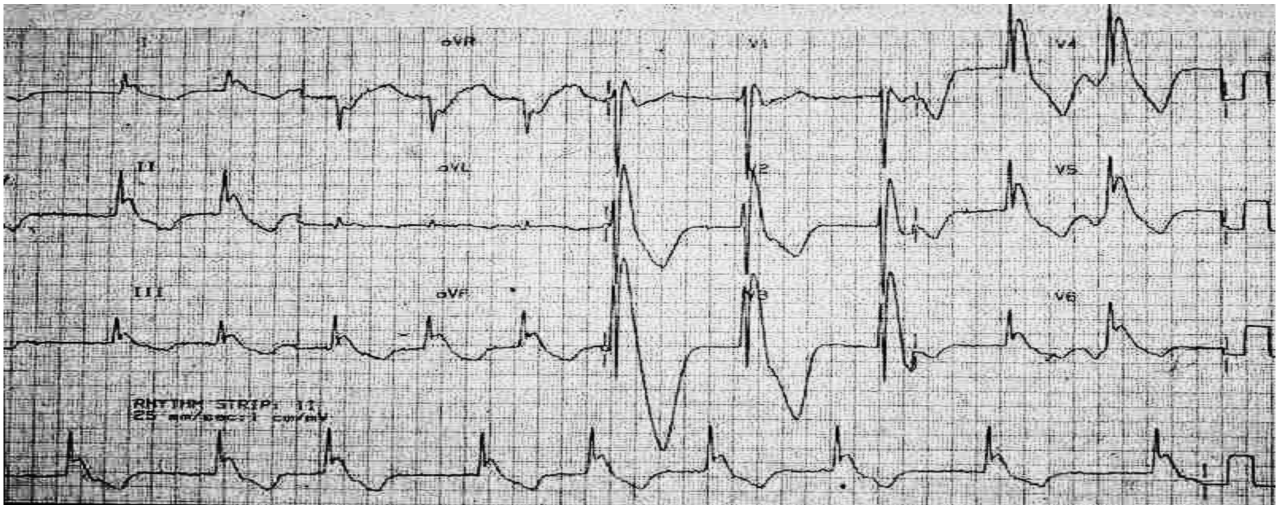


Fig 2.42 . Marked Osborn waves in severe hypothermia [13]

Hypothyroidism : This abnormality shows low voltage QRS, bradycardia and widespread T waves. EKG may change secondary to effects on myocardium of reduce levels of thyroxine. Decreased activity of the sympathetic nervous system.

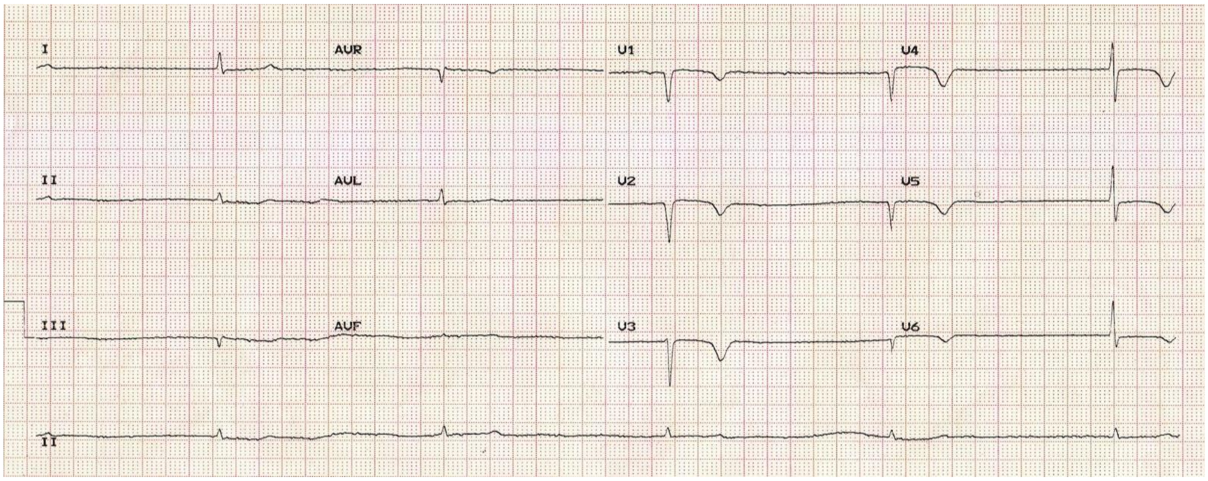


Fig 2.43 . Hypothyroidism [13]

First Degree Heart Block :

When PR interval > 200ms, then it is said to be First degree heart block.

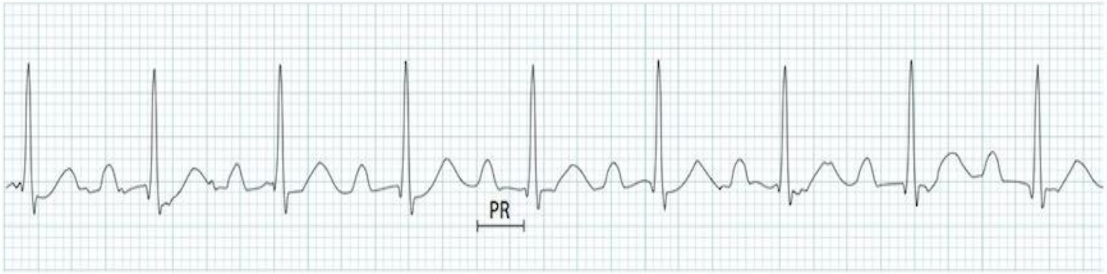


Fig 2.44 . First Degree Heart Block with abnormal PR interval [20]

Multifocal Atrial Tachycardia :

The heartbeat rate for this kind of abnormality is above 100 bpm. Irregular EKG waveform with different PP, PR and RR intervals. A irregular atrial rhythm arising from multiple ectopic foci within the atria. More than three different forms of P wave are present in the EKG signal.

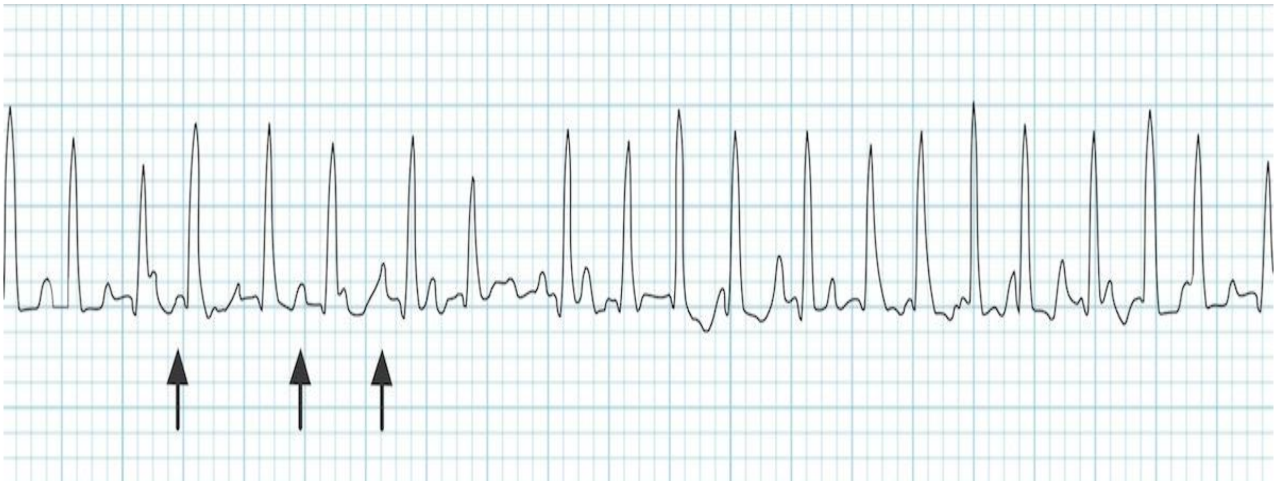


Fig 2.45 . Multifocal Atrial Tachycardia showing more different P waves [21]

Anterior Myocardial Infarction :

It carries the worst prognosis of all infarct locations, due to larger infarct size. The change in EKG signal are ST elevation with Q wave formation.

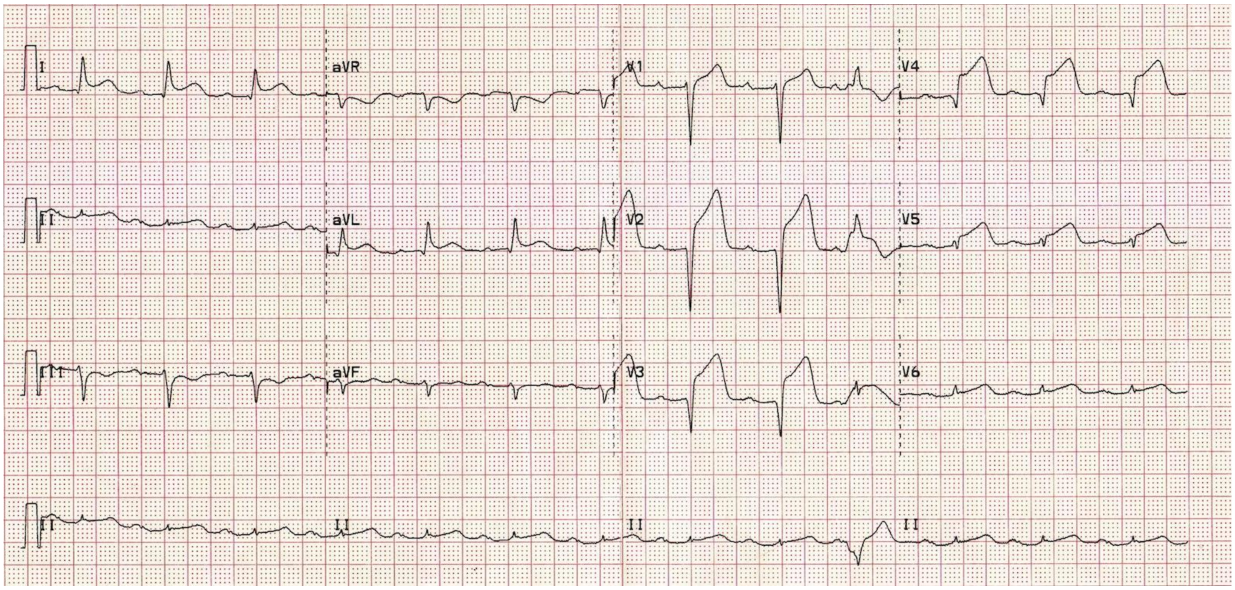


Fig 2.46 : Anterior Myocardial Infarction [13]

CHAPTER III

BACKGROUND STUDY ON DOS ATTACKS

Deny of access to valid users, depletion of network resources or computer resources, can be the results of Distributed Denial of Service (DDoS) attacks. There are various kinds of attacks which were performed for this investigation. They are Ping attack, Smurf attack, ARP (Address Resolution Protocol) attack, TCP (Transmission Control Protocol) SYN attack. The network situation has been changed for last ten years and we should know that some properties of present protocols may be abused. There are some security mechanisms to follow for security concerns [22].We provide you the basic study on these attacks to understand better and then provide you the results how they can influence the network and cause problems. The action conducted on a computer which has configuration:

- Processor: Intel ® Core ™ 2 CPU 4300 @ 1.80 GHz
- RAM : 2 GB
- Network Card Adapter : Broadcom NetXtreme 57xx Gigabit Controller

3.1 Ping Attack

It is used in the command line to know reachability of a remote computer. Bandwidth and computing resources are exhausted because of Ping based Distributed Denial of Service attack. They are famous to be harmful for web based services. This attack has minimal impact on computer's memory. However, it affects processor exhaustion either and this is major drawback. Ping flooding is basic form of DDoS attack, because it can be implemented by any one very easily. Each time the computer gets ping request, it has to reckon and send a reply with equal information. This is how it exhausts the computer resources and make it unavailable for valid users. ICMP echo request message is used by Ping request and ICMP echo reply message is used by Ping reply. The address of the source in an echo message will be the destination of the echo reply message. Type field 8 for Echo request and Type field 0 for echo reply [23].

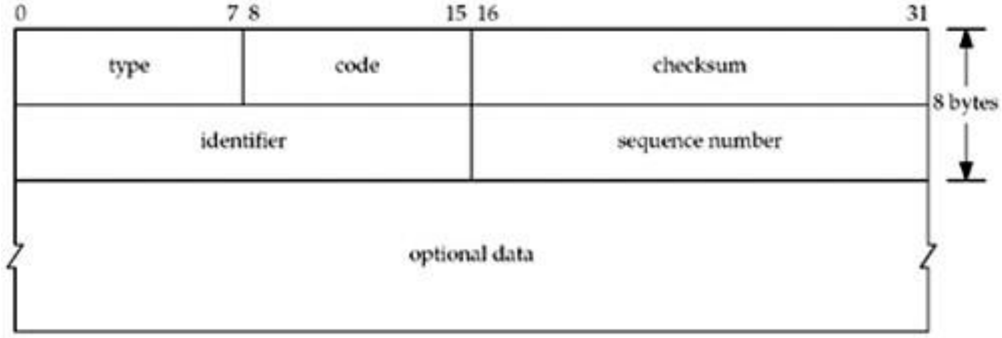


Fig 3.1 . Ping Request Packet [24]

3.2 Smurf Attack

Distributed Denial of Service (DDoS) attack continues to be a important threat to cyber infrastructure. A Distributed Denial of Service (DDoS) attack involves multiple DoS segments configured to push attack traffic to a single victim computer to make its resources unavailable to valid users. DDoS attacks are of different types, one type of DDoS attacks is called amplification attack in which the attack traffic is amplified in magnitude by definite intermediary systems before it effects the victim computer. Smurf is an example of amplification DDoS attack [25]. It is a Distributed Denial of Service attack, where attacker uses unsecured network to send large number of ICMP messages with victims computer spoofed IP address. Using weakness of TCP protocol with spoofed IP address and ICMP messages this attack is very crucial and it leads to network congestion. Valid user can't access the network. In this kind of attack, victim computer freezes when it receives huge attack. It normally leads to processor exhaustion and impacts memory. IP address of a target computer is used as the source IP address in the ICMP echo request. Then the reply messages are sent to the destination. This technique pushes every computer to respond to the bogus ping packets and reply to the targeted computer, which floods it. This technique is called a Smurf attack because the DoS tool that is used to perform the attack is called Smurf. One way to diminish the risk of this attack is to disable IP-directed broadcast, which is often not used or needed. Some operating systems are configured to prevent the computer from responding to ICMP packets. This attack happens at network layer. This attack is most devastating one in Denial of Service attacks. When we consider the results in this research, Smurf attack greatly impacted the performance of the victim computer [26]. When the attack is introduced, it consumes the processor completely.

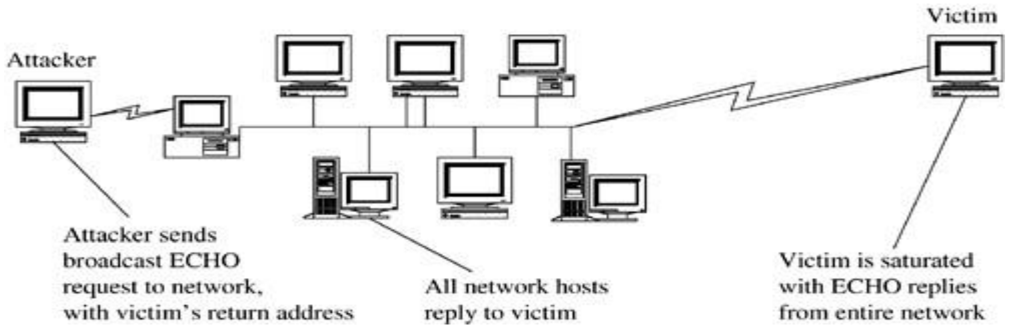
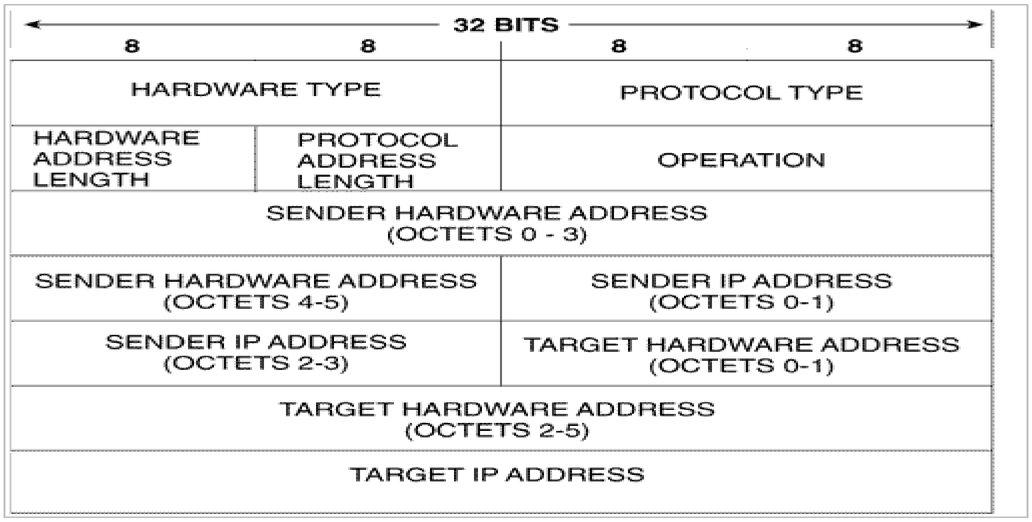


Fig 3.2 : Smurf Attack [27]

In this attack, ICMP request and ICMP echo reply messages are used. If the network has N number of computers, then for each ICMP echo request that is broadcasted will introduce equal number of ICMP echo reply messages to the victim computer because of spoofed IP address. If we consider N number of computers in the domain and M are the echo requests that are broadcasted, then N X M echo reply messages are sent to the victim computer. In case the attacker use more than one domain to introduce the traffic, then it will get amplified load and gets lot of traffic to victim computer and it effects the processor and memory of the computer. Firewalls, routers, Intrusion Prevention Systems (IPS) and some security software can be used to avoid this kind of Distributed Denial of Service (DDoS) attack. Without a proper configured router or firewall, the computer can affect from the attack. Firewalls must be configured to examine not only incoming traffic but also external traffic.

3.3 ARP Attack

ARP (Address Resolution Protocol) is used to find MAC address of a computer using its IP address. This will happen by broadcasting an ARP request packet with IP address details in it over an local area network. All the hosts that are connected in local area network gets the ARP Request and checks with their own IP address. The computer which has the same IP address sends ARP reply packet which includes its MAC address to the sender. Now, this ARP reply is not a broadcast message, because it knows the destination computer to send. The other computers which doesn't match with the IP address in the ARP request message that is broadcasted, simply drops the packet.



32 BITS			
8	8	8	8
HARDWARE TYPE		PROTOCOL TYPE	
HARDWARE ADDRESS LENGTH	PROTOCOL ADDRESS LENGTH	OPERATION	
SENDER HARDWARE ADDRESS (OCTETS 0 - 3)			
SENDER HARDWARE ADDRESS (OCTETS 4-5)		SENDER IP ADDRESS (OCTETS 0-1)	
SENDER IP ADDRESS (OCTETS 2-3)		TARGET HARDWARE ADDRESS (OCTETS 0-1)	
TARGET HARDWARE ADDRESS (OCTETS 2-5)			
TARGET IP ADDRESS			

Fig 3.3 : ARP Request and Reply format [28]

Operation field is 1 for ARP request, it is 2 for ARP reply. Hardware address type is 1 for Ethernet and 0x0800 for IP for Protocol address type.

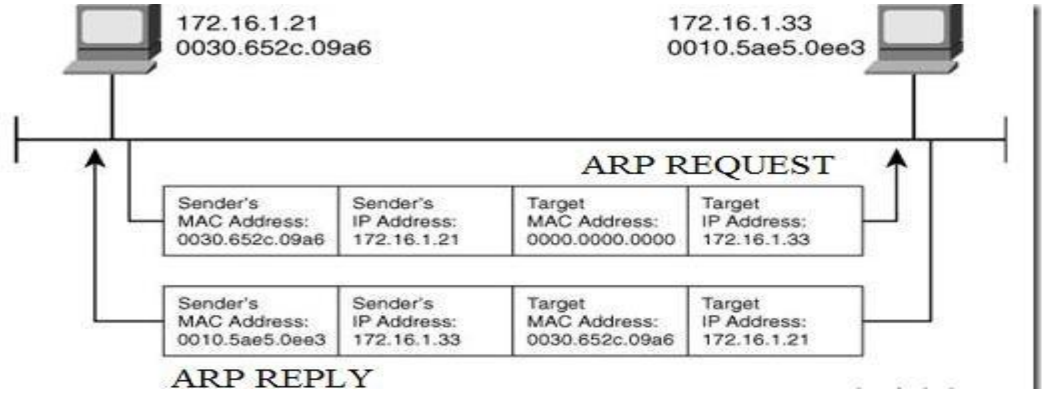

172.16.1.21
0030.652c.09a6
172.16.1.33
0010.5ae5.0ee3
ARP REQUEST
Sender's MAC Address: 0030.652c.09a6
Sender's IP Address: 172.16.1.21
Target MAC Address: 0000.0000.0000
Target IP Address: 172.16.1.33
Sender's MAC Address: 0010.5ae5.0ee3
Sender's IP Address: 172.16.1.33
Target MAC Address: 0030.652c.09a6
Target IP Address: 172.16.1.21
ARP REPLY

Fig 3.4 : ARP Request and Reply [29]

There are different kinds of ARP attack. 1) Brute force ARP attack , also known as Denial of Service attack. Continuous ARP requests are sent to the victim computer intentionally to make network and computing resources unavailable. It depends on the traffic that the victim computer can become useless. 2) ARP Poisoning, Wrong MAC address is written on ARP table, so it leads to data going over incorrect place. 3) ARP snooping, it's also called "Man-in-the-middle" attack. He can observe and have the capability to modify the data in between. When this ARP attack performed on victim computer it also causes processor exhaustion to other computers which are on local area network [30].

