A Novel IDS Technique To Detect DDoS and Sniffers in Smart Grid

S.SHITHARTH, DR.D.PRINCE WINSTON
Department of Electrical and Electronics Engineering
Anna University,Chennai
INDIA
shitharth.it@gmail.com,dpwkcet@gmail.com

Abstract: - Smart grid doesn't have a single standard definition to define it. Commonly, Smart Grid is an incorporation of advanced technologies over the normal electrical grid. Smart grid provides some novel features that mainly includes two way communication and automatic self-healing capability. Like the Internet, the Smart Grid consists of many new technologies and equipment that are bind together. These technologies works with the electrical grid to respond digitally accordingly to our quickly changing electric demand. Even though it is stuffed with pros, it suffers a lot due to its fragile data security. Smart grid usually have a centralized control system called SCADA to monitor and maintain all the data sources. Attackers would always tend to sneak through this centralized system through numerous types of attacks. Since SCADA system has no definite protocol, it can be fixed into any kind of protocol that is required by the utility. In this paper, the proposed method provides two techniques one to detect and remove sniffers from the network. Another one is to safeguard the SCADA system from the DDoS attack. Promiscuous mode detection and MD-5 algorithm is used to find the sniffers and by analyzing the TTL values, DDoS attack is been identified and isolated.

Key-Words: -Smart grid, Network Security, Cyber Threats, DDOS ,SCADA ,Sniffer, Promiscuous mode.

1 Introduction

Fundamentally, smart grid is an intelligent grid that connects generation, transmission, distribution and customer end-use technologies with information. It also posses dual way communication. The need to incorporate all the systems that produce and distribute energy with customer usage is one of the very reliable design principles of smart grid. System integration is accomplished using information and communication systems.[1] Smart grid is not forcibly a combination of specific parts. It is a process of using information and communications to integrate all the components that make up each electric system. Rather having a simple electrical infrastructure, smart grid has an intelligent infrastructure. Smart grid has three different perspectives such as regulatory, utility and customer perspective.

2.Significance of Smart Grid

The crucial factor that makes smart grid an ineluctable technology is the two way communication model. This keeps the consumers active and makes them to participate in the grid system.[2] They can choose their tariff with lot of options. Customers would also get a clear idea about their electricity charges and understand about how far their individual behaviour in handling the power resources reflects in their billing. On utility side,smart grid also gives instantaneous information on system operations, power failures and power outages. It also monitor the weather conditions that makes a definite impact in the grid system.

Hence, the need of smart grid is approaching the consumers with full pace. The major driving forces such as aging infrastructure,non-reliable intermittent resources and increase in energy demand and sustainability makes the world to move towards the smart grid. National Institute of Standards and

Technology (NIST) provides a clear reference of the Smart grid overview in Fig 1. And a comparison of normal and electrical grid is made in Table 1.

Table 1. Examination of Smart Grid Over Electrical Grid

Attributes	Existing System (Electrical Grid)	Advanced system (Smart Grid)
Availing Business Model	Centralized operation	Distributed operation
Serving obligation	Provides complete customer pay is provided by utility	Few customer pay is provided by utility
Generation Resources	1.Centralized 2.Mostly Thermal	1.Distributed 2.Mostly renewable
Communication	Single way communication	duplex communication
Metering-Usage Measurement	Accumulated Usage	Periodic Measurement
Customer Role	Passive	Active
Sensors	Less in Number	Fully loaded with sensors
Restrain Capacity	In limited Areas	Pervasive over Smart Grid
Restitution Capability	Manually Restored	Self Healing

3. SCADA:

SCADA (Supervisory Control And Data Acquisition) is a centralized control system in smart grid .It gathers information from all metering system and from RTU's. It remotely controls the operations of the smart grid and also gives alarm during emergency. The SCADA system control can either be manual or be automatic. The SCADA software architecture is shown in fig 2.