3.4 TCP (Transmission Control Protocol) SYN Attack

The transmission Control Protocol is a transport layer protocol. It uses a three way handshake to transfer information. The attackers found some drawbacks in this approach and they try to send duplicate TCP connection trails. As this unwanted traffic is going to victim computer, processor and memory exhausts very easily, results in poor performance.

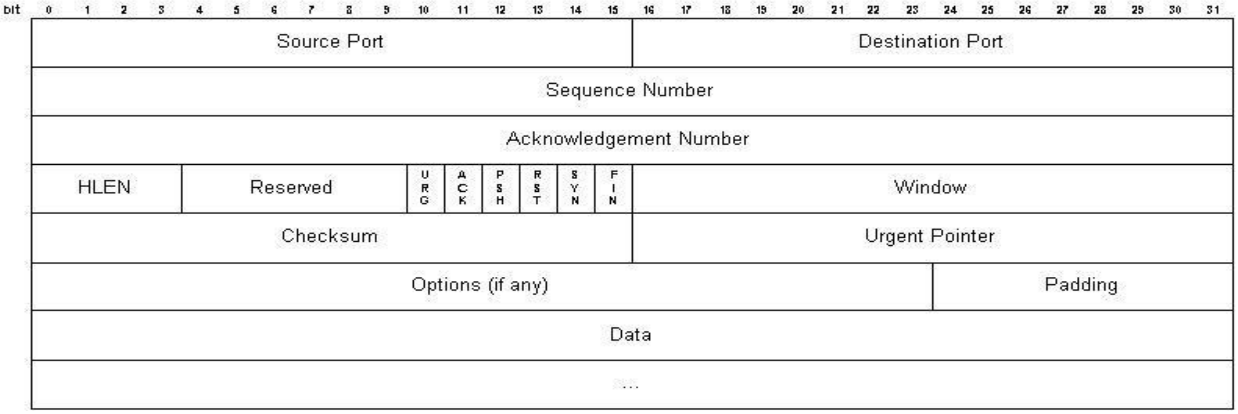


Fig 3.5 : TCP header format [31]

Let's take a look on Internet protocol and TCP connections in brief. Internet protocol is the common Layer-3 protocol. Based on some routing algorithms, IP packets are directed to fixed destination in Internet Infrastructure. As IP is a connection less protocol packets can have different status like delayed, duplicated and lost [32]. Transmission Control Protocol is responsible for those services. It is a reliable communication. It is a layer-4 protocol. We focus on the study that is required for understanding TCP SYN attack. TCP protocol is vast notion so that we consider related study.

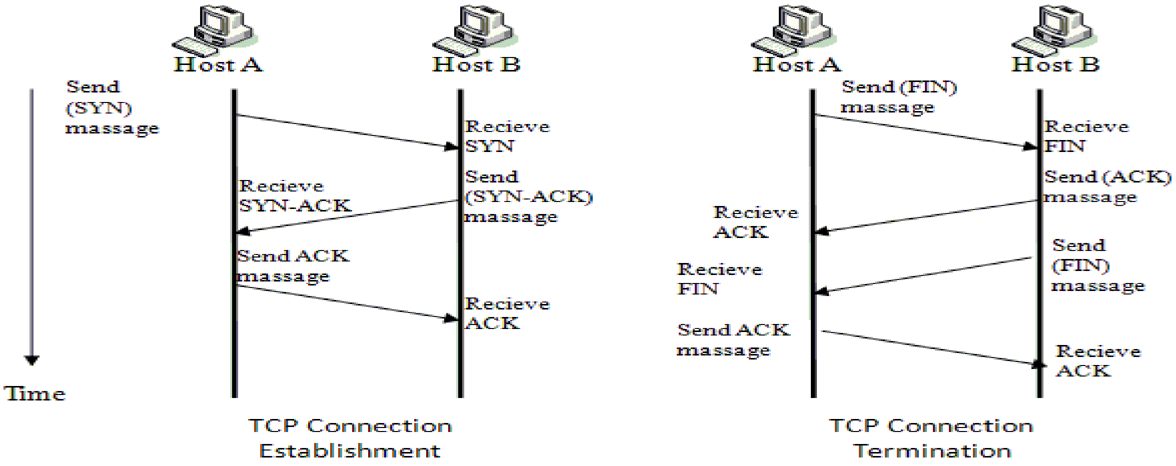


Fig 3.6 : TCP Establishment and Termination [33]

TCP Connection Establishment :

In three-way handshake approach, for data to get transfer, there is process to follow. Host A sends a TCP segment by enabling flag SYN=1. Host B sends reply a SYN/ACK , SYN is set to 1 and ACK field is given a value which is earlier sequence number plus one. When Host A receives that datagram, it sends another acknowledgement to Host B. This is the procedure to establish a TCP connection .It can be seen in the above figure. If Host A wants to terminate the connection FIN bit is set to 1, then in reply Host B sends an acknowledgement ACK which is set to 1 . These steps are followed in the same way, if Host B wants to close the connection. It sends FIN bit which is set to 1 to Host A and then it replies with ACK=1.

Client sends a TCP segment with SYN bit set to 1. The server replies with SYN/ACK with SYN is set to 1 and ACK set to previous sequence number plus one. In this situation, connection remains half open because server is waiting for reply ACK from client. Client will send ACK before the time expires for half open connection. Here, the attacker sends lots of TCP segments to victim computer so it creates more half open connections. This is TCP SYN flood attack. More number of half open connections consume important network resources like processor, memory, bandwidth. More than 90% of attacks utilize TCP and TCP SYN flooding is very common [34].

CHAPTER IV

EFFECTS OF NETWORK ATTACKS ON DATA COLLECTION OF EKG SIGNALS

In the last year, DDoS attacks emerged in strategy and tactics. Media reports say that there is huge increase in DDoS attacks to divert IT staff while keeping malware in bank accounts and customer data. More than 47 % view DDoS attacks as greater than in 2012 and they are equally harmful. In 2013 DDoS attacks have continuously attacked websites and shut down operations which results in cost millions of dollars. 87 % of companies were affected multiple times due to DDoS attacks. In 2014, the Neustar security operations center reduced these huge attacks. 55% of DDoS attacks happened for theft: intellectual property, customer data and funds. The IT sector of each business bears mostly with these DDoS attacks, when compared to other areas like marketing, security, risk management [6] .

4.1 Procedure

Attach the EKG Sensor to the interface. Start the data capturing software application. It will identify the EKG Sensor and it gets ready to collect data. Specifications of the sensor are Offset: ~1.00 V (±0.3 V), Gain: 1 mV body potential / 1V sensor output. Capture the EKG signal of the subject who is at rest. The subject whose EKG signal is being captured should stay calm and relaxed. In detail, put an electrode patch on the right upper arm. Connect the green (or negative) alligator clip to the right upper arm electrode patch.

Put an electrode patch on the left upper arm. Connect the red (or positive) alligator clip to the left upper arm electrode patch. Put an electrode patch on the inside surface of the area behind the right ankle bone. Connect the black (or “reference”) alligator clip to the ankle electrode patch. This is the reference point for the isoelectric line [35]. The configuration of the computer used for these experiments :

- Processor: Intel ® Core ™ 2 CPU 4300 @ 1.80 GHz
- RAM : 2 GB
- Network Card Adapter : Broadcom NetXtreme 57xx Gigabit Controller

Logger lite (1.3.2) is the software application used to collect EKG data [36].

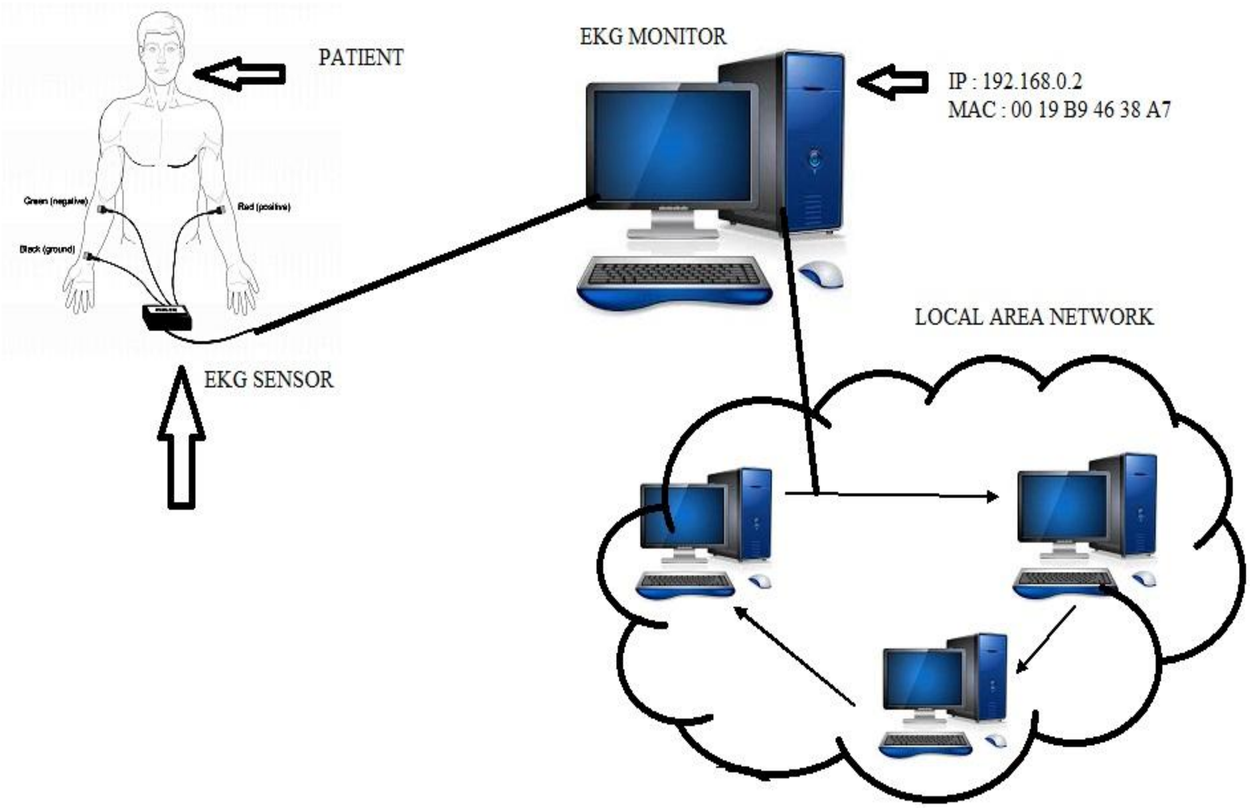


Fig 4.0: Experimental Setup

4.2 Common Abnormalities found in the Results

Abnormalities in the EKG information [37] can be seen under different attacks. In the table 4.0, the common abnormalities that we observed in the results are listed.

Table 4.0 : Common Abnormalities observed in the attacked EKG signal [38]

ABNORMALITY	DESCRIPTION	EKG SIGN
Normal Sinus Rhythm	Sinus rhythm is obvious if its frequency stays between 60-100/ min.	Regular P waves, and they are followed by a QRS complex
Sinus Tachycardia	Sinus rhythm, if its frequency stays more than 100/min	Regular P waves, and they are followed by a QRS complex
Sinus bradycardia	Sinus rhythm, if its frequency stays less than 60/min	Regular P waves, and they are followed by a QRS complex
Atrial Fibrillation	The ventricles respond to those pulses coming through AV node.	Irregularly irregular, irregular QRS complex, can't measure QT interval, T wave is vague.
Atrial Flutter	This is also called supraventricular Tachycardia. Can't say whether T wave and P wave are present. Rhythm is too fast. P waves lose their distinction due to increased atrial rate.	QRS complex is normal, however, may be widened if the flutter waves are hidden in the complex. T wave is not visible in this abnormality. QT interval cannot be measured as we don't see T wave.
Hyperkalaemia	The electrolyte Potassium (k^+) level in the blood increases and peaked T waves and shortened QT interval appear. To avoid risk, temporary treatment will be given, however removal of unwanted potassium level can be done by stimulating urine or dialysis.	Peaked or tall T waves, shortened or absent ST segment.
Hyperthermia	If the body temperature is between 32-35 degrees, then it is mild Hypothermia. If the	J waves deviate in moderate hypothermia (30 degrees C)

	body temperature is between 29-32 degrees, then it is moderate Hypothermia. If the body temperature is less than 29 degrees, then it is severe Hypothermia.	
Hypothyroidism	Effects on the myocardium of reduced levels of thyroxine.	low voltage QRS, bradycardia and widespread T waves.
Hyperthyroidism	Atrial tissue is very sensitive to the effects of thyroid hormone, hence the preponderance of atrial tachydysrhythmias.	low voltage QRS, tachycardia and atrial fibrillation
Pericarditis	Infection of the pericardium generates chest pain and tachycardia. The pericardium is a thin, two-layered, fluid-filled sac that covers the outer surface of the heart. Involvement of underlying epicardium occurs which is indicated by widespread ST segment	If ST elevation does occur, then the ST waves will appear 'saddle shaped' thus helping you to differentiate it from MI. Also, the elevation in MI tends to be confined to a certain area, but in pericarditis, it is widespread
Multifocal Atrial	A rapid, irregular atrial rhythm arising from multiple ectopic foci within the atria.	Heart rate > 100 bpm, minimum three distinct P waves
Anterior Myocardial Infarction	Anterior myocardial infarction carries the worst prognosis of all infarct locations, mostly due to larger infarct size.	ST elevation
Premature Ventricular Contraction	The immature heartbeat originating from an ectopic focus in the ventricles.	Broad QRS complex, different ST segment and changes in T wave.

4.3 Results In Windows XP With Service Pack3

In this section, we are going to see the effects of ARP (Address Resolution Protocol) attack at different traffic loads on the data collection of EKG signals in the operating system Windows XP with Service Pack3.

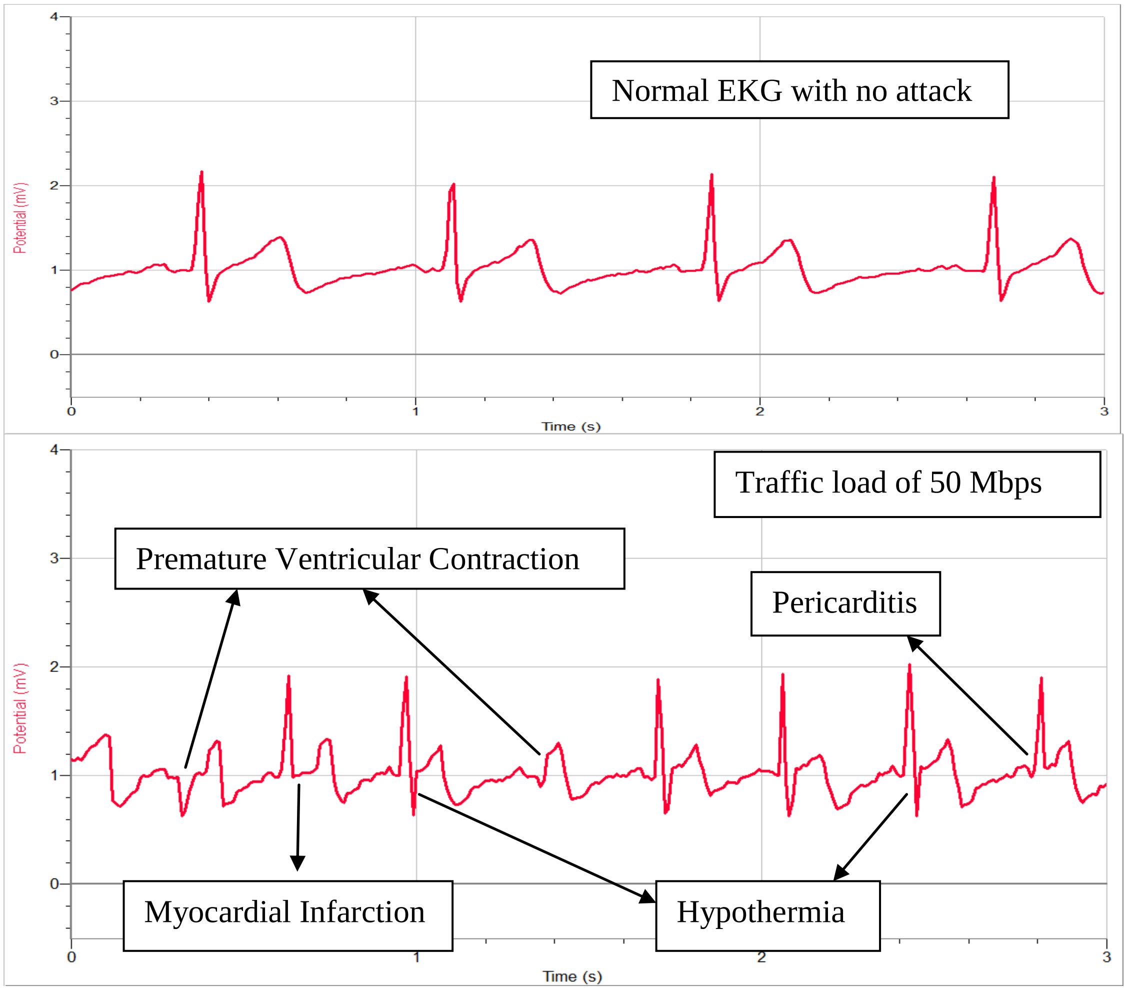


Fig 4.1 : Normal EKG vs Abnormal EKG at ARP attack of 50 Mbps traffic

In the operating system Windows XP with SP3 under ARP attack of 50 Mbps traffic, has adverse effects on data collection of the EKG signal. In the Figure 4.1, the normal EKG signal has changed completely and showed some abnormalities. Premature Ventricular Contraction, this abnormality is observed as the origin of heart beat is changed to ventricles, and this is indicated in the above figure. In addition, we observe moderate Hypothermia abnormality in the above attacked EKG signal. Precarditis is the other abnormality we can notice as PR segment and ST segment starts alomost closely in the same level. At this traffic, the system froze for about four minutes and then showed the EKG signal on the display. Thus, it violates the Availability element in the CIA security triad.

From the Table 4.1, we can say that R-R intervals are increased in the attacked EKG signal which indicates Sinus Tachycrdia. The QT interval modifies on the rate of heartbeat. It adapts slowly to decelerations than to accelerations of the heart rate.With less than 0.32 sec QT interval, it refers to the abnormality Shorten QT syndrome types 1-3 [39]. Before introducing the attack, the processor utilization was 2% and RAM by 6.5%, and then it went to 55% and 7.45% with the attack traffic. There is not much change in RAM utilization, however processor usage has increased to 55%. This consumption of processor is not the worst case, however the interesting thing is the attacked EKG signal turned out with five abnormalities. From this, it violates the integrity element in the CIA security triad.