4. Attacks in SCADA system :

In SACDA there are so many vulnerabilities due to the complete integrated computerized grid system.[4]**.**Hence there are various types of attacks that march towards the SCADA system. Some of the major types of attacks are Eavesdropping or Replay Attack, SQL injection attacks, Denial of Service Attacks, Identity Spoofing or IP Spoofing, Man in the middle attack, Related Key Attacks and Spyware Threats. [5] Even though there are considerable ways of countermeasures that have been identified, many unsupervised threats and attacks are raising regularly. In this paper, a novel IDS method to detect DDoS attack and Sniffing attack in SCADA is discussed.

5. Promiscuous Mode :

Promiscuous mode [6] is a mode for a wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is intended to receive. This mode is normally used for packet sniffing that takes place on a router or on a computer connected to a hub (instead of a switch) or one being part of a WLAN.

6.Detection and Removal of sniffers by Double Layer Protection:

In this paper, an IDS technique called double layer protection method is proposed for the detection and isolation of sniffers. Initially, we transmit all our data packets through MD-5 encryption technique. A hash value is produced using a hash function in MD-5 mechanism. It is done by using NS-2 tool by implementing the TCL code of MD-5 algorithm.

6.1 MD-5 algorithm for the 1st layer detection.

MD-5 (Message Digest) algorithm is always preferred for preserving the data integrity. This algorithmis used to produce 128 bit hash value.MD-5 algorithm has the following steps :

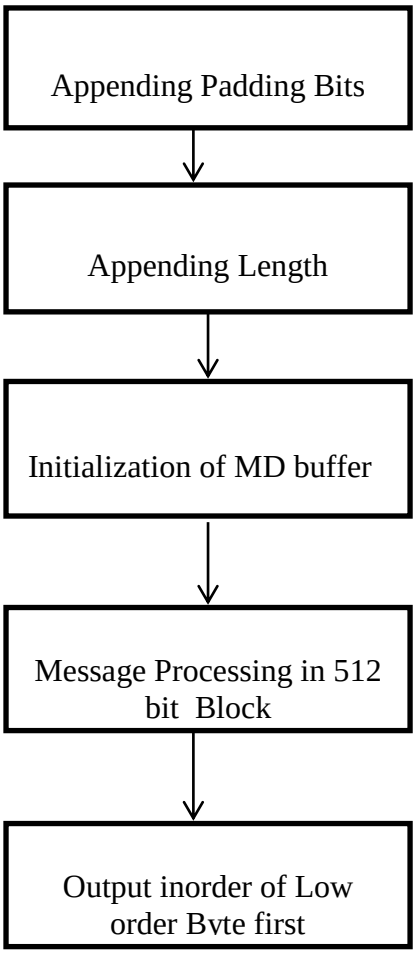

Fig 4.Steps in MD-5 Algorithm

Initially, MD-5 fixes the output length of 128 bits in spite of any variable length input message. Theoriginal message is padded with one bit and as many zeros are added to bring the message into 64 bits.In the diagram A,B,C,D represents the 32 bit word. The MD-5 algorithm uses 512 message block to alter thestate of the constants based on a non linear function F. For each block of input, four round operations areperformed with 16 operations in each round.

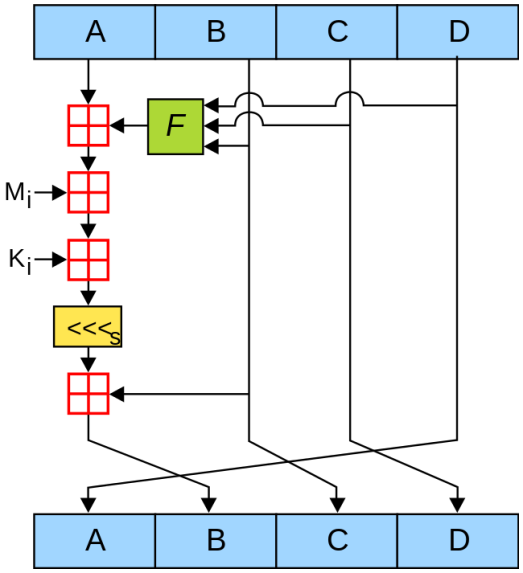

Fig 5 : Sample MD-5 operation

F denotes a Non linear function

M_i denotes a 32-bit block of the message input

K_i denotes a 32-bit constant, different for each operation.

<<< denotes a left bit rotation by s places; s varies for each operation

⊞ denotes addition modulo 2^{32}

The four possible predefined functions of F in MD-5 is :

FF(B,C,D) = BC v not(B) D

FG(B,C,D) = BD v C not(D)

FH(B,C,D) = B xor C xor D

FI(B,C,D) = C xor (B v not (D))

Main loop in MD-5 algorithm is as follows :

fori from 0 to 63

if 0 = i = 15 then

F := (B and C) or ((not B) and D)

g := i

else if 16 = i = 31

F := (D and B) or ((not D) and C)

g := (5×i + 1) mod 16

else if 32 = i = 47

F := B xor C xor D

g := (3×i + 5) mod 16

else if 48 = i = 63

F := C xor (B or (not D))

g := (7×i) mod 16

dTemp := D

D := C

C := B

B := B + leftrotate((A + F + K[i] + M[g]), s[i])

A :=dTemp

end for

The result of MD-5 algorithm in NS-2 is shown in the fig.6. Even though the messages are encrypted with a secured hash key, they can be cracked by using advanced techniques. Intruder may use wireless network hacking tools such as Aircrack, Airsnort and Netstumbler to crack WPA access. Hence until unless the system identifies the source system of the sniffing packets, it is quite tedious to safeguard the integrity of the data. Hence one more layer of security called PMD(Promiscuous Mode Detection) is introduced to find the source of the intruder.

6.2 Detection of sniffer using PMD technique

In this approach, the malicious system is identified by sending fake ARP packets to all sources that send data packets to the supervisory system. Since the ARP packets is present in all IPV4 based system, we prefer to send these packets. The ARP packets will find out the system that has promiscuous mode in activation which is probably a sniffer. [7,8]

In detail, every system has a NIC(Network Interface Card) to receive the incoming packets. All sniffers has an intention to receive all the incoming packets to gain information from the victim system. Hence they would activate promiscuous mode in their NIC. After the activation of PMD mode, NIC would not check the MAC address of the incoming packets and it simply forwards all the packets to the system kernel. We use Address resolution packets to query MAC address from the ip address.[9] System kernel will response to all packets it receive and mistakenly it may also respond to the packets that are not belong to its machine address. By using this mechanism, we can send duplicate ARP packets to all nodes present in our network. If the NIC has not enabled its promiscuous mode, then it rejects[10] the ARP packets that doesn't belong to its machine address. But if it accepts the packet, then it is confirmed that the system is running sniffers. As soon as the malicious system is identified, it must be isolated.

6.3 Detecting DDoS attack by TTL analysis technique:

Before the detection of the sniffers by MD-5 algorithm and PMD activation, we have to analyze and stop the fake incoming packets that is responsible for DDoS attack [11]. The challenge is to find and differentiate the nature of the incoming packet whether it is a genuine

request or not. Most of the DDoS attacks happen outside the network.[12] Hence a finite method of identifying the fake incoming packets that comes from outside the network is to be identified. Such a method is TTL analysis technique.ie; Analyzing the TTL(Time To Live) value of the incoming packets and there by differentiating the packets by its normal and abnormal TTL value. Hence the packets that are from outside the network may have crossed more hops than the packets inside the network. Therefore, the malicious packets are detected by its abnormal TTL value and it is rejected. (packets inside the same network has no change in its TTL value). Table 2.explains the variation of TTL value with respect to OS and its protocol.

Table 2. Different TTL values for different OS and their protocols

OS	**Version**	**Protocol**	**TTL value**
CISCO	-	ICMP	254
LINUX	2.0 x kernel	ICMP	64
LINUX	2.4 x kernel	ICMP	255
LINUX	REDHAT 9	ICMP,TCP	64
SOLARIS	2.5.1,2.6,2.7,2.8	ICMP	255
WINDOWS	2000,XP,VISTA,7,8	ICMP/TCP/UDP	128
MAC	10.5.6	ICMP/TCP/UDP	64