Table 4.1 : Windows XP with SP3 at ARP attack of 50 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.73,0.75,0.83	0.37,0.37,0.35,0.39	2%	6.5%
50 Mbps	0.34,0.44,0.39,0.36,0.37,0.38	0.21,0.19,0.19,0.21,0.20	55%	7.45%

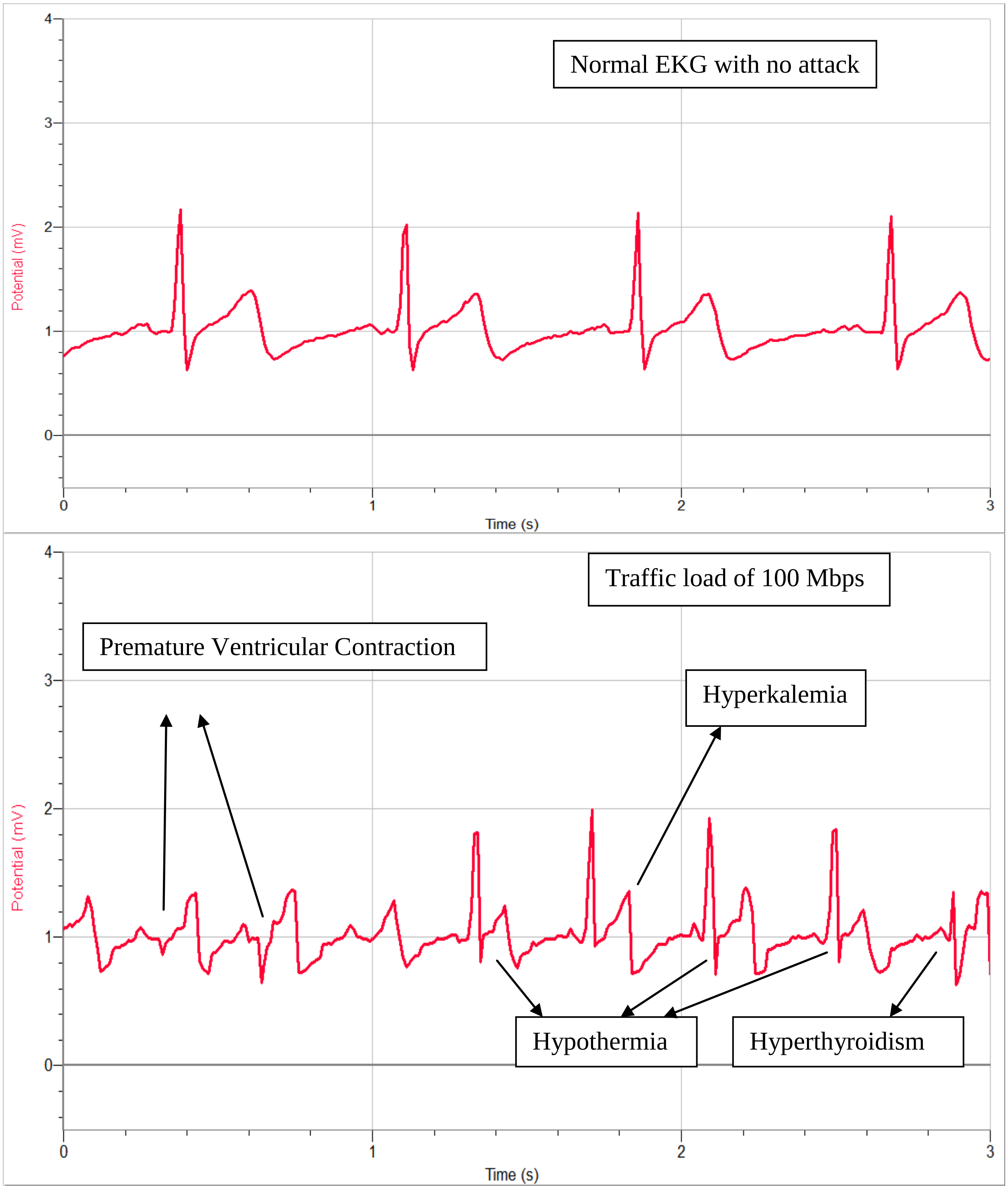


Fig 4.2 : Normal EKG vs Abnormal EKG at ARP attack of 100 Mbps traffic

At this 100 Mbps traffic with ARP attack, we can notice these abnormalities Premature Ventricular Contraction, Hyperkalemia, Hyperthyroidism, Hypothermia and Sinus Tachycardia. The computer under this attack froze for about five minutes and then displayed the EKG signal.From this, it violated the Availability element in the CIA security triad.The starting point of heart beat is from ventricles, we noticed Premature ventricular contraction abnormality. As we observe more R-R intervals in the attacked EKG signal than in the normal EKG signal, Sinus tachycardia abnormality is considered. Other noticed abnormalities are Hypothermia, Hyperkalemia and Hyperthyroidism. J point deviation in the effected EKG signal, which leads to Hypothermia. Low voltage QRS complexes refers to the abnormality Hyperthyroidism. Peaked T waves represents the abnormality Hyperkalemia. In the Figure 4.2, we can see indications in the attacked EKG signal which resembles the above mentioned abnormalities.

In the Table 4.2, R-R intervals are increased in the attacked EKG signal because of the increased heartbeat rate. QT intervals has modified much in the effected EKG signal which was under attack, when compared to the normal EKG signal. This QT interval changes much with the increase in the heartbeat rate. This QT interval information also indicates the abnormality shorten QT syndrome genotypes 1-3. RAM utilization has not effected much, however processor usage has increased to 54%. This consumption of processor is not the worst case, however the interesting thing is denial of servce attacks effected the EKG signal with five abnormalities. Hence, it violates the integrity element in the CIA security triad which is not good.

Table 4.2 : Windows XP with SP3 at ARP attack of 100 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.73,0.75,0.83	0.37,0.37,0.35,0.39	2%	6.5%
100 Mbps	0.37,0.38,0.40,0.38	0.19,0.18,0.20,0.18	54%	7.7%

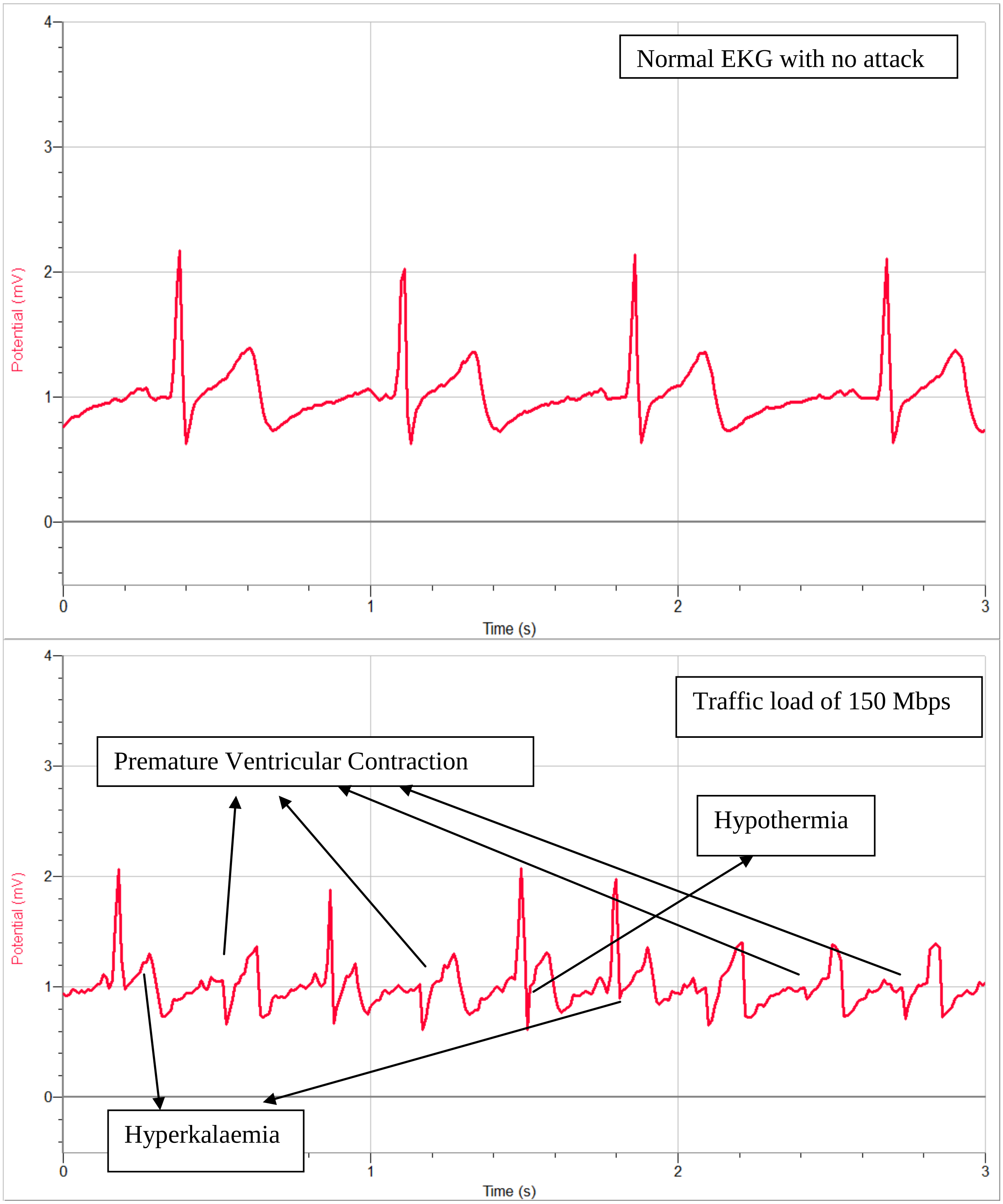


Fig 4.3 : Normal EKG vs Abnormal EKG at ARP attack of 150 Mbps traffic

In the Figure 4.3, at ARP attack of 150 Mbps traffic load , we can notice Premature Ventricular Contraction, Hypothermia,Hyperkalemia and Sinus Tachycardia abnormalities. With this traffic load, the computer froze for about five minutes to display the EKG signal. Many RR intervals indicates the abnormality Sinus Tachycardia. J point deviation resembles the abnormality moderate Hypothermia.The origin of heart beat signal is from the ventricles which disrupts the normal heart beat and this abnormality is called Premature Ventricular Contraction.

The Table 4.3, gives the information on RR intervals, QT intervals, processor and RAM usage values of both normal and attacked EKG signals at ARP attack of 150 Mbps traffic.Because of increased heartbeat rate, more number of RR intervals are present and possible vaues are listed in the table and QT intervals has reduced. The low values in QT interval indicates Shorten QT syndrome abnotmality. It is recently discovered arrhythmogenic disease This 54% processor utilization is not harmful, even thogugh the attacked EKG signal under ARP attack has turned out abnormal EKG signal. Because, the network attack modified the EKG signal with five abnormalities. From this, it violates the integrity element in the CIA security triad which is dangerous in the health care system.

Table 4.3 : Windows XP with SP3 at ARP attack of 150 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.73,0.75,0.83	0.37,0.37,0.35,0.39	2%	6.5%
150 Mbps	0.69,0.62,0.31	0.18,0.17,0.16,0.19	54%	7.7%

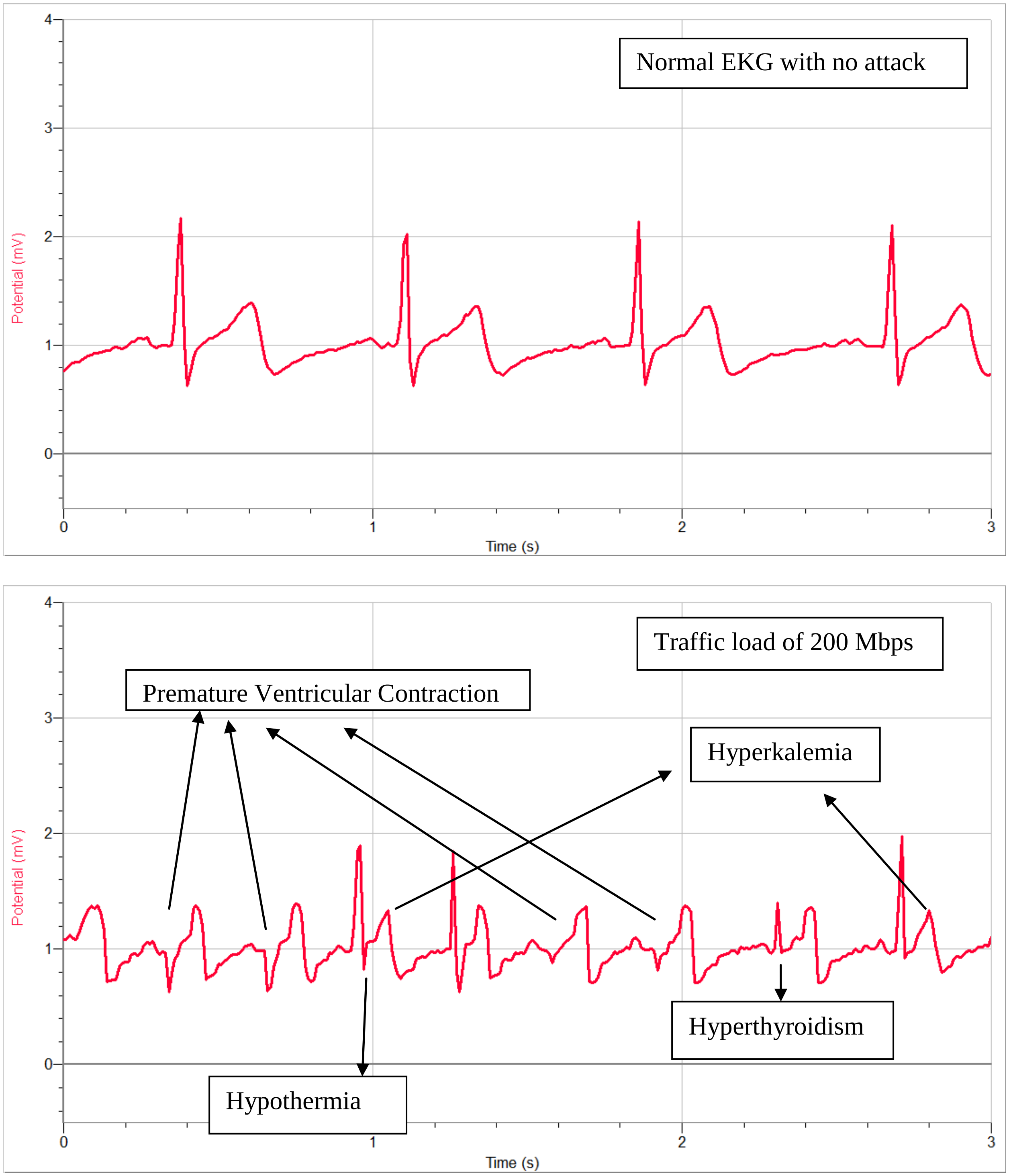


Fig 4.4 : Windows XP with SP3 at ARP attack of 200 Mbps traffic

The abnormalities like Premature Ventricular Contraction ,Hypothermia, Hyperkalemia, Hyperthyroidism and Sinus Tachycardia can be observed at 200 Mbps traffic condition under ARP attack which is shown in the Figure 4.4.With this above traffic load, the computer froze for about ten minutes to display the EKG signal.This clearly shows that element Availability in the CIA security triad is violated. The computer would be completely froze and it doesn't allow any application to open, unless the running attack is stopped. At one point in the attacked EKG signal, it reflected two abnormalities Hypothermia and Hyperkalemia simultaneously. We observed J point deviation which refers to Hypothermia and peaked T wave that resembles the abnormality Hyperkalemia.

As more numbers of RR intervals are present, which indicates the abnormality Sinus Tachycardia. J point deviation indicates the abnormality moderate Hypothermia. The origin of heart beat signal is from the ventricles which disrupts the normal heart beat and this abnormality is called Premature Ventricular Contraction. Also, tall or peaked T waves are shown in the attacked EKG signal, refers to abnormality Hyperkalemia. In Sinus Tachycardia, if it includes low voltage QRS complexes , then it is another abnormality, Hyperthyroidism. In the Table 4.4, RAM utilization has not much changed in the abnormal EKG signal.The processor utilization was found to be 54% which is not much consumed, even though the attacked EKG signal under ARP attack has changed the EKG signal to an abnormal one. From this, it violates the integrity element in the CIA security triad, which is a big issue in the health care system.

Table 4.4 : Windows XP with SP3 at ARP attack of 200 Mbps traffic

Traffic (Mbps)	Processor Used	RAM Used
Normal	2%	6.5%
200 Mbps	54%	7.7%

The operating system Windows XP with SP3 is not strong enough to hold the ARP attack. This attack has showed adverse effects on the data collection of EKG signal. The normal EKG signal which is taken at rest condition changed completely with the introduction of attack traffic. QT and RR intervals effected much under ARP attack, because with this attack traffic the rate of heartbeat increased. It displayed different abnormalities in which some are considered serious heart issues. The hackers and attackers are leveraging easily noticeable network blocks to aim and exploit Windows end-user servers and computer systems. Microsoft’s Windows XP with SP2 was found to be a good approach to mitigate the adverse effect of the TCP SYN attacks on Windows based computer systems [40].In the case of operating system Windows XP with SP3, the TCP SYN attack doesn't show effects on the attacked EKG signal. Ping attack, TCP SYN attack, ARP attack were performed on this operating system.

The results of the Ping attack and the TCP SYN attack didn't trouble the data collection of EKG signal, even with different traffic conditions. Hence, the attacked EKG signal is similar to the normal EKG signal with no attack. Ping attack consumed around 25 % of the processor utilization and 7.05% of the total RAM. If we observe the effects on data collection of EKG signal, ARP attack has shown the abnormal EKG signal. TCP SYN flodding normally causes more harm, where it completely disables the computer or network resources .

4.4 Results in Windows 7 Enterprise

In this section, we are going to see the effects of ARP (Address Resolution Protocol) attack at different traffic loads on the data collection of EKG signals in the operating system Windows 7 Enterprise .

ARP Attack :

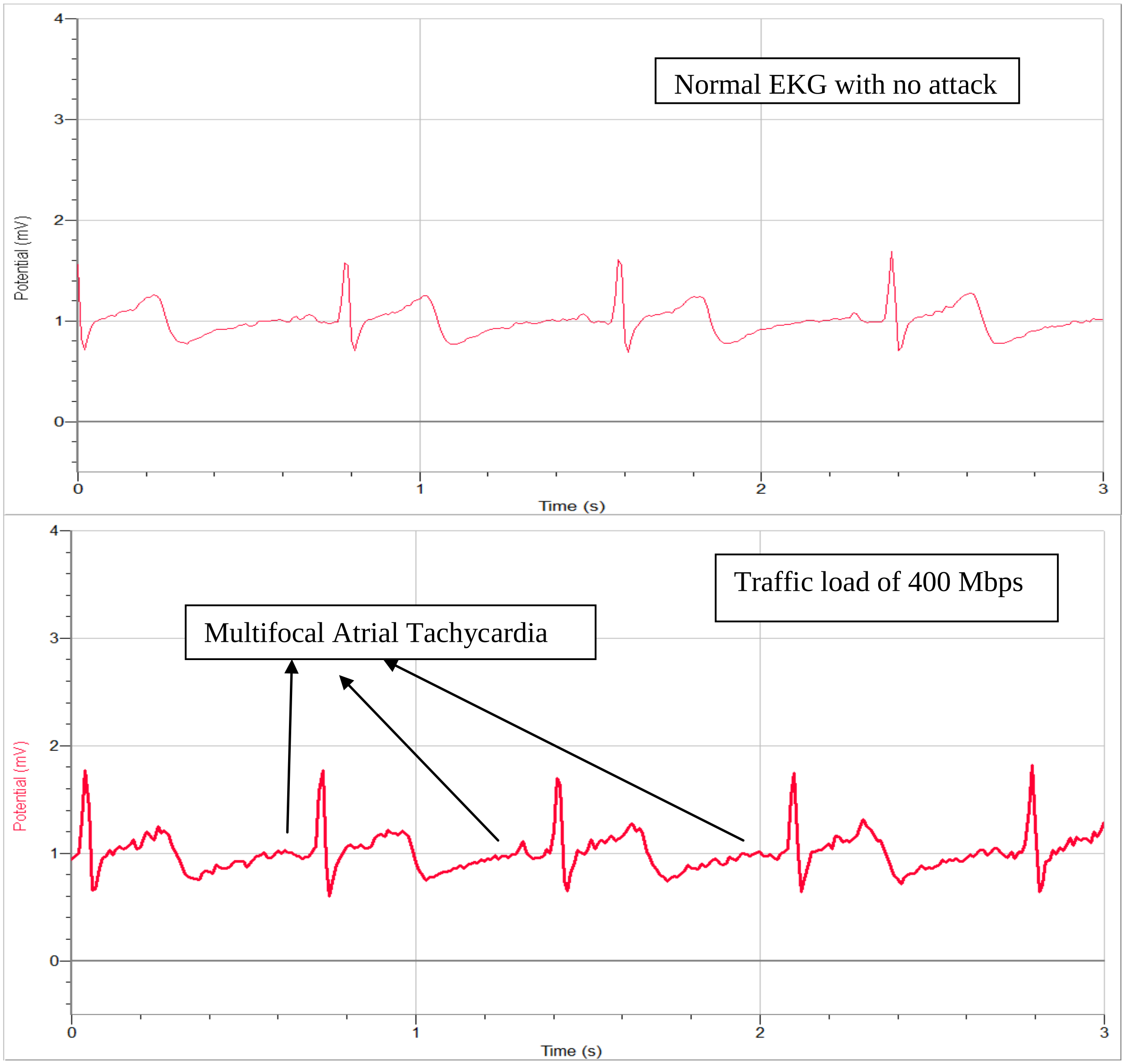


Fig 4.5 : Normal EKG vs Abnormal EKG at ARP attack of 400 Mbps traffic

In the operating system Windows 7 Enterprise, at ARP attack of 400 Mbps traffic load, data collection of the normal EKG signal has effected and we see the abnormality Mutifocal Atrial Tachycardia. As different forms of P waves are present, this resembles Multifocal Atrial Tachycardia. This violates the Integrity element in security concern. When compared to operating system Windows XP with SP3,the ARP attack has less influence on data collection of the EKG signal.Only under 400 Mbps and 1000 Mbps traffic conditions, EKG signal has modified with some abnormalities.Moreover, the computer froze about five minutes in all the traffic conditions, which disobeys the Availability component in the CIA security triad. However, they displayed the same EKG information which is similar to EKG signal with no attack. But in these exceptional cases like 400 Mbps and 1000 Mbps, they displayed abnormality Multifocal Atrial Tachycardia.

In Figure 4.6, with the ARP attack of 1000 Mbps traffic condition, the attacked EKG signal was displayed with Multifocal Atrial Tachycardia abnormality. Three distinct P waves were found in the attacked EKG signal which resembles the above abnormality. The subject whose EKG was capturing needs to wait with electrodes placed on the body, until it turns out the display of EKG signal. The computer froze for about five minutes to display the attacked EKG signal. Again in this case, it violates the Availability and Integrity components in the CIA security triad. Before introducing the attack the processor and RAM utilization was found to be 2% and 18.25%. After the introduction of attack traffic they increased to 45% and 18.25%. Even 45% of processor consumption is not a devastating number to bring out some abnormalities in the attacked EKG signal, however network attacks silently altered the normal EKG signal with abnormality.

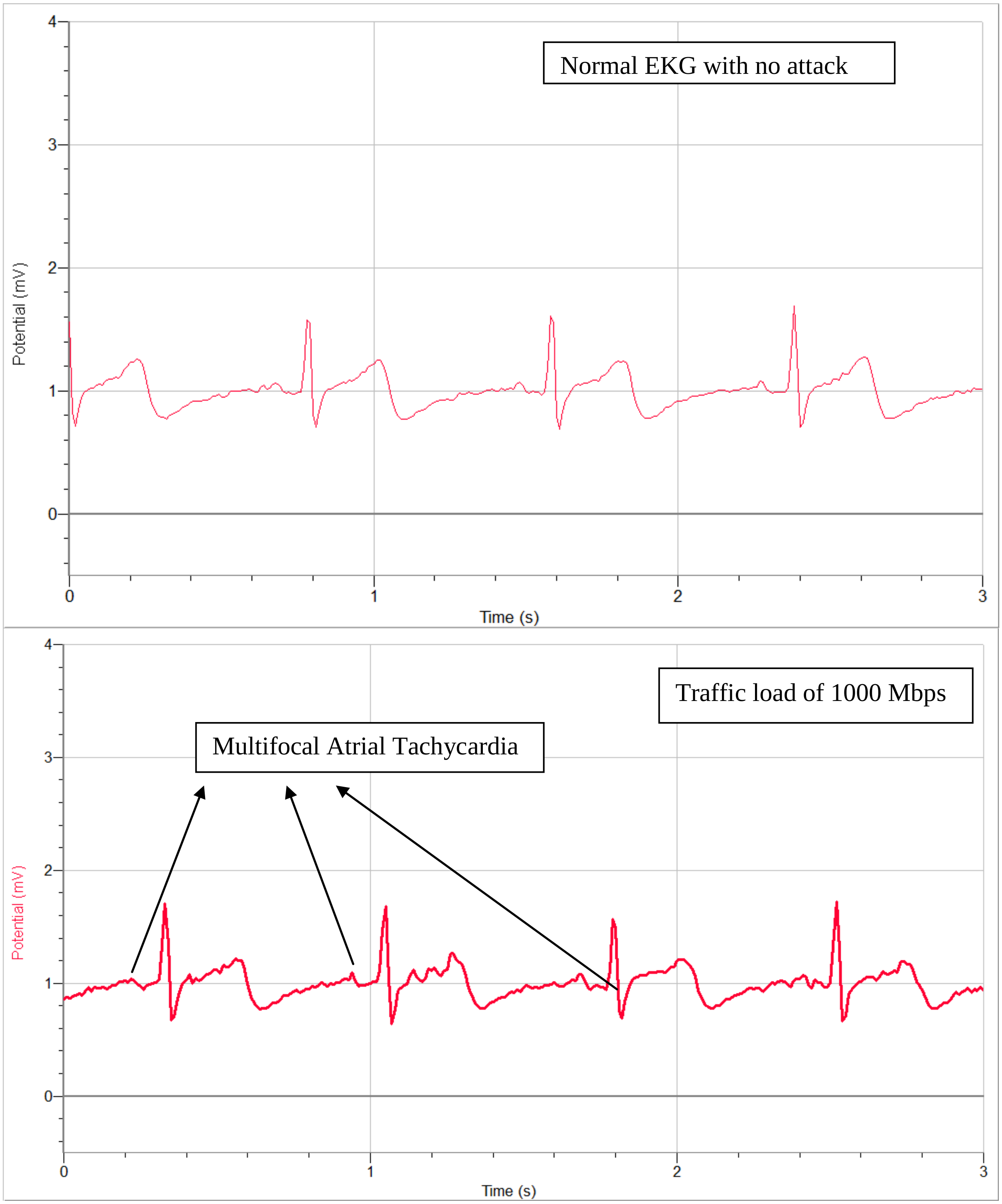


Fig 4.6 : Normal EKG vs Abnormal EKG at ARP attack of 1000 Mbps traffic

In this operating system Windows 7 Enterprise, it is good enough to hold the ARP and TCP SYN attacks, however there are some exceptional cases such as 400 Mbps and 1000 Mbps with ARP attack. In those cases, the attacked EKG signal turned out to be abnormal one. TCP SYN was the other attack performed under different attack traffic conditions. The processor utilization went up to 74% and RAM used is 7.7%, hence it is processor intensive. Microsoft's Windows 7, had come a long way in giving its users with a safer, more reliable, secured and more responsive operating system. Microsoft’s Windows 7 operating system is considered to be more capable of limiting adverse effects of DDoS flood attacks [41]. Sinus tachycardia and Sinus bradycardia are common abnormalities that we can noticed in most of the attacked EKG signals; however these abnormalities were not displayed when EKG signal collected on the computer under the influence of denial of service attacks in this operating system. Mutifocal Atrial Tachycardia is the one abnormality observed at ARP attack.

4.5. Results in Windows 7 Ultimate With SP1

In this section, we are going to see the effects of Smurf attack and Ping attack at different traffic loads on the data collection of EKG signals in the operating system Windows 7 Ultimate with Service Pack1.

In this operating system Windows 7 Ultimate with SP1, the abnormalities found on the attacked EKG signal are Atrial Fibrillation which was indicated by irregular EKG signal, and also low voltage QRS complex which resembles a Hypothyroidism.

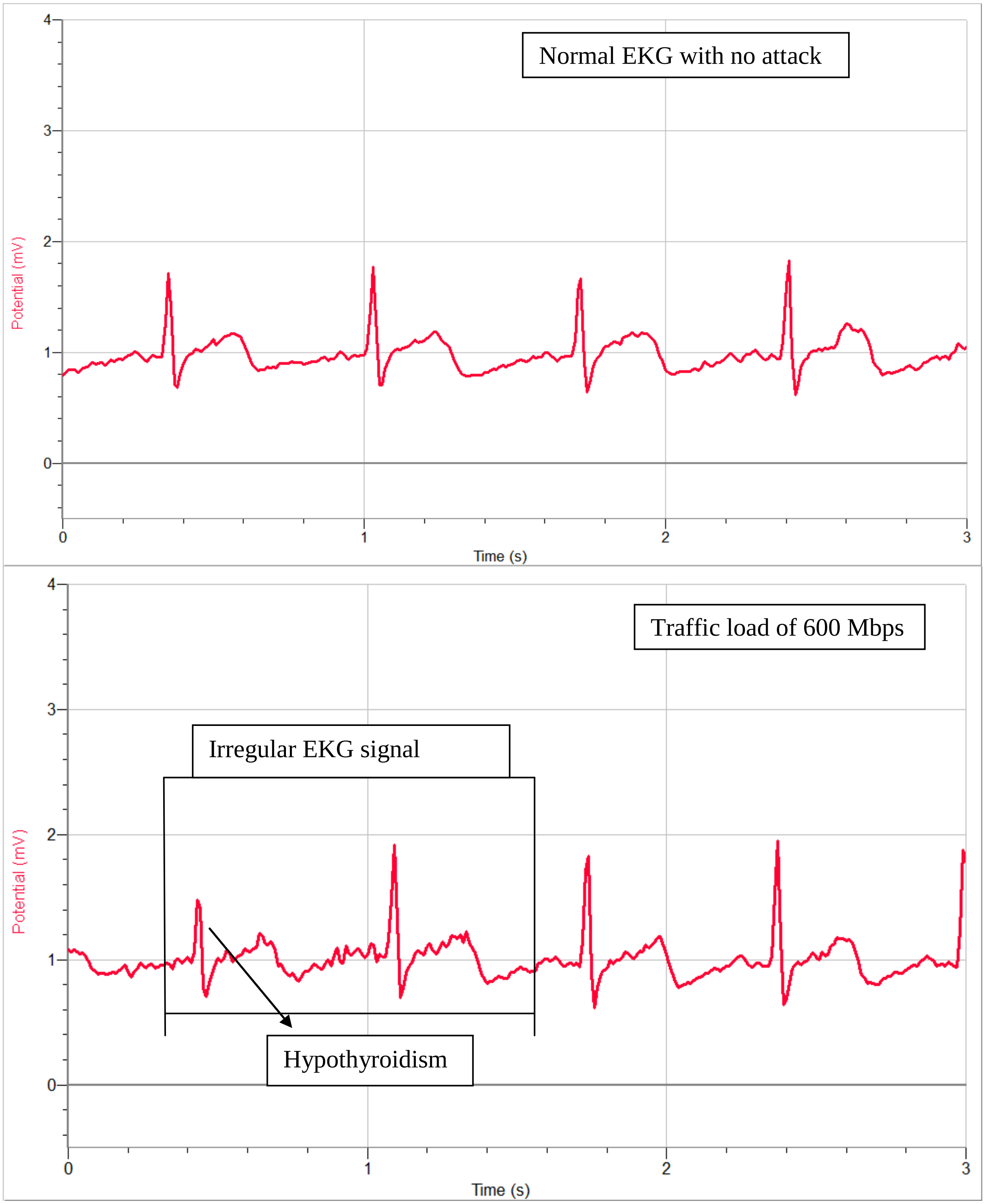


Fig 4.7: Normal EKG vs Abnormal EKG at Smurf attack of 600 Mbps traffic

Smurf attack has an impact on data collection of EKG signals at 600 Mbps, 800 Mbps and 900 Mbps traffic loads. In this case of attack traffic 600 Mbps, the computer froze for about eight to ten minutes and then it displayed the EKG signal with abnormalities. By this it violates both integrity and availability elements in the CIA security triad. The processor utilization is 76% and RAM utilization is 25.7%. Certainly, it seems procesor intensive. With this consumption of processor, it displayed the EKG signal with one abnormality and irregular EKG signal at some point of time. If we notice the other results with ARP attack, the processor usage increased to to 54% and showed five abnormalities in one EKG signal at a particular attack traffic. However, this Smurf attack consumed 76% of processor, and the outcome effected with irregular EKG signal at some portion.

At Smurf attack of 800 Mbps traffic, noticeable abnormalities are Sinus tachycardia, Hyperthyroidism and Multifocal Atrial Tachycardia. As more number of R-R intervals are present, it indicates Sinus Tachycardia. More than three distinct P waves were recorded, which resembles the abnormality Multifocal Atrial tachycardia. By low voltage QRS complex, we can consider the abnormality Hyperthyroidism. The computer froze for about eight to ten minutes and then the EKG signal loaded with mentioned abnormalities. In this case also, they failed to hold the elements of CIA secuirty traid. Integrity failed because the attacked EKG signal effected and displayed the abnormalities, where the person who is monitoring the real time EKG signals may raise false alarm and do misdiagnose. Element availability in the security triad has also failed due to the computer freezing for several minutes, before it displayed the EKG signal under the attack. These kind of false alarms are raised due to the effects of denial of service attacks which are harmful for the health care system.

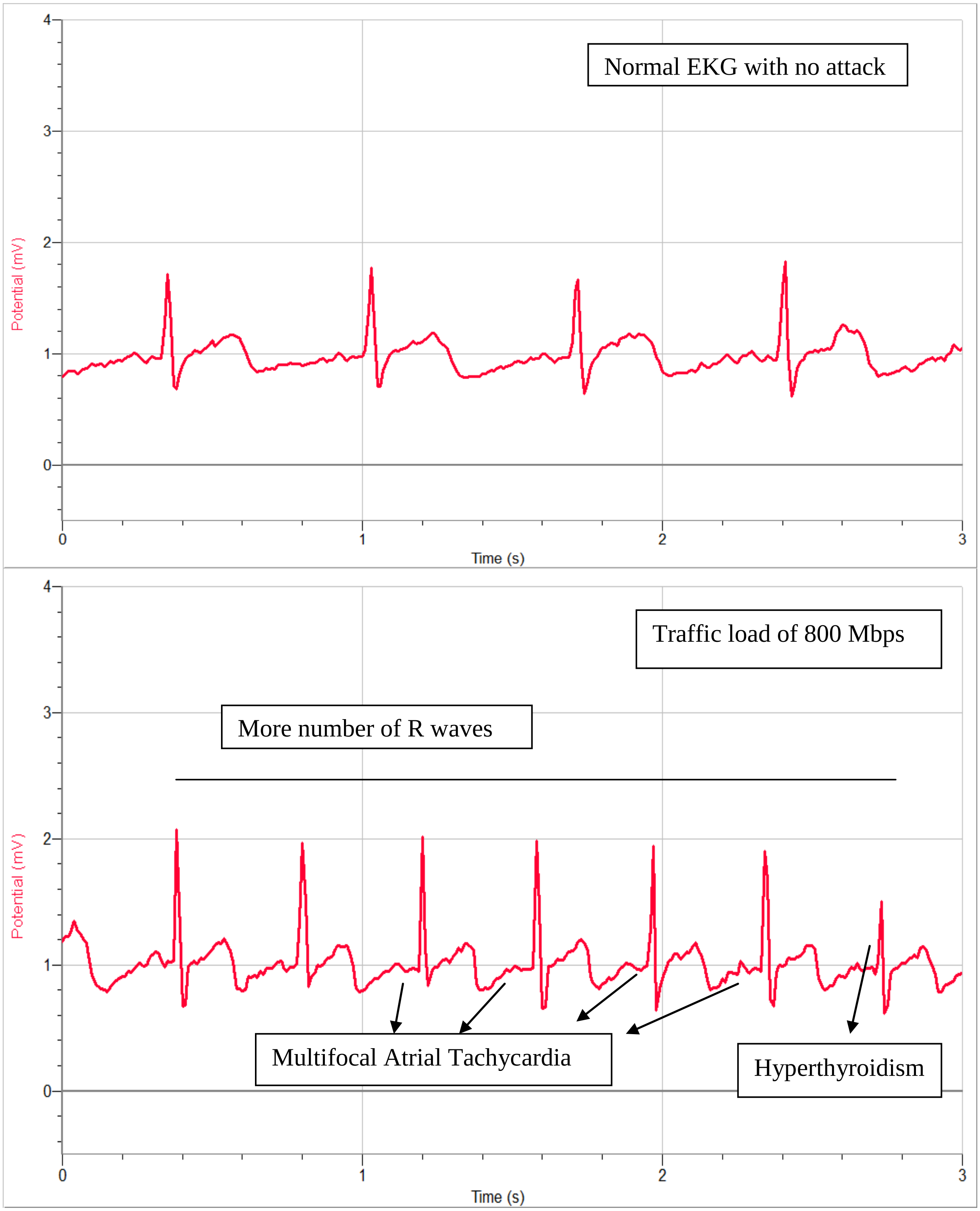


Fig 4.8 : Normal EKG vs Abnormal EKG at Smurf attack of 800 Mbps traffic

In the Table 4.5, The QT and RR interval values were effected on the attacked signal, they were different to the normal EKG signal intervals. As the heartbeat rate increased, we noticed more number of RR interval values and shorten QT interval values. These low values of QT interval refers to the abnormality Shorten QT syndrome. Interestingly, with 600 Mbps traffic the processor utilization is 76% and it remained the same for 800 Mbps attack traffic. However, the effects on the EKG signal are different. These network attacks or denial of service attacks have poor effects on the network resources of the victim computer. Abundant research is going on different DDoS mechanism to avoid these kind of devastating performances on target systems.

Table 4.5: Windows 7 Ultimate with SP1 at Smurf attack of 800 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.68,0.69,0.69	0.35,0.37,0.37,0.35	2%	23%
800 Mbps	0.42,0.40,0.38,0.39,0.38,0.38	0.24,0.25,0.23,0.25,0.24,0.25	76%	25.7%

In the Figure 4.9, with 900 Mbps traffic under Smurf attack, the noticeable abnormalities are Multifocal Atrial Tachycardia, Hyperthyroidism and Sinus Tachycardia. The low voltage QRS complexes in the increased heartbeat rate indicates a Hypothyroidism abnormality. Three distinct forms of P wave which resembles the abnormality Multifocal Atrial Tachycardia. More number of RR intervals are present, hence Sinus Tachycardia is considered.

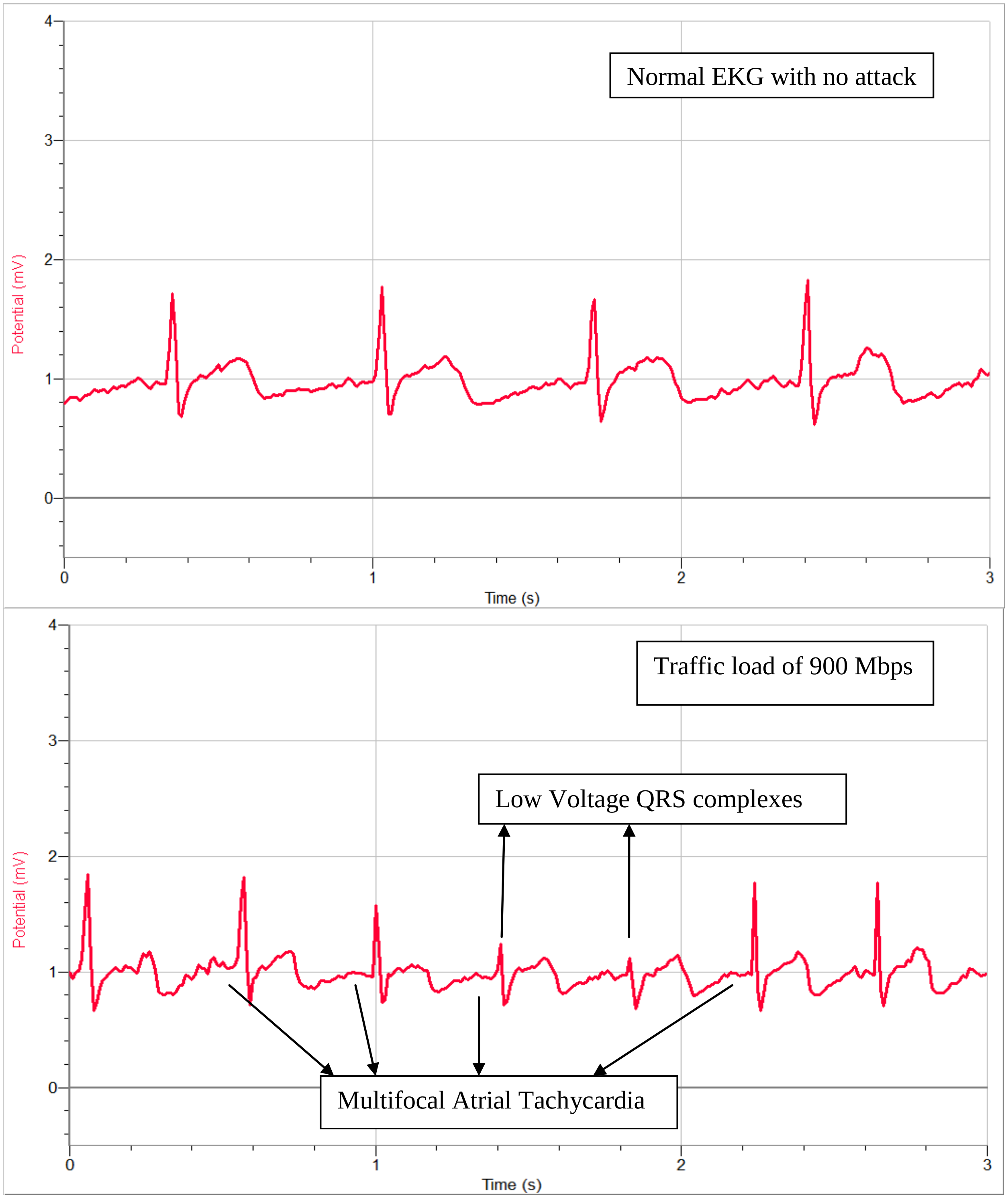


Fig 4.9 : Normal EKG vs Abnormal EKG at Smurf attack of 900 Mbps traffic

In all traffic conditions, the computer freezes for several minutes to load the EKG signal, which disobeys the availability factor in the secuirty concern. Moreover, we saw changes on the attacked EKG signals in 600 Mbps, 800 Mbps and 900 Mbps. From this, we are clear that these cases violated both the elements availability and integrity in the CIA security triad. In the Table 4.6, the QT and RR intervals were effected on the EKG signal at Smurf attack of 900 Mbps traffic load. We observed, that there is increase in rate of heartbeat which increases the RR interval and shortens the QT interval. The shorten QT interval values indicates Shorten QT syndrome genotype 1 -3. The processor and RAM utilization on the attacked signal was found to be 76% and 25.7% which says that it is processor intensive.