Normal TTL value: if 30<TTL<= 64 : 98 <TTL<= 128 : 225 <TTL<= 255

Abnormal TTL value: if 1<TTL<= 30 : 64 <TTL<= 98 : 128 <TTL<= 225

7.Experimental setup and result analysis :

As it is discussed earlier, to detect sniffers the supervisory system send ARP packets to all the system present in the network. The tool used for the deployment of this technique is Network simulation-2.As soon as the malicious packet sender is identified, he is excluded from the network. [13,14]. After the detection of sniffers, we also cross check the integrity of the data through encryption technique.ie; Thereby the confidentiality of our data is been preserved. CISCO packet tracer is the tool used to setup packet filtering for the detection of DDoS attack. In this tool, the packet tracer uses statements such as ACCPET and DENY to create a access list for filtering the packets. Such a s simulation setup is shown in fig 7.

7.1 Access list for ip packets based on TTL filtering:

Here Cisco Packet Tracer is used for the simulation. By pinging the nodes of the network, the TTL value decrementation is tested. There should be some filtering mechanism for TTL values created by the access list in Cisco packet tracer. The following access list contain TOS level 3 to filter IP packets with the exact TTL values of 30 and 40 (variable) and also with the TTL value higher than 160. IP packets with TTL ≠ 1are identified and information about such packets that doesn't [15] satisfy the filter is immediately passed to the console. Then the console will reject or block those malicious packets.

ip access-list extended incoming filter
denyip any anytos 3 TTL eq 30 40
denyip any any TTL gt 154 fragments
permitip any any precedence flash TTLreqlog
interfaceethernet 0
ip access-group incoming filter in
Number of Routers :3
Number of Servers : 2
Number of Clients : 6
Number of Switch : 2

7.2 Filtering Packets Based on TTL Value

Following steps are to be followed to execute our filtering strategy. Add the permit and deny statements until unless, it fulfils our filtering criteria.

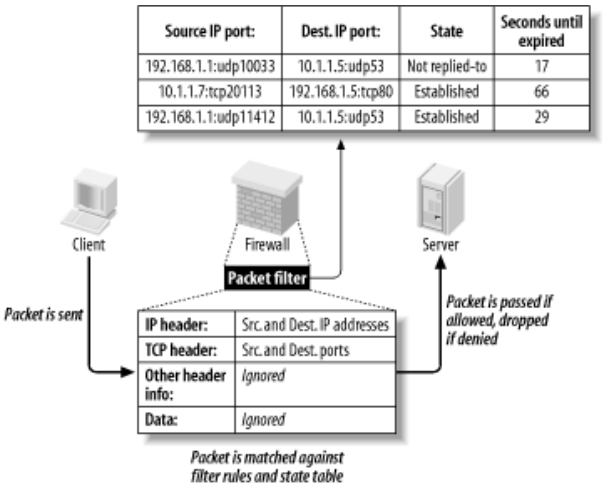

Fig. 8. Structure showing how the packet filter works

7.3 Summary Steps:

1. enable
2. configure terminal
3. ip access-list extended *access-list-name*
4. [*sequence-number*] permit *protocol source source-wildcard*

destination destination-wildcard [option *option-name*] [precedence *precedence*] [tos *tos*]

[TTL *operator value*] [log] [time-range *time-range-name*] [fragments]

5. Continue to add permit or deny statements to achieve the filtering you want.
6. exit
7. interface *type number*
8. ip access-group *access-list-name* {in | out}