Table 4.6 : Windows 7 Ultimate with SP1 at Smurf attack of 900 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.68,0.69,0.69	0.35,0.37,0.37,0.35	2%	23%
900 Mbps	0.51,0.43,0.41,0.42,0.41,0.40	0.26,0.23,0.26,0.26,0.24,0.24	76%	25.7%

Ping Attack :

In this section, we are going to see the effects of Ping attack at 300 Mbps traffic load on the data collection of EKG signals in the operating system Windows 7 Ultimate with Service Pack1. As tall T wave or peaked T wave is present, Hyperkalaemia is the abnormality to be considered. This situation is very bad because it doesn't freeze normally and displayed the EKG signal. The person who is monitoring the EKG signal of the respective subject can presumes that he is receiving the precise EKG information without any error, which can lead to wrong diagnosis.

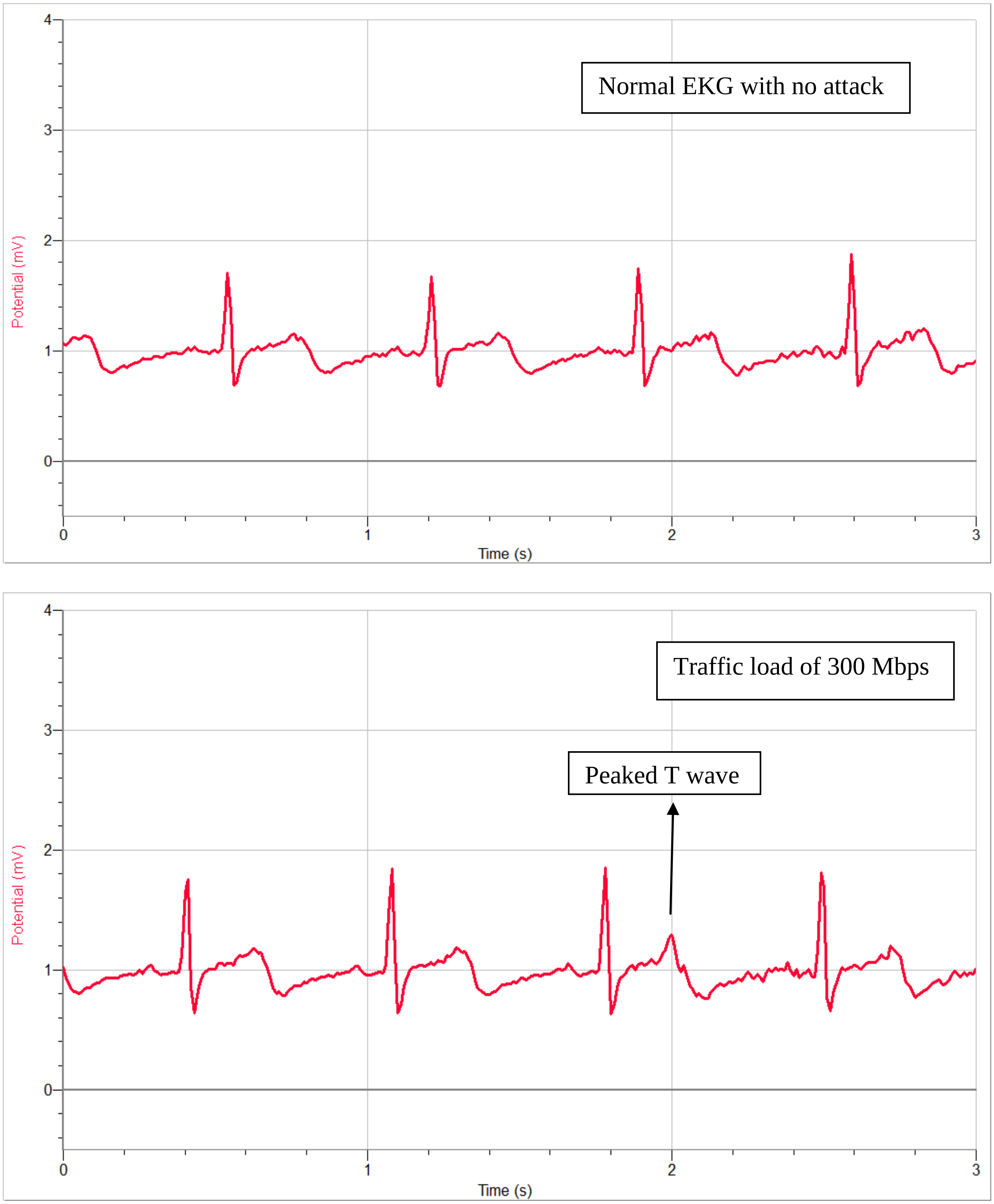


Fig 4.10 : Normal EKG vs Abnormal EKG at Ping attack of 300 Mbps traffic

4.6. Results in Windows 8 Enterprise

In this section, we are going to see the effects of ARP (Address Resolution Protocol) attack, Smurf attack, Ping attack at different traffic loads on the data collection of EKG signals in the operating system Windows 8 Enterprise.

Smurf attack :

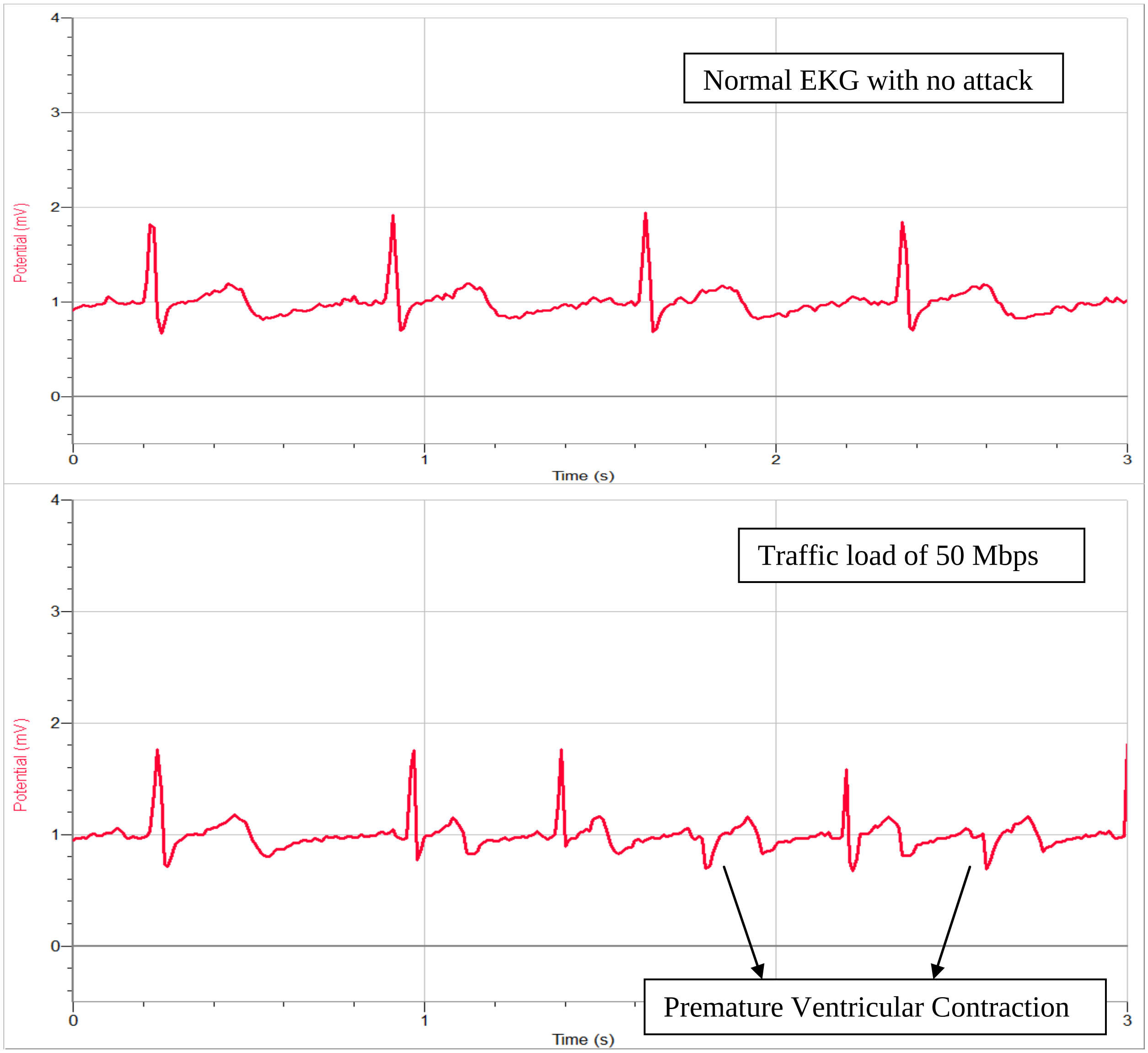


Fig 4.11 : Normal EKG vs Abnormal EKG at Smurf attack of 50 Mbps traffic

Under the Smurf attack of 50 Mbps attack traffic load, the attacked EKG signal showed Premature Ventricular Contraction and Sinus Tachycardia. The computer froze under this attack for four minutes, it could not perform any task or even open the applications and then displayed the abnormal EKG signal. Hence, we noticed both integrity and availability components in the CIA security triad were violated. This kind of performance is detrimental in the health care systems. If we observe the normal EKG signal with no attack, then the attacked signal seems abnormal that can lead to wrong diagnosis. From the Table 4.7, we observed the values of QT and RR interval and it indicates the rate of heartbeat which is increased. The possible values of RR intervals are given in the table. The processor and RAM utilization was 73% and 25% on the attacked EKG signal. This is processor intensive.

Table 4.7: Windows 8 Enterprise at Smurf attack of 50 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.69,0.72,0.73	0.36,0.37,0.36,0.37	2%	10%
50 Mbps	0.73,0.42,0.81	0.38,0.22,0.22,0.21,0.21,0.21	73 %	25 %

In the Figure 4.12, with 100 Mbps traffic under Smurf attack, the EKG signal showed abnormalities like Sinus Tachycardia, Myocardial Infarction and Premature Ventricular Contraction. In the Table 4.8, the QT and RR intervals were effected on the abnormal EKG signal under Smurf attack of 100 Mbps traffic load. We noticed, that there is an increase in rate of heartbeat which increases the RR interval and shortens the QT interval. The shortened QT interval vaues refers to Shorten QT syndrome genotype 1 -3. The processor and RAM utilization on the attacked signal was found to be 73% and 25% which is clearly processor intensive.

Table 4.8: Windows 8 Enterprise at Smurf attack of 100 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.69,0.72,0.73	0.36,0.37,0.36,0.37	2 %	10 %
100 Mbps	0.87,0.77,0.41	0.28,0.20,0.20,0.20,0.22,0.18	73 %	25 %

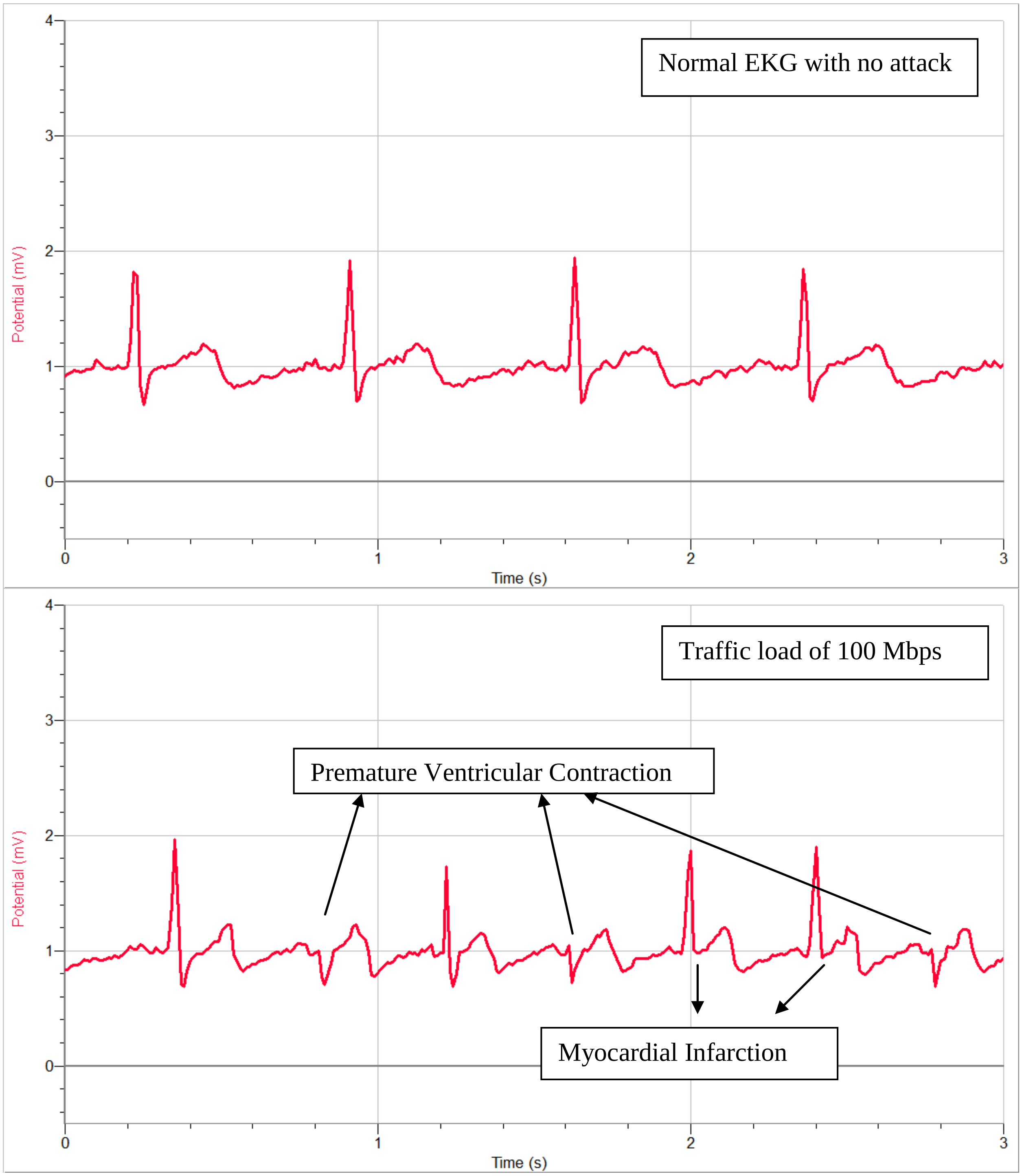


Fig 4.12 : Normal EKG vs Abnormal EKG at Smurf attack of 100 Mbps traffic

Under this Smurf attack of 300 Mbps traffic, the effect on the attacked EKG signal is too adverse. Five abnormalities are noticed such as Multifocal Atrial Tachycardia, Sinus Tachycardia, Hypothermia, Hyperthyroidism and Premature Ventricular Contraction in the attacked EKG signal. This is shown in the Figure 4.13, more distinct P waves are visible which indicates the abnormality Multifocal Atrial tachycardia. With J point deviation , Moderate Hypothermia is considered. Moreover, the displayed attacked EKG signal also includes low voltage QRS complexes, which refers to the abnormality Hyperthyroidism . The origin of the heartbeat is from the ventricles, which disrupts the normal one, then the abnormality Premature Ventricular Contraction is noticed. With the above mentioned abnormalities, we notice that Smurf attack has adverse effects on the data collection of EKG signals than any other attacks. The computer froze for about five minutes and then displayed the abnormal EKG signal. This violates both elements integrity and availability in the CIA security triad.

In the Table 4.9, The QT and RR intervals are effected on the attacked EKG signal under Smurf attack of 300 Mbps traffic load. We saw that there is an increase in the RR intervals and QT interval has reduced because of incresed heartbeat rate. The shorten QT interval vaues refers to Shorten QT syndrome genotype 1 -3. The processor and RAM utilization on the attacked signal were found to be 73% and 25% . This shows that it is processor intensive.

Table 4.9: Windows 8 Enterprise at Smurf attack of 300 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.69,0.72,0.73	0.36,0.37,0.36,0.37	2 %	10 %
300 Mbps	0.68,0.37,0.33,0.31	0.35,0.27,0.20,0.21,0.22	73 %	25 %

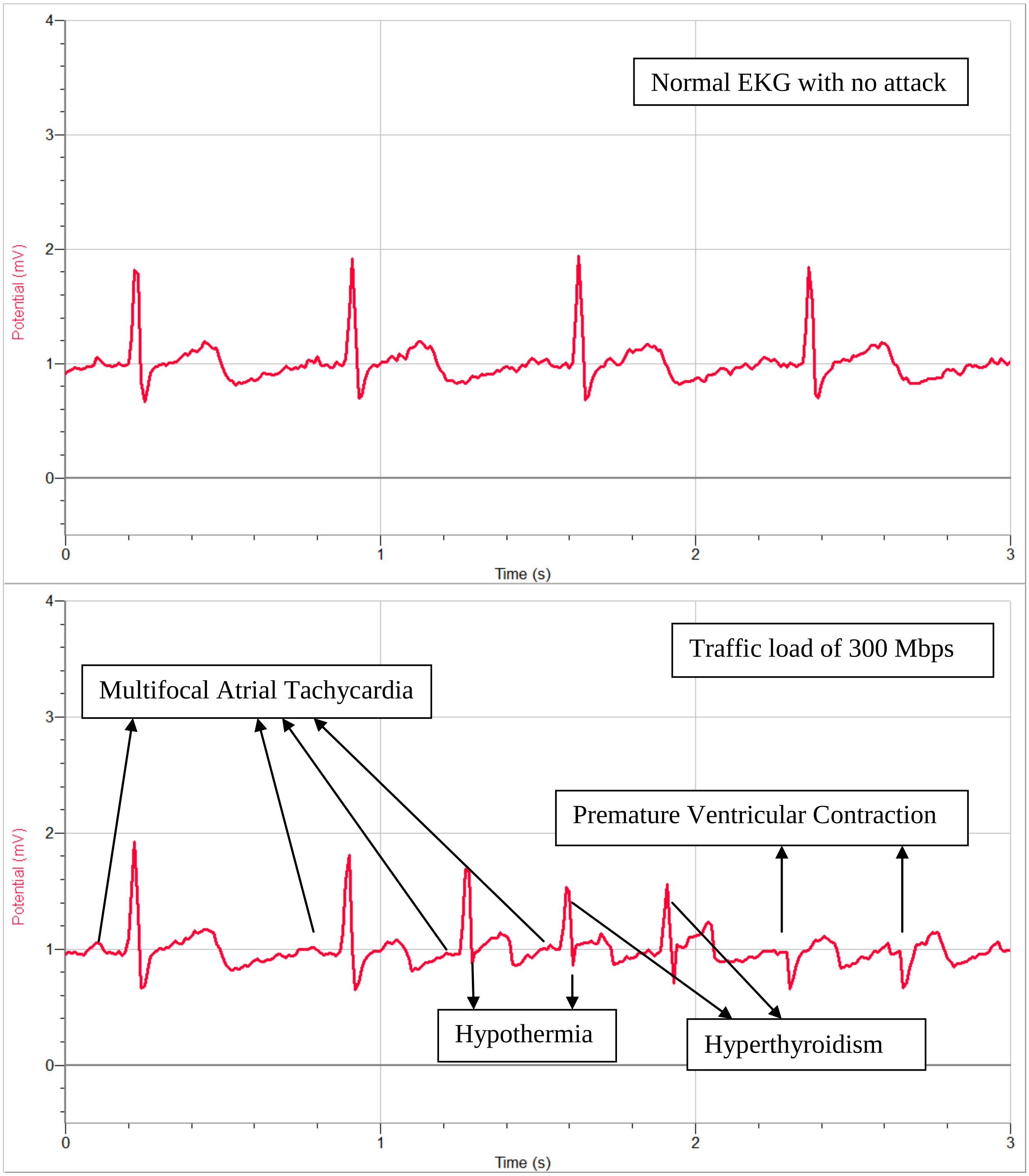


Fig 4.13 : Normal EKG vs Abnormal EKG at Smurf attack of 300 Mbps traffic

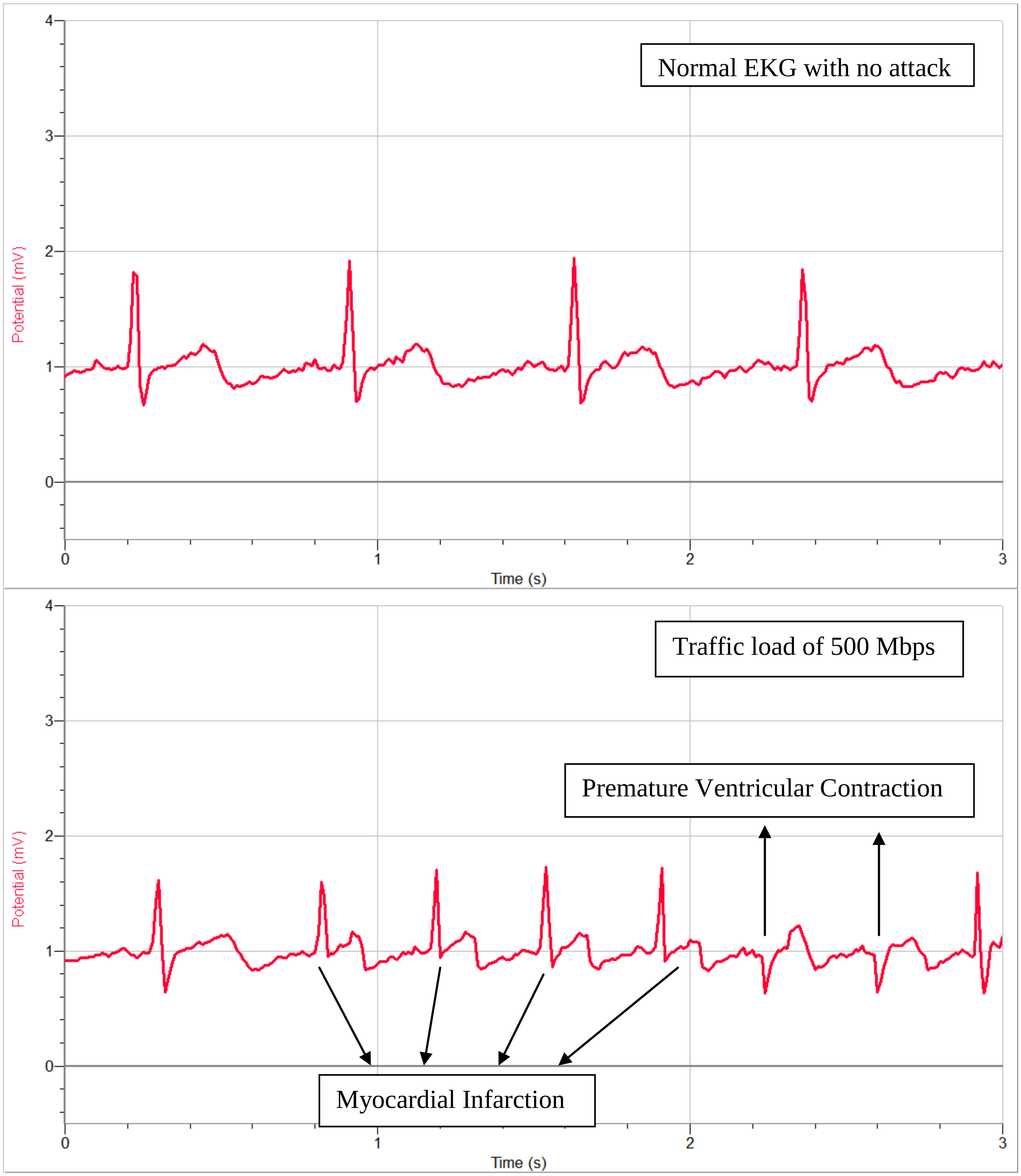


Fig 4.14 : Normal EKG vs Abnormal EKG at Smurf attack with 500 Mbps traffic

Under this Smurf attack of 500 Mbps traffic load, the effected EKG signal has abnormalities including Sinus Tachycardia, Myocardial Infarction and Premature Ventricular Contraction. In the Table 4.10, the RR intervals count is more in the attacked EKG signal under 500 Mbps traffic, than in the normal one. We even observed R-R interval value 1.01second , which is long. The QT interval has reduced so much as the heartbeat rate increased so much. QT interval modifies more slowly to decelerations than to accelerations of the heartbeat rate. It also refers to Shorten QT syndrome . This is more processor intensive. The processor and RAM utilization were 73% and 25% in the attacked EKG signal.

Table 4.10: Windows 8 Enterprise at Smurf attack of 500 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.69,0.72,0.73	0.36,0.37,0.36,0.37	2 %	10%
500 Mbps	0.52,0.37,0.35,0.37,1.01	0.37,0.20,0.20,0.22,0.22,0.20,0.22	73 %	25 %

In the Figure 4.15, at Smurf attack of 700 Mbps traffic load, abnormalities found are Premature Ventricular Contraction, Sinus Tachycardia, Myocardial Infarction, Hypothermia and Hyperkalaemia. Interestingly, five abnormalities are observed in the attacked EKG signal. In the Table 4.11, the QT interval has reduced as the heartbeat rate increased. As sinus tachycardia is considered as one of the abnormalities, more number of RR intervals are present in the attacked signal. The processor and RAM utilization were 73% and 25%, which indicates that it is processor intensive. The normal EKG signal information with the RR interval, the QT interval, processor usage and RAM details are also provided.

Table 4.11 : Windows 8 Enterprise at Smurf attack of 700 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.69,0.72,0.73	0.36,0.37,0.36,0.37	2 %	10 %
700 Mbps	0.75,0.40,0.75,0.37	0.20,0.20,0.20,0.22,0.20,0.21,0.20	73 %	25 %

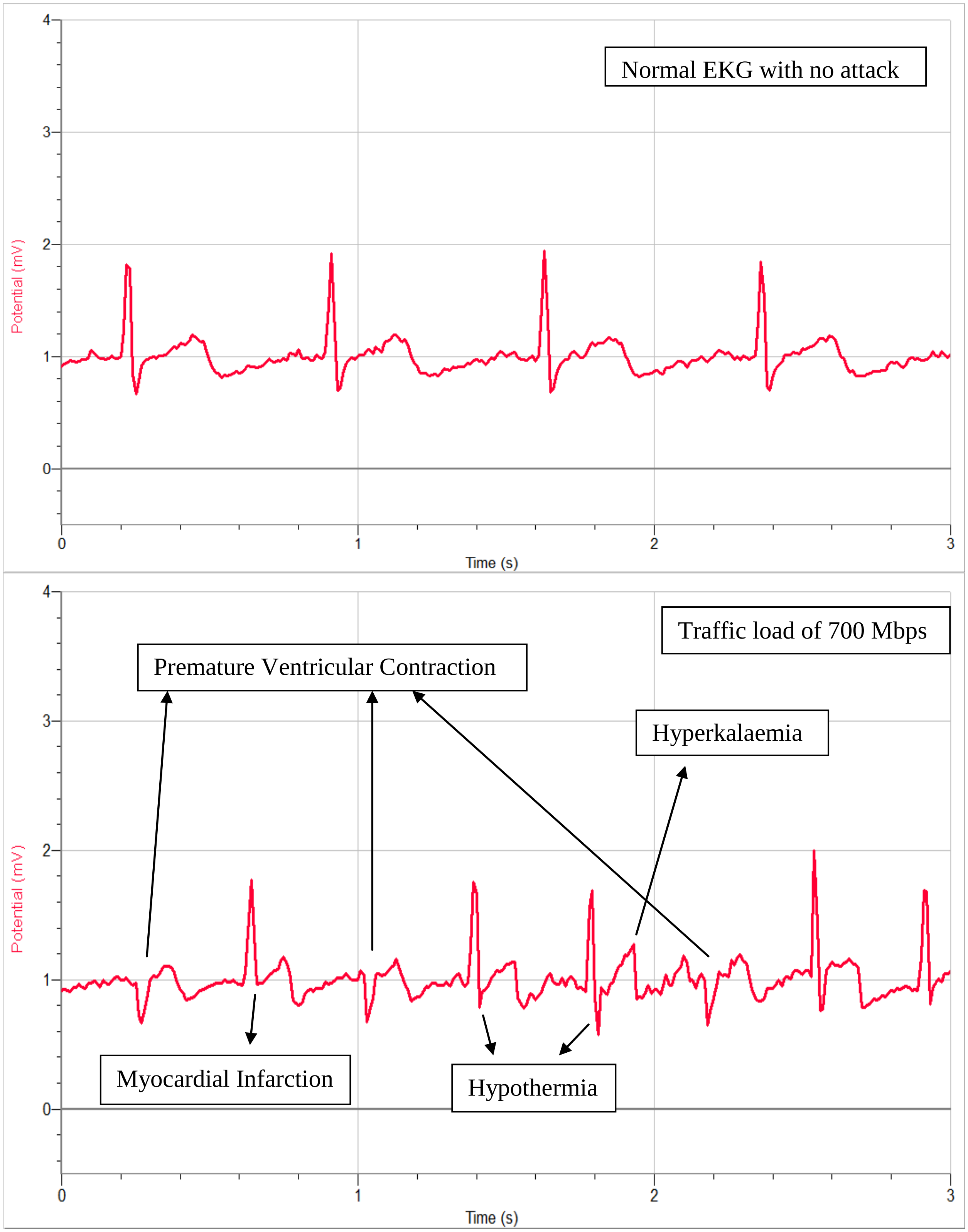


Fig 4.15 : Normal EKG vs Abnormal EKG at Smurf attack of 700 Mbps traffic

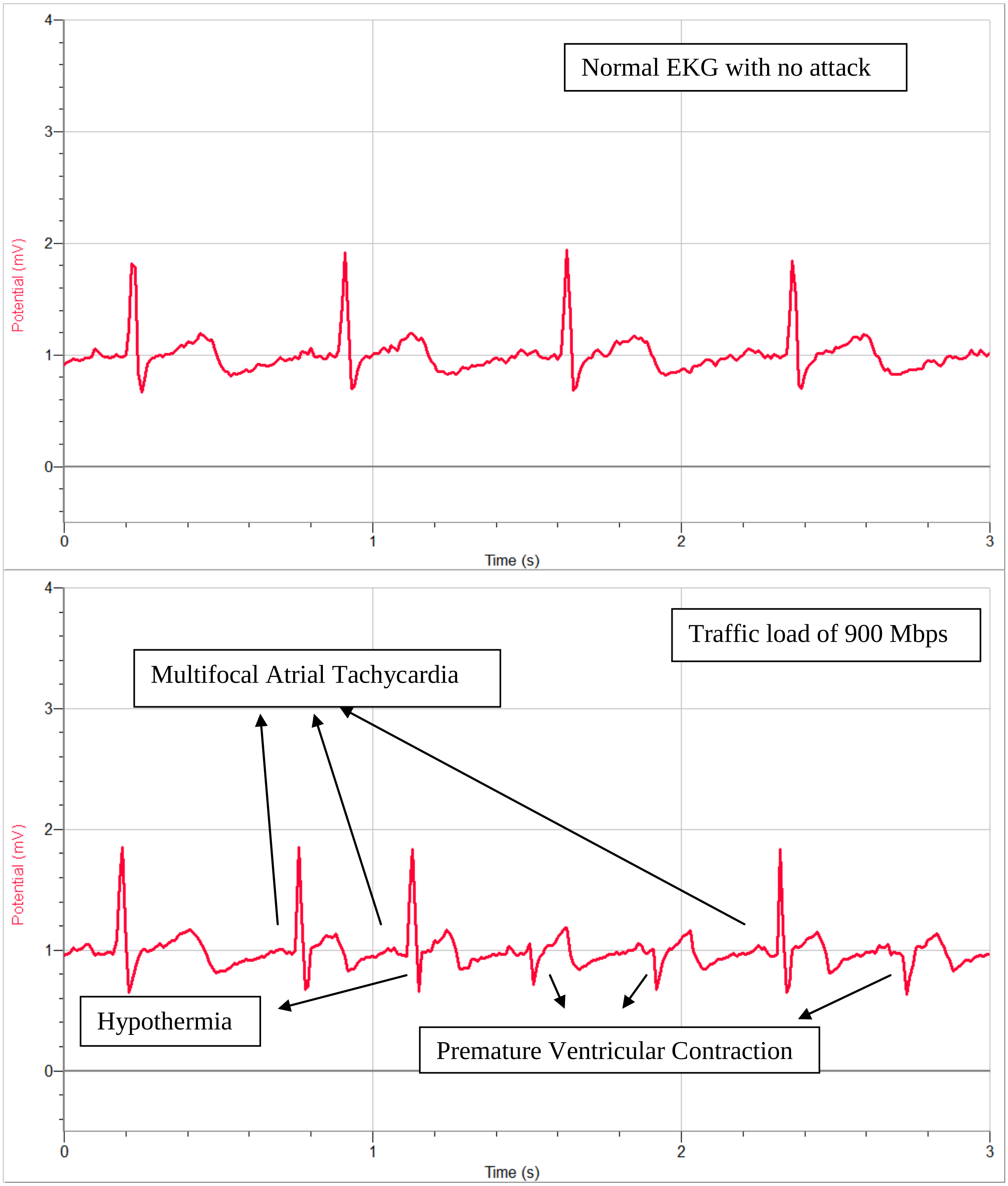


Fig 4.16 : Normal EKG vs Abnormal EKG at Smurf attack with 900 Mbps traffic

In the Figure 4.16, at Smurf attack of 900 Mbps traffic, the abnormalities observed are Hypothermia, Multifocal Atrial Fibrillation, Sinus Tachycardia and Premature Ventricular Contraction. Smurf attack, has adverse effects on the data collection of EKG signals than any other attack. The computer froze for about seven minutes in all the traffic conditions under this attack and then displayed the abnormal EKG signal. By this, availability and integrity elements in the CIA security triad are violated. QT interval modifies more slowly to decelerations than to accelerations of the heartbeat rate. In the Table 4.12, the QT interval has reduced so much as the heartbeat rate increased so much. It also refers to Shorten QT syndrome . This is more processor intensive. The processor and RAM utilization are 73% and 25% in the attacked EKG signal. With the increase in the heartbeat rate, more number of RR interval values are present. Possible values of RR are listed in the table.

Table 4.12 : Windows 8 Enterprise at Smurf attack of 900 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.69,0.72,0.73	0.36,0.37,0.36,0.37	2 %	10 %
900 Mbps	0.57,0.37,1.19	0.36,0.19,0.21,0.12,0.19,0.21	73 %	25 %

In this case of 1000 Mbps traffic under Smurf attack, the computer froze for about eight minutes and displayed the EKG signal which has some abnormalities. The subject whose EKG was monitored needs to wait for about eight minutes having EKG sensor electrodes attached to the the body until the computer starts showing EKG signal in the display. This violated availability and integrity elements in the security concern. The abnormalities we observed with this traffic load are Hypothermia, Sinus Tachycardia, Myocardial Infarction and Hypothyroidism. In the Figure 4.17, it includes normal EKG signal which was taken at rest position and attacked EKG signal which is abnormal.

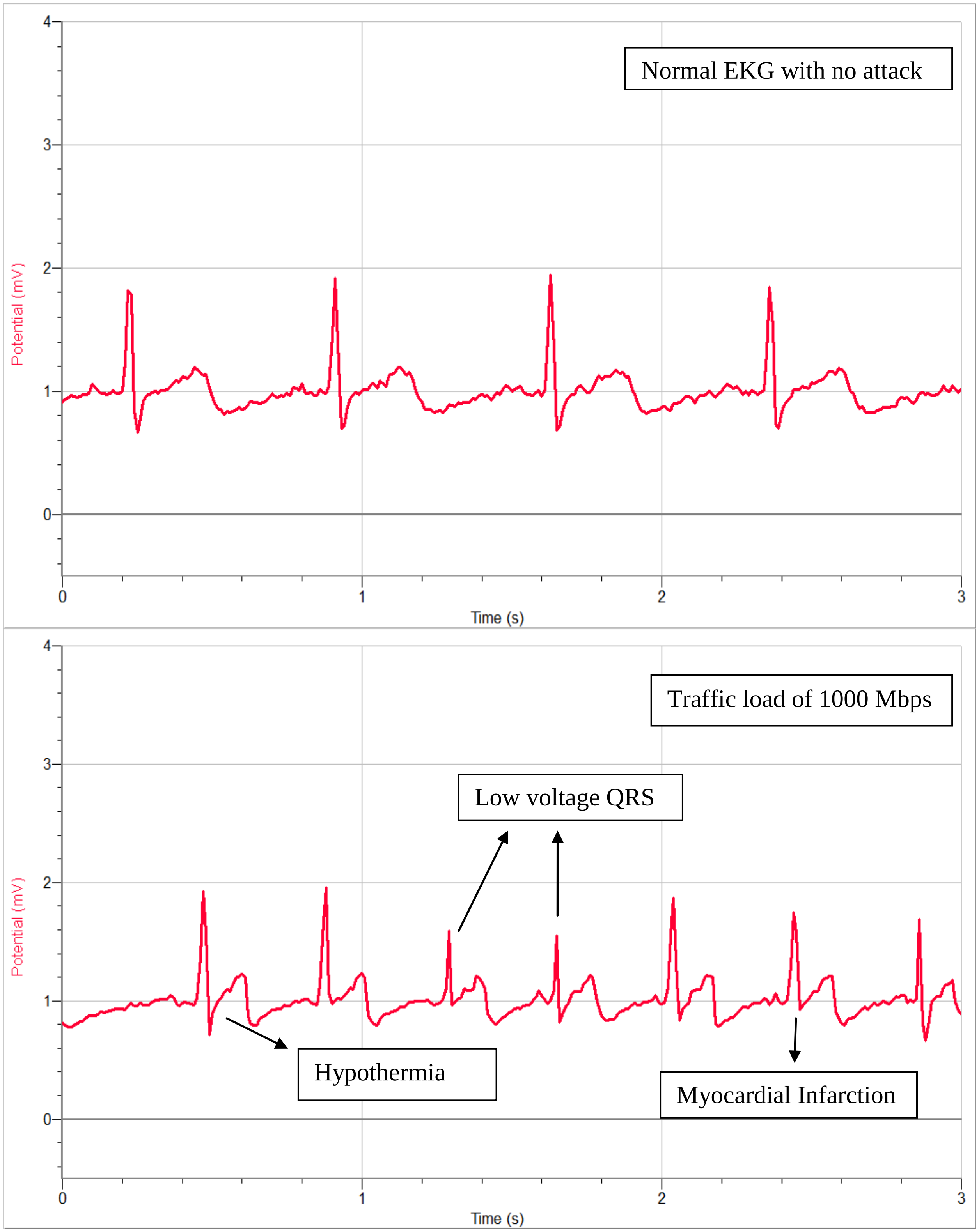


Fig 4.17 : Normal EKG vs Abnormal EKG at Smurf attack of 1000 Mbps traffic

In the Table 4.13, the QT and RR interval effected in the attacked EKG signal at 1000 Mbps traffic under Smurf attack. The QT interval has reduced which indicates Shorten QT sydrome genotype 1-3. As the heartbeat rate increased, in the attacked EKG signal QT interval has reduced and an increase of RR intervals are present. The processor and RAM usage were found to be 73% and 25% which clearly shows that it is processor intensive.

Table 4.13: Windows 8 Enterprise at Smurf attack of 1000 Mbps traffic

Traffic	RR Interval (sec)	QT Interval (sec)	Processor Used	RAM Used
Normal	0.69,0.72,0.73	0.36,0.37,0.36,0.37	2%	10%
1000 Mbps	0.40,0.42,0.36,0.39,0.40,0.42	0.24,0.23,0.20,0.23,0.21,0.23	73 %	25 %

Ping Attack:

This is another kind of attack that was performed with different traffic conditions, the processor utilization was found to be 52% and RAM used is 25%. Even though the processor utilization is not high, however we saw abnormal EKG signal under this attack. We observed abnormalities Sinus bradycardia and Left Atrial Enlargement. Sinus bradycardia, as less number of R-R intervals are present in the attacked EKG signal than R-R intervals in the normal EKG signal with no attack. Left Atrial Enlargement noticed in the attacked EKG signal because of camel hump P wave.

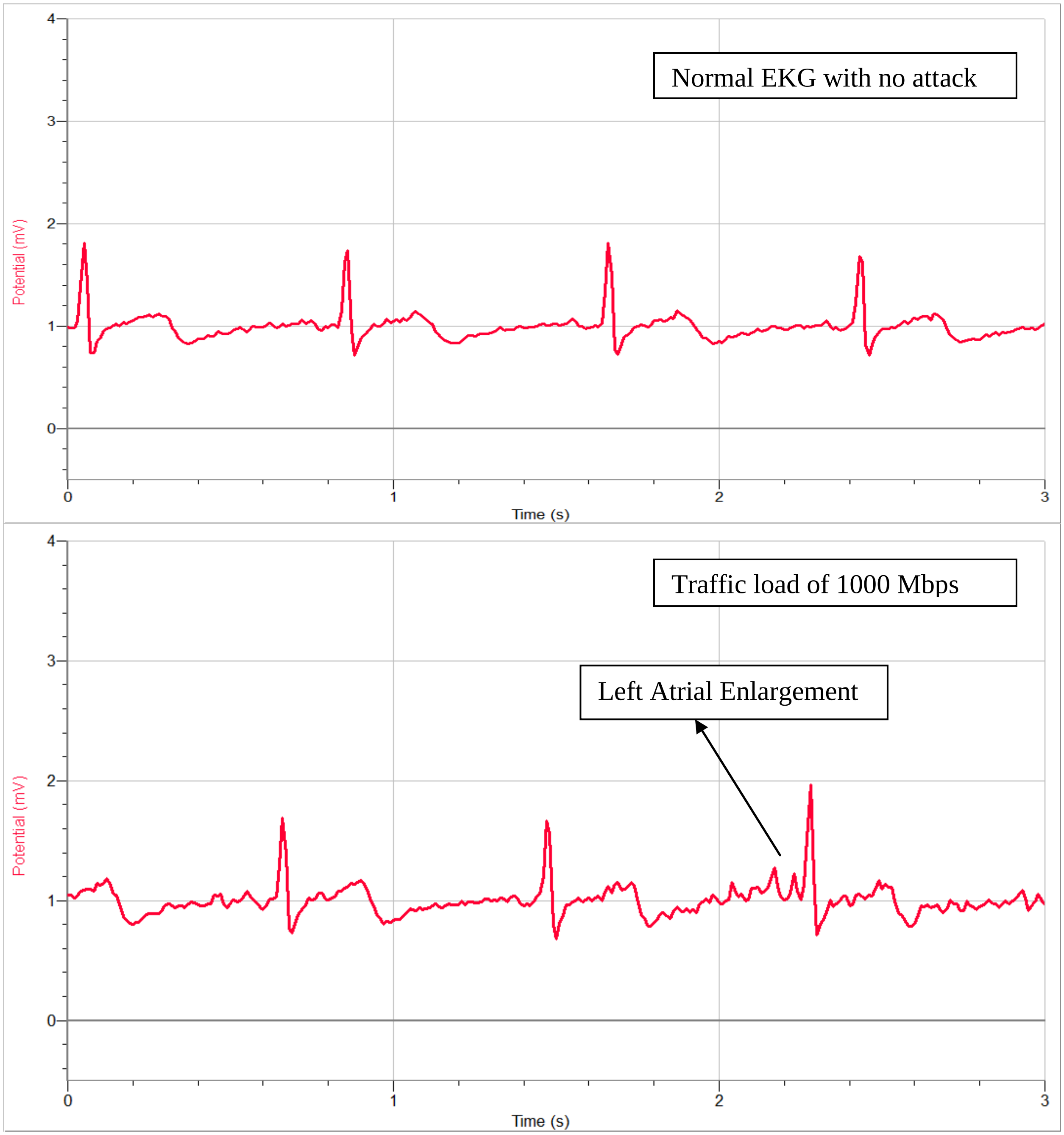


Fig 4.18 : Normal EKG vs Abnormal EKG at Ping attack with 1000 Mbps traffic

ARP Attack :

The result of attacked EKG signal under ARP attack with 500 Mbps traffic load is shown in the below figure.