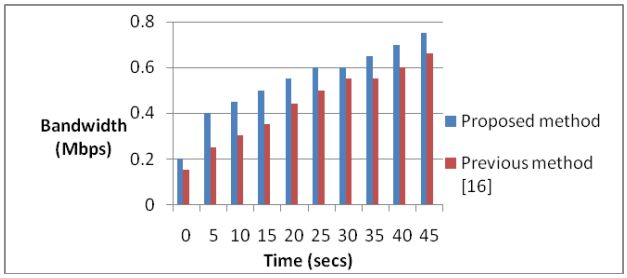

Fig .9. Comparison of Bandwidth in previous and proposed method

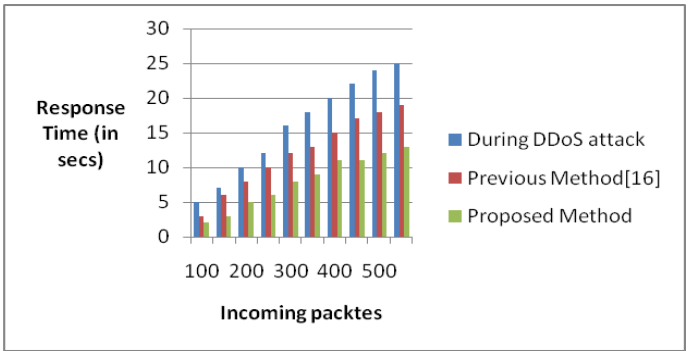

Fig. 10. Comparison of Response time with incoming packets

8. Conclusion:

Overall, this paper deals with detection and isolation of DDOS attack and packet sniffing. The DDOS attack is identified by fixing the TTL values with certain threshold and there by analyzing the abnormal value packets as malicious. Sniffing is detected by MD-5 and PMD. MD-5 safeguard the data integrity by encryption and decryption technique. PMD helps to find the source of the sniffing packets. NS-2 and CISCO packet tracer are tools used for simulation respectively.

One thing to be noted is, TTL technique is used to detect the attacks from outside the network and PMD is used to detect the sniffers inside the network. It is a tedious process to incorporate two different mechanisms in a single SCADA system, since there is a big time delay. Therefore, a unique hybrid technique would be framed in future so that it must be able to detect attacks in both scenario with

9. References:

[1] NETL, The NETL Modern Grid Initiative Powering our 21st-Century Economy: MODERNGRID BENEFITS. Department of Energy, 2007.

[2] M. J. Assante, \Infrastructure Protection in the Ancient World," Hawaii International Conference on System Sciences, vol. 0, pp. 1-10, 2009

[3] NIST, \Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture,and High-Level Requirements, NISTIR 7628," 2010. [Online]. Available: http://csrc.nist.gov/publications/.

[4] CNN, \Staged cyber attack reveals vulnerability in power grid,"2007.[Online] Available: http://www.youtube.com/watch?v=fJyWngDco

[5] P. McDaniel and S. McLaughlin, \Security and Privacy Challenges in the Smart Grid," IEEE Security Privacy Magazine, vol. 7, no. 3, pp. 75-77, 2009.:

[6] Daiji Sanai, "Detection of Promiscuous mode using ARP packets,"2001.[Online].Available :http://www.securityfriday.com.

[7] NIST, \Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid," 2010.

[8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, \Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," in 2010 First IEEE International Conference on Smart GridCommunications, 2010, pp. 220-225.

[9] Fengun Li, Bo Luo, Peng Liu, "Secure and privacy-preserving information aggregation for Smart Grids." in Apr 13, 2011 International Journal of Security and networks, 2010, pp. ISSN 1747-8413 (Online)

[10] Fengun Li, Lawerence KS, Bo Luo, "Preserving Integrity for Smart Grid data aggregation." in Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on Smart Grid Communications, pp.366 - 371 .

[11] Cisco Secure Policy Manager 2.2, 2000. http://www.cisco.com/warp/public/cc/pd/sqsw/sqppmn/.

[12] A. Mayer, A. Wool, and E. Ziskind. Fang: A Firewall Analysis Engine. IEEE Symp. on Security and Privacy, Oakland, CA 2000

[13] Internet Security Systems Internet Scanner,2000.http://documents.iss.net/literature/InternetScanner/is_ps.pdf.

[14] FadiAloula, A. R. Al-Alia , Rami Al-Dalkya, Mamoun Al-Mardinia, Wassim El-Hajjb "Smart Grid Security : Threats, Vulnerabilities and Solution." in International Journal of Smart Grid and Clean Energy, Sept 2012. .

[15] Cisco, Online Available "http://www. cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/8014-acl-wp.html".

[16] S.A Arunmozhi ,Y.Venkataramani "DDoS Attack and Defence Scheme in Wireless Ad Hoc Networks." in International journal of Network Security and Communications(IJNSA) Vol3, No 3, May 2011.