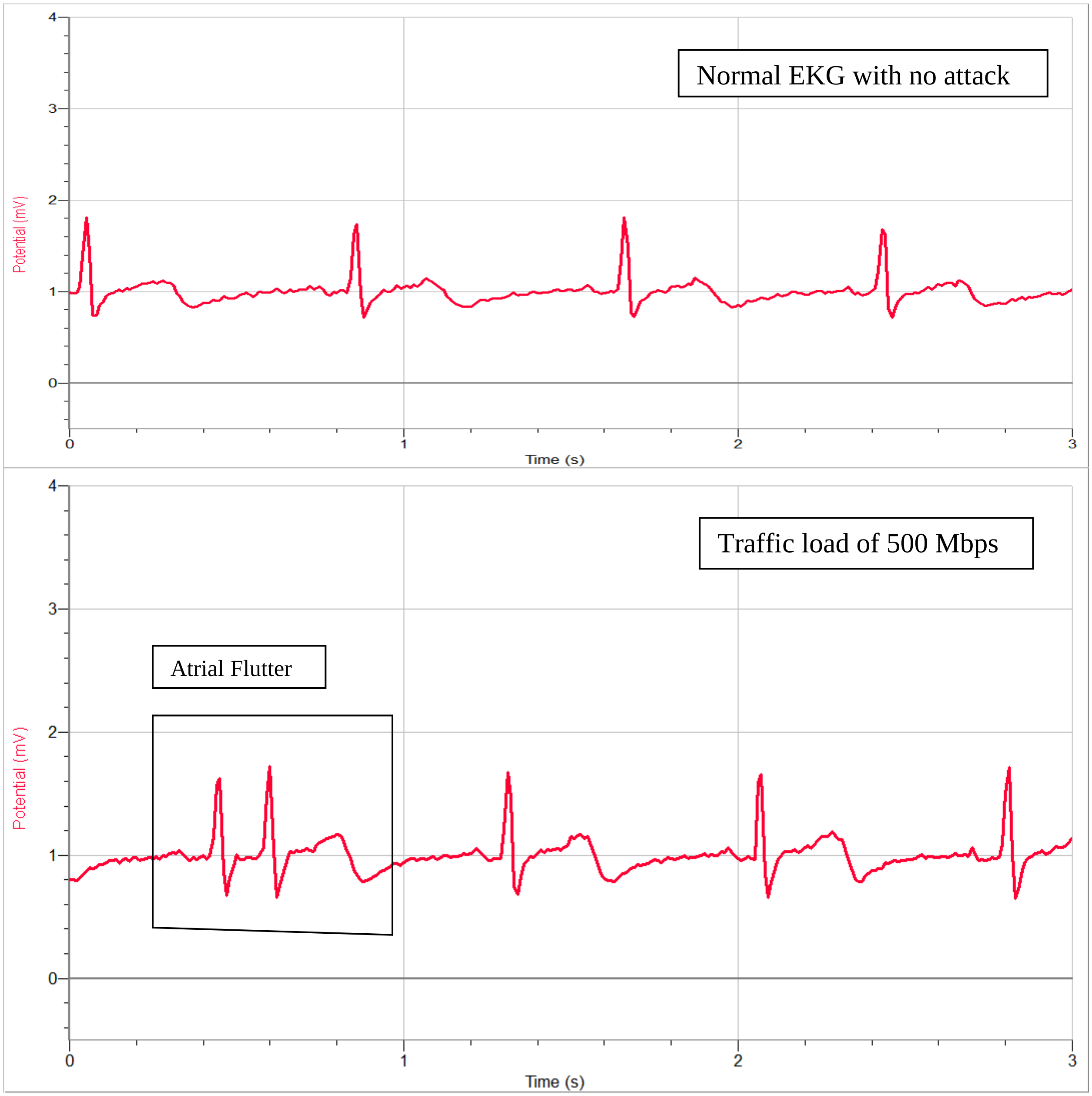


Fig 4.19 : Normal EKG vs Abnormal EKG at ARP attack of 500 Mbps traffic

At ARP attack of 500 Mbps traffic load, the abnormalities found are Sinus Tachycardia and Atrial Flutter. Atrial Flutter abnormality , because there is no end of T wave and origin of P wave at some point of heart beat. Sinus Tachycardia, more number R-R intervals in the attacked EKG signal than in the EKG signal at normal condition.

ARP attack, Smurf attack, TCP SYN attack and Ping attack were performed on this operating system Windows 8 Enterprise. Based on the results, this operating system is more vulnerable to Smurf attack. The interesting things are : 1) First, at ARP attack of 200 Mbps traffic, the victim computer has effected due to the attack and processor exhaustion. It disabled the software application which captures the EKG signal. Hence, attack is stopped and turned on the computer again to recover the EKG signal that was captured earlier which is not displayed at that time. 2) Second, at ARP attack of 300 Mbps traffic, the response of the computer is very similar to the above case and froze for more than ten minutes and doesn't show any data on the display for a long time. 3) Third, at TCP SYN attack from 700 Mbps traffic load to 1000 Mbps traffic there was a situation, where the computer froze completely and disabled the option to capture the EKG signal. Hence, the sensor plugged in again and waited for some time to make that option enable in the software application.

4.7 Results in Windows 8.1 Enterprise

Denial of Service attacks, such as ARP, TCP SYN, Ping and Smurf attacks were performed in the operating system Windows 8.1 Enterprise. The maximum traffic that reached to the victim computer was 1000 Mbps by the simulator, the attacked EKG signal doesn't look abnormal. It means the normal EKG signal with no attack and the attacked EKG signal under different traffic load conditions has shown no abnormalities. Moreover, the computer doesn't even crash at all and it was normal under all attacks. Hence, this holds the security elements Availability and Integrity. This is the better operating system which sustained for the above mentioned denial of service attacks at all traffic loads under 1000 Mbps, when compared to other operating systems.

Windows 8.1 Enterprise operating system that has more likely complied with HIPAA standards, and also not compromised with the elements Integrity and Availability of the CIA security triad. The other deployed operating systems showed different abnormalities in different traffic loads at various attacks. They have violated the HIPAA standards and CIA security triad as well. Real time EKG signals monitoring is an important data collection for medical services. Hence, the data displays on the EKG monitor, which is the computer must provide reliable information for the person who is monitoring it for diagnosis.

The results of attacked EKG signals at high traffic loads under ARP, TCP SYN, Ping, Smurf attacks are displayed. In the case of ARP attack, the Figure 4.20 shows you how the attacked EKG signal was at 1000 Mbps traffic. This figure 4.20, compared the normal EKG with no attack and attacked EKG signal. The attacked EKG signal doesn't show any abnormalities for this attack even for worst traffic load of 1000 Mbps. Security Integrity is not affected and in that sense it can comply with HIPAA standards for security.

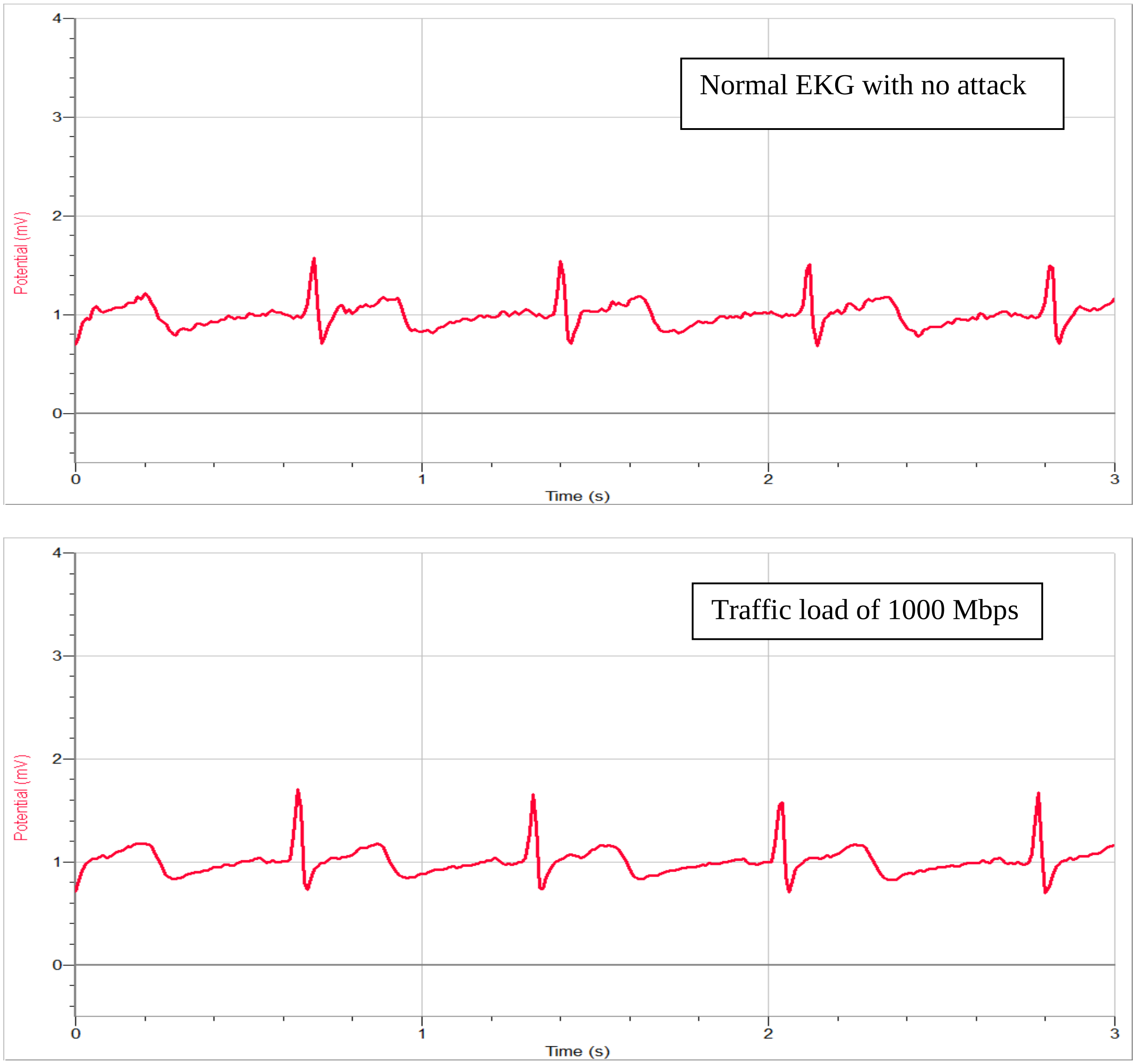


Fig 4.20 : EKG with no attack vs Worst case ARP attack of 1000 Mbps traffic

In the case of Ping attack, the Figure 4.21 shows you how the attacked EKG signal was at 1000 Mbps traffic. This figure 4.21, compared the normal EKG with no attack and attacked EKG signal. The attacked EKG signal doesn't show any abnormalities for this attack even for worst traffic load of 1000 Mbps. Security Integrity is not affected and in that sense it can comply with HIPAA standards for security.

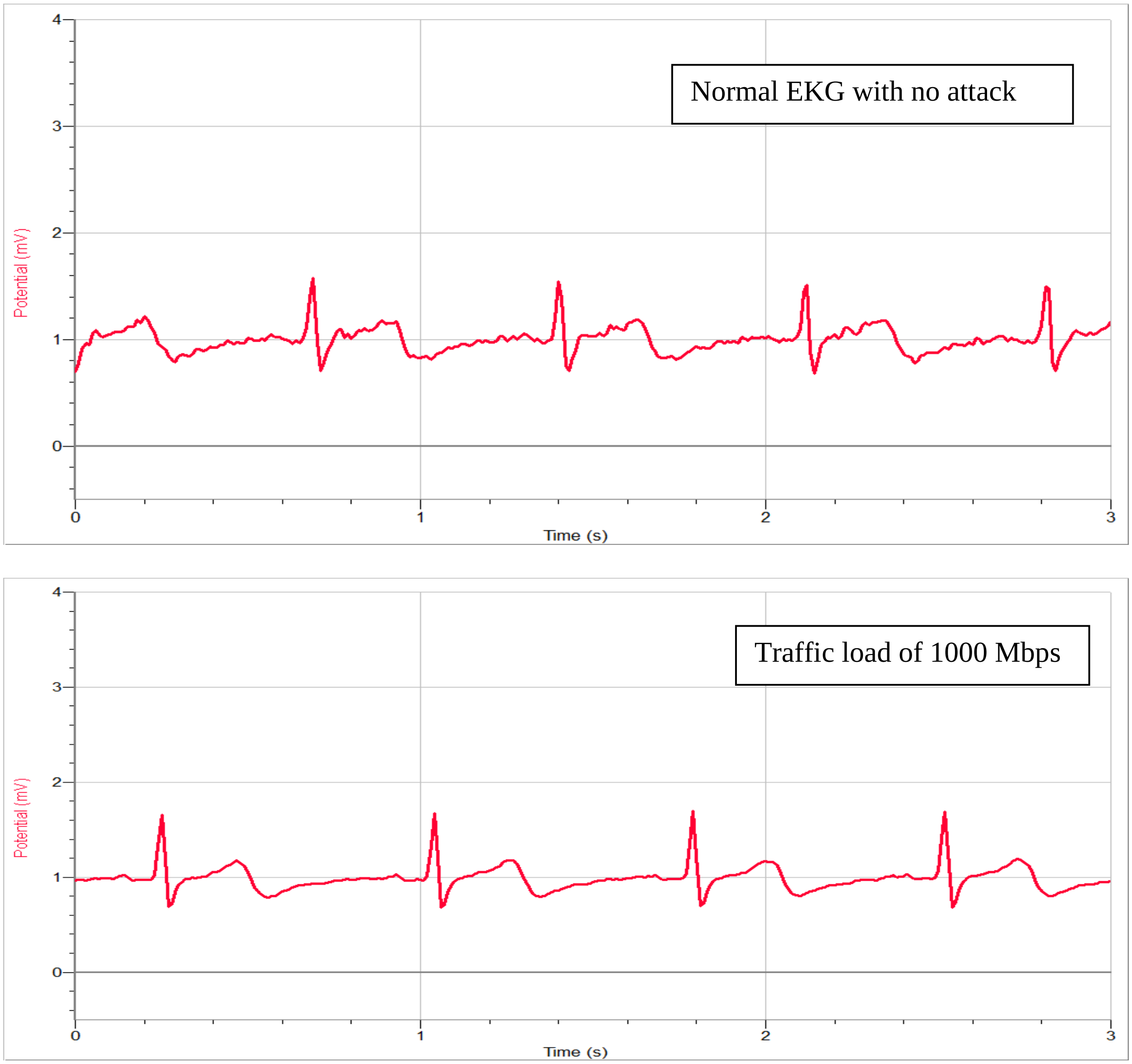


Fig 4.21 : EKG with no attack vs Worst case Ping attack of 1000 Mbps traffic

In the case of Smurf attack, the Figure 4.22 shows you how the attacked EKG signal was at 1000 Mbps traffic. This figure 4.22, compared the normal EKG with no attack and attacked EKG signal. The attacked EKG signal doesn't show any abnormalities for this attack even for worst traffic load of 1000 Mbps. Security Integrity is not affected and in that sense it can comply with HIPAA standards for security.

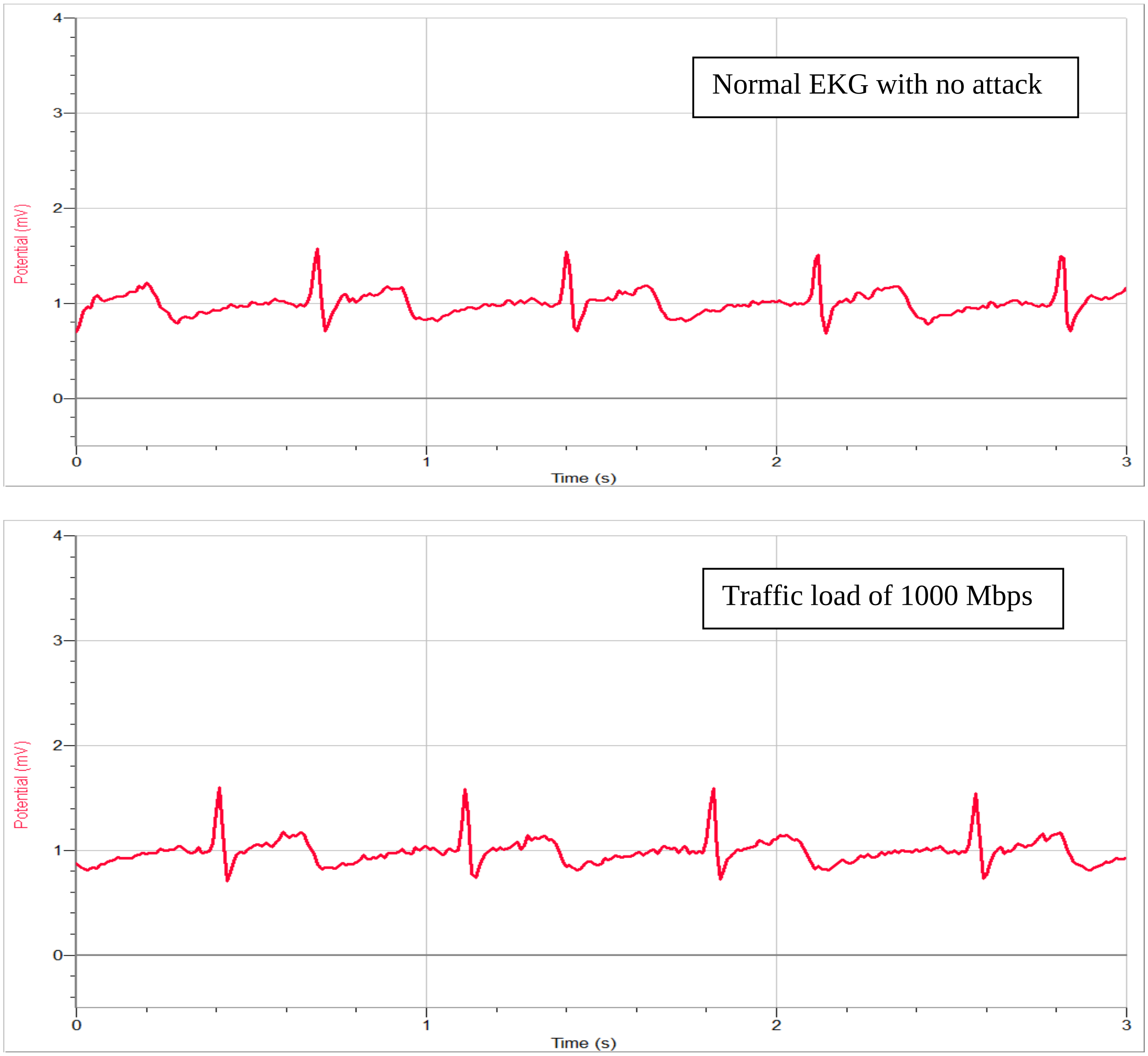


Fig 4.22 : EKG with no attack vs Worst case Smurf attack of 1000 Mbps traffic

In the case of TCP SYN attack, the Figure 4.23 shows you how the attacked EKG signal was at 1000 Mbps traffic. This figure 4.23, compared the normal EKG with no attack and attacked EKG signal. The attacked EKG signal doesn't show any abnormalities for this attack even for worst traffic load of 1000 Mbps. Security Integrity is not affected and in that sense it can comply with HIPAA standards for security.