APPENDIX

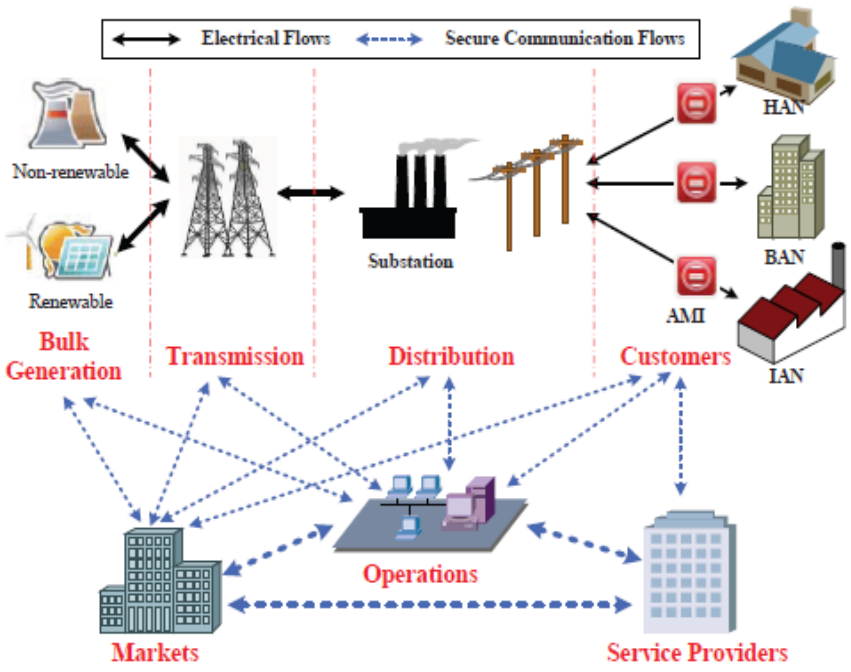

Fig. 1. NIST reference model for Smart Grid [3]