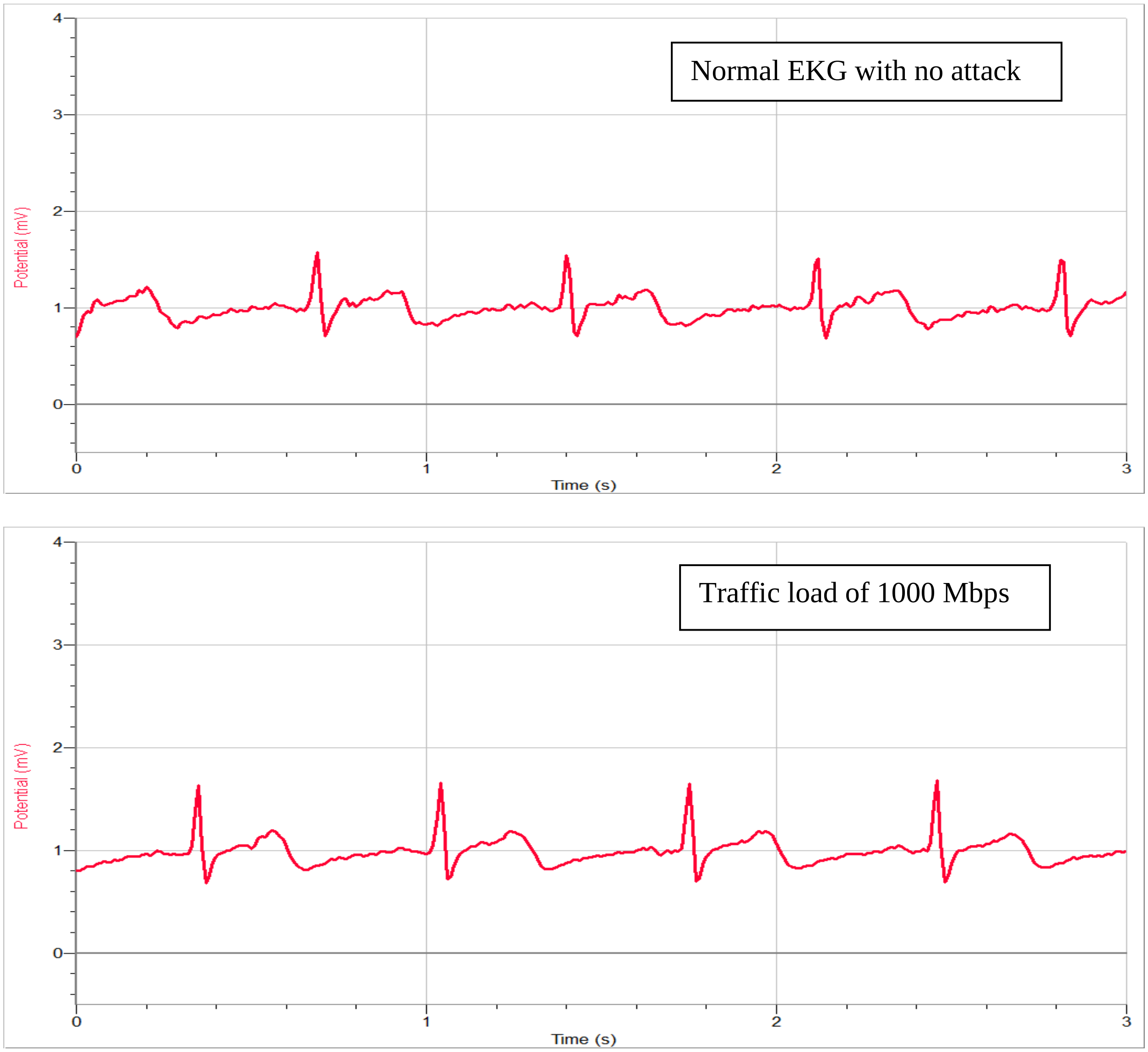


Fig 4.23 : EKG with no attack vs Worst case TCP SYN attack of 1000 Mbps traffic

4.8 Availability Problems in Windows Vista Ultimate

In this operating system, Availability element is violated. If the simulator starts running the attack of 100 Mbps traffic to the computer where EKG is monitored, the computer crashed and EKG signal is lost. Attack was stopped and restarted the computer. For ARP,TCP SYN, Ping and Smurf attacks the computing resources of the computer were exhausted. The computer froze for a long time and it also disabled the software application which collects the

EKG data. Hence, this computer needs to start again which leads to loss of EKG information. By this, it is violating the element availability. This operating systems didn't comply with HIPAA standards and also compromised with the element availability in the CIA security triad. This leaves the health care system unprotected.

The Table 4.14, gives the information about total data bit rate and packets received at ARP attack. The range of traffic introduced to the victim computer is from 100 Mbps to 1000 Mbps traffic, and their respective data bit rates and packets received count are given. When the attack traffic has sent to the victim computer, for an example if 100 Mbps traffic is pushed towards the computer from simulator, the destination receives only 76.19 Mbps because it's the actual payload, the rest is allotted for the packet header.

Table 4.14: Total Data Bit Rate & Packets per second received at ARP attack

Traffic (Mbps) Sent	Total Data Bit rate (Mbps) Received	Total Packets per second (fps) Received
100	76.19	148,809.52
200	152.38	297,619.05
300	228.571	446,428.57
400	304.762	595,238.09
500	380.952	744,047.62
600	457.153	892,857.14
700	533.333	1041,666.7
800	615.385	1201,923.1
900	695.652	1,358,695.7
1000	761.905	1,488,095.2

Table 4.15, gives the information about total data bit rate and packets received at TCP SYN attack. The range of traffic introduced to the victim computer is from 100 Mbps to

1000 Mbps traffic, and their respective data bit rates and packets received count are given. For an example if 100 Mbps traffic is pushed towards the computer from simulator, the destination receives only 76.19 Mbps because it's the actual payload, the rest is allotted for the packet header.

Table 4.15: Total Data Bit Rate & Packets per second received at TCP SYN attack

Traffic (Mbps) Sent	Total Data Bit rate (Mbps) Received	Total Packets per second (fps) Received
100	76.19	148,809.52
200	152.38	297,619.05
300	228.571	446,428.57
400	304.762	595,238.09
500	380.952	744,047.62
600	457.153	892,857.14
700	533.333	1041,666.7
800	615.385	1201,923.1
900	695.652	1,358,695.7
1000	761.905	1,488,095.2

Table 4.16, gives the information about total data bit rate and packets received at Smurf attack. The range of traffic introduced to the victim computer is from 100 Mbps to 1000 Mbps traffic, and their respective data bit rates and packets received count are given. For an example if 100 Mbps traffic is pushed towards the computer from simulator, the destination

receives only 76.19 Mbps because it's the actual payload, the rest is allotted for the packet header.

Table 4.16: Total Data Bit Rate & Packets per second received at Smurf attack

Traffic (Mbps) Sent	Total Data Bit rate (Mbps) Received	Total Packets per second (fps) Received
100	76.19	148,809.52
200	152.38	297,619.05
300	228.571	446,428.57
400	304.762	595,238.09
500	380.952	744,047.62
600	457.153	892,857.14
700	533.333	1041,666.7
800	615.385	1201,923.1
900	695.652	1,358,695.7
1000	761.905	1,488,095.2

Table 4.17, gives the information about total data bit rate and packets received at Ping attack. The range of traffic introduced to the victim computer is from 100 Mbps to 1000 Mbps traffic, and their respective data bit rates and packets received count are given. For an example if 100 Mbps traffic is pushed towards the computer from simulator, the destination receives only 76.19 Mbps because it's the actual payload, the rest is allotted for the packet header.

Table 4.17: Total Data Bit Rate & Packets per second received at Ping attack

Traffic (Mbps) Sent	Total Data Bit rate (Mbps) Received	Total Packets per second (fps) Received
100	86.486	84,459.459
200	172.973	168,918.92
300	260.163	254,065.04
400	345.946	337,837.84
500	432.432	422,297.3
600	520.325	508,130.08
700	609.524	595,238.09
800	695.652	679,347.83
900	780.488	762,195.12
1000	864.865	844,594.59

CHAPTER V

CONCLUSIONS

This thesis investigates the effects of different network attacks on integrity of EKG signal data collection over Microsoft's Windows platform. EKG - BTA is the EKG sensor from Vernier company connected to the computer for capturing the EKG signal, and Logger Lite(1.3.2) is the software application used to collect the EKG data. Over the last decade, computer networks have been targeted to widespread security attacks. Network attacks are combined by attack – the network protocol-based attack, host-based attacks and attacks on network application layer [42]. In the last year, DoS attacks emerged in strategy and tactics. There is growing trend in DDoS attacks, about 55% of DDoS attacks happened for theft: intellectual property, customer data and funds. If you compare the DDoS attacks impact on internet, it is devastating many top companies. Almost 90 % of attacks are repetitive [43] . Advance research is going on to use EKG signal as Biometric Identification to access permission in vital areas. As the EKG signal is a Live signal, this information is more reliable than finger print, Iris, face recognition and other biometric standards [44].

Based on the above results, we can conclude that operating system Windows 8.1 Enterprise has sustained to attacks like ARP, TCP SYN, Ping, Smurf under 1000 Mbps traffic. Interestingly, with Smurf attack, the processor consumption was 85% and still the operating system hold the security elements availability and integrity in the CIA security triad and more likely to comply with HIPAA standards. The attacked EKG signal doesn't show any abnormalities when compared to normal EKG signal. Moreover, the computer didn't freeze under all attack traffic conditions. From this, we can say that Windows 8.1 Enterprise is good enough to hold the above denial of service attacks under 1000 Mbps traffic load. All the experiments were done in a controlled environment in the Network Research Lab. Windows 8.1 Enterprise didn't violate Integrity and Availability and they are more likely to comply with HIPAA standards. The person who monitors real time EKG signals, can easily raise false alarm when that particular computer is deployed with above operating systems other than Windows 8.1 Enterprise.

Below are the tables which provides the total information on what network attack under which operating system and how much attack traffic experienced by the target system. The Table 5.1 refers to the operating system Windows XP with Service Pack3, with details such as attack implemented, how much traffic generated and changes in the EKG signal which turns out to be abnormalities.

Table 5.1 : False EKG Abnormalities found in Windows XP with SP3

I = Integrity Violation , A = Availability Violation

Operating System	Attack & CIA Violations	Traffic (Mbps)	Display of Abnormality	Changes in EKG signal
Windows XP with SP3	ARP Violations: I,A	50	Premature Ventricular Contraction, Myocardial Infarction, Pericarditis, Hypothermia, Sinus Tachycardia	More number of R-R intervals are present.
Windows XP with SP3	ARP Violations: I,A	100	Premature Ventricular Contraction, Hyperkalaemia, Sinus Tachycardia Hypothermia, Hyperthyroidism,	More number of R-R intervals are present. Low voltage QRS complex.

Windows XP with SP3	ARP Violations: I,A	150	Premature Ventricular Contraction, Hyperkalaemia, Hypothermia, Sinus Tachycardia.	Peaked T waves. More number of R-R intervals are present.
Windows XP with SP3	ARP Violations: I,A	200	Hyperkalaemia, Hyperthyroidism, Sinus Tachycardia, Premature Ventricular Contraction	Low voltage QRS complex, Peaked T waves. More R waves

The Table 5.2 refers to the operating system Windows 7 Ultimate with Service Pack1, with details such as attack implemented, how much traffic generated and changes in the EKG signal which turns out to be abnormalities.

Table 5.2: False EKG Abnormalities found in Windows 7 Ultimate with SP1

I = Integrity Violation , A = Availability Violation

Operating System	Attack & CIA Violations	Traffic (Mbps)	Display of Abnormality	Changes in EKG signal
Windows 7 Ultimate SP1	Ping Violations: I	300	Hyperkalaemia	Peaked T wave
Windows 7 Ultimate SP1	Smurf Violations: I,A	600	Hypothyroidism, Atrial Fibrillation	Irregular EKG signal, Low voltage QRS.
Windows 7 Ultimate SP1	Smurf Violations: I,A	800	Hyperthyroidism, Multifocal Atrial Tachycardia.	Low voltage QRS complex, More number of R-R intervals are present.
Windows 7 Ultimate SP1	Smurf Violations: I,A	900	Hyperthyroidism, Multifocal Atrial Tachycardia	Low voltage QRS complex, More number of R-R intervals are present.

The Table 5.3 refers to the operating system Windows 7 Enterprise, with details such as attack implemented, how much traffic generated and changes in the EKG signal which turns out to be abnormalities .

Table 5.3 : False EKG Abnormalities found in Windows 7 Enterprise

I = Integrity Violation , A = Availability Violation

Operating System	Attack & CIA Violations	Traffic (Mbps)	Display of Abnormality	Changes in EKG signal
Windows 7	ARP Violations: I,A	400	Multifocal Atrial Tachycardia	Three distinct P waves
Windows 7	ARP Violations: I,A	1000	Multifocal Atrial Tachycardia	Three distinct P waves

The Table 5.4 refers to the operating system Windows 8 Enterprise, with details such as attack implemented, how much traffic generated and changes in EKG signal which turns out to be abnormalities.

Table 5.4 : False EKG Abnormalities found in Windows 8 Enterprise

I = Integrity Violation , A = Availability Violation

Operating System	Attack & CIA Violations	Traffic (Mbps)	Display of Abnormality	Changes in EKG signal
Windows 8	ARP Violations: I,A	500	Atrial Flutter	The end of T wave and origin of P wave are combined.
Windows 8	Ping Violations: I,A	1000	Left Atrial Enlargement	Camel hump P waves are present.
Windows 8	Smurf Violations: I,A	50	Premature Ventricular Contraction, Sinus Tachycardia	More number of R-R intervals are present
Windows 8	Smurf	100	Premature Ventricular	More number of

	Violations: I,A		Contraction, Sinus Tachycardia, Myocardial Infarction	R-R intervals are present
Windows 8	Smurf Violations: I,A	300	Premature Ventricular Contraction, Multifocal Atrial tachycardia, Hypothermia, Hyperthyroidism	Three distinct P waves, Low Voltage QRS complex
Windows 8	Smurf Violations: I,A	500	Premature Ventricular Contraction, Myocardial Infarction, Sinus Tachycardia	More number of R-R intervals are present
Windows 8	Smurf Violations: I,A	700	Premature Ventricular Contraction, Myocardial Infarction , Hypothermia, Hyperkalemia	Peaked T wave
Windows 8	Smurf Violations: I,A	900	Premature Ventricular Contraction, Multifocal Atrial Tachycardia, Hypothermia, Sinus Tachycardia.	Three distinct P waves
Windows 8	Smurf Violations: I,A	1000	Hypothermia, Myocardial Infarction, Hyperthyroidism, Sinus Tachycardia	More number of R-R intervals are present.

The Table 5.5 refers to the operating system Windows 8.1 Enterprise, with details such as attack implemented, how much traffic generated and changes in the EKG signal.

Table 5.5 : Results in Windows 8.1 Enterprise

I = Integrity Violation , A = Availability Violation

Operating System	Attack & CIA Violations	Traffic (Mbps)	Display of Abnormality	Changes in EKG signal
Windows 8.1 Enterprise	ARP Violations: None	1000	None	None
Windows 8.1 Enterprise	TCP SYN Violations: None	1000	None	None

Windows 8.1 Enterprise	Smurf Violations: None	1000	None	None
Windows 8.1 Enterprise	Ping Violations: None	1000	None	None

The components of Integrity and Availability in the CIA security triad are not violated for the operating system Windows 8.1 Enterprise. Hence, from the above experimental results, Windows 8.1 Enterprise didn't suffer from loss of Integrity and Availability for the DoS attacks considered. Hence, it is more likely to comply with HIPAA standards of security.

REFERENCES

[1] Technology News : Denial of Service Attacks rip the internet. April 2000 http://ezhost.utpa.edu:2158/stamp/stamp.jsp?tp=&arnumber=839316&tag=1

[2] A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. BY Zargar S.T, Tipper.D. Communications Surveys & Tutorials, IEEE, Volume : 15, Issue: 4, Pages : 2046 - 2069

[3] DDoS &Security Report : http://www.arbornetworks.com/asert/2015/01/ddos-attacks-in-the-wake-of-french-anti-terror-demonstrations/

[4] Associated Press, Big Story : http://bigstory.ap.org/article/806d34082511483cafe2deaa1a7e6061/car-hits-injures-officer-french-presidential-palace

[5] Latest News on DDoS Attacks. http://www.ddosattacks.net/

[6] A Taxonomy of DDoS Attack and DDoS Defense Mechanisms by Jelena Mirkovic, Peter Reiher. http://www.eecis.udel.edu/~sunshine/publications/ccr.pdf

[7] DDOS Protection Center ; https://www.incapsula.com/ddos/ddos-attacks/

[8] The information on CIA triad ; http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[9] HIPAA, http://health.state.tn.us/hipaa/

[10] Functioning of the heart : http://www.sads.org.uk/heart_function.htm

[11] Information on Electrocardiography. http://www.ohio.edu/people/schwiria/objectives&introtoekg.htm

[12] EKG Learning Center [Online]. http://ecg.utah.edu/

[13] ECG Library. Life in the Fastlane http://lifeinthefastlane.com/ecg-library/

[14] EKG Interpretation made Incredibly easy by Wolters Kluwer, Lippincott Williams & Wilkins.

[15] "Information on Electrocardiogram", ECGpedia, http://en.ecgpedia.org/wiki/Main_Page

[16] Bioelectromagnetism "Basis of ECG Diagnosis". http://www.bem.fi/book/19/19.htm

[17] EKG Academy which provides information on the abnormalities of Electrocardiogram. http://ekgacademy.azurewebsites.net/learn-ekg-intro.asp

[18] Pericarditis abnormality details : http://co.grand.co.us/DocumentCenter/Home/View/629

[19] Pubmed Central is a joint literature of biological and life sciences at US National Library of Medicine and National Institutes of Health. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3627796/

[20] EKG Quick Reference Guide; http://www.practicalclinicalskills.com/ekg-reference-guide-details.aspx?lessonID=35

[21] EKG Quick Reference Guide; http://www.practicalclinicalskills.com/ekg-reference-guide-details.aspx?lessonID=9

[22] Security Mechanisms in Network Protocols. Intelligent Systems, Modelling and Simulation (ISMS), 2010 International Conference on, Pages : 427 - 430.

[23] S. Kumar, “PING Attack – How Bad Is It?” Computers & Security Journal, Vol.25, July 2006.

[24] Ping Packet Format : https://soumyageorgek.wordpress.com/2010/11/30/receiving-an-echo-reply-in-python/

[25] "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet" by S. Kumar. Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on, Publication Year: 2007 , Page(s) : 25.

[26] The World Wide Web Security ; http://www.w3.org/Security/Faq/wwwsf6.html

[27] Smurf Attack : http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

[28] ARP Request Format : http://ipv6.com/articles/general/Address-Resolution-Protocol.htm

[29] ARP Reply Format : http://www.barrgroup.com/Embedded-Systems/How-To/ARP-RARP

[30] S. Kumar and O. Gomez, “Denial of Service Due to Direct and Indirect ARP Storm Attacks in LAN Environment,” J. Information Security, vol. 1, no. 2, 2010, pp. 88–94.

[31] Transmission Control Protocol header Format. http://condor.depaul.edu/jkristof/technotes/tcp.html

[32] Transmission Control Protocol, DARPA Internet Program Protocol Specification, RFC 793. https://www.ietf.org/rfc/rfc793.txt

[33] Transmission Control Protocol Connection Establishment. http://wiki.mikrotik.com/wiki/Manual:Connection_oriented_communication_(TCP/IP)

[34] TCP / IP Protocol Suite, Attacks and Security tools. http://www.academia.edu/7134687/TCP_IP_Protocol_Suite_Attacks_and_Security_Tools

[35] EKG Senor from Vernier Company[Online]. http://www.vernier.com/products/sensors/ekg-bta/

[36] Logger Lite Software Application to collect EKG signal. http://www.vernier.com/products/software/logger-lite/#download

[37] EKG Abnormalities. http://almostadoctor.co.uk/content/systems/-cardiovascular-system/ecgs/ecg-abnormalities

[38] Summary of EKG Abnormalities. http://almostadoctor.co.uk/content/systems/-cardiovascular-system/ecgs/summary-ecg-abnormalities

[39] Mitigation of TCP-SYN Attacks with Microsoft's Windows XP Service Pack2 (SP2) Software. ICN 2008: 238-242

[40] Internet Server unavailable because of malicious SYN attacks. https://support2.microsoft.com/default.aspx?scid=kb;en-us;142641&sd=tech

[41] Resilience against Distributed Denial of Service Attacks. Security & Privacy, IEEE Volume 10, Issue 2, Pages: 60 - 64.

[42] Analysis of Network Communication Attacks. Research and Development, 2007. SCOReD 2007. 5th Student Conference on, Publication Year: 2007 , Page(s): 1 - 6

[43] The Danger Deepens 2014 Neustar Annual DDoS Attacks and Impact Report. https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

[44] Biometric Human Identification based on EKG.

http://www.physionet.org/pn3/ecgiddb/biometric.shtml

BIOGRAPHICAL SKETCH

Raghava Teja Pingali worked as a Technical Engineer in Electronics Corporation of India Limited, a public sector in India. He obtained his Electronics and Communications Engineering from Sri Chandrasekarendra Saraswathi Viswa Mahavidhyalaya, deemed university in 2008, with a project work on entitled : CCTV (Closed Circuit Television) Security using Microcontrollers. He earned his MS in Electrical Engineering from The University of Texas Pan American in May 2015.

Current Mailing Address :

42-3/1-95, Ayyappa Towers GF3,
Raghunadh Rao Street, Ramakrishna Puram,
Vijayawada, Andhra Pradesh, India - 520003.