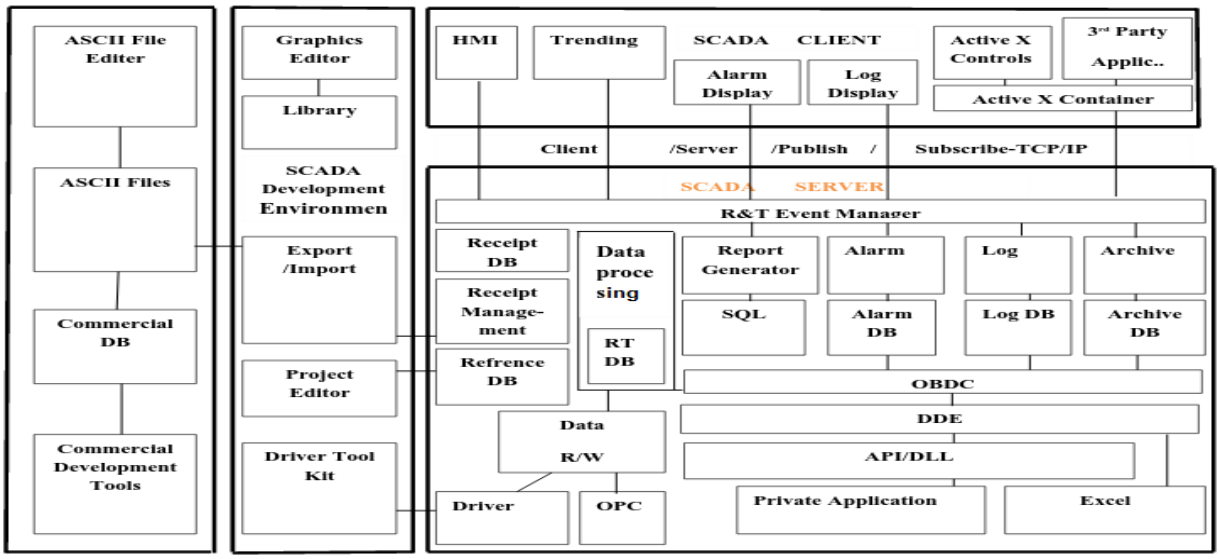

Fig. 2. SCADA Software Architecture

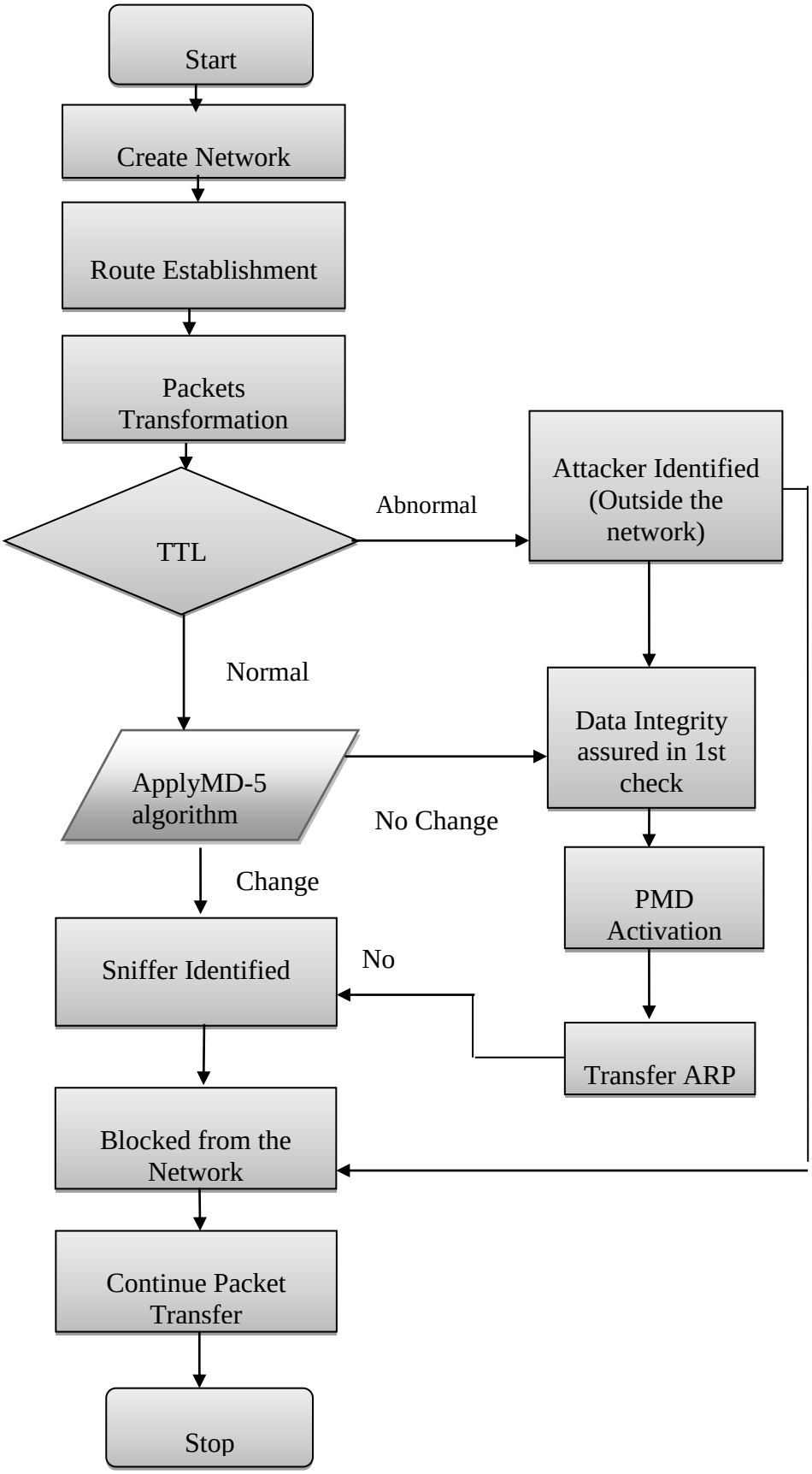

Fig 3.Flowchart for Proposed Work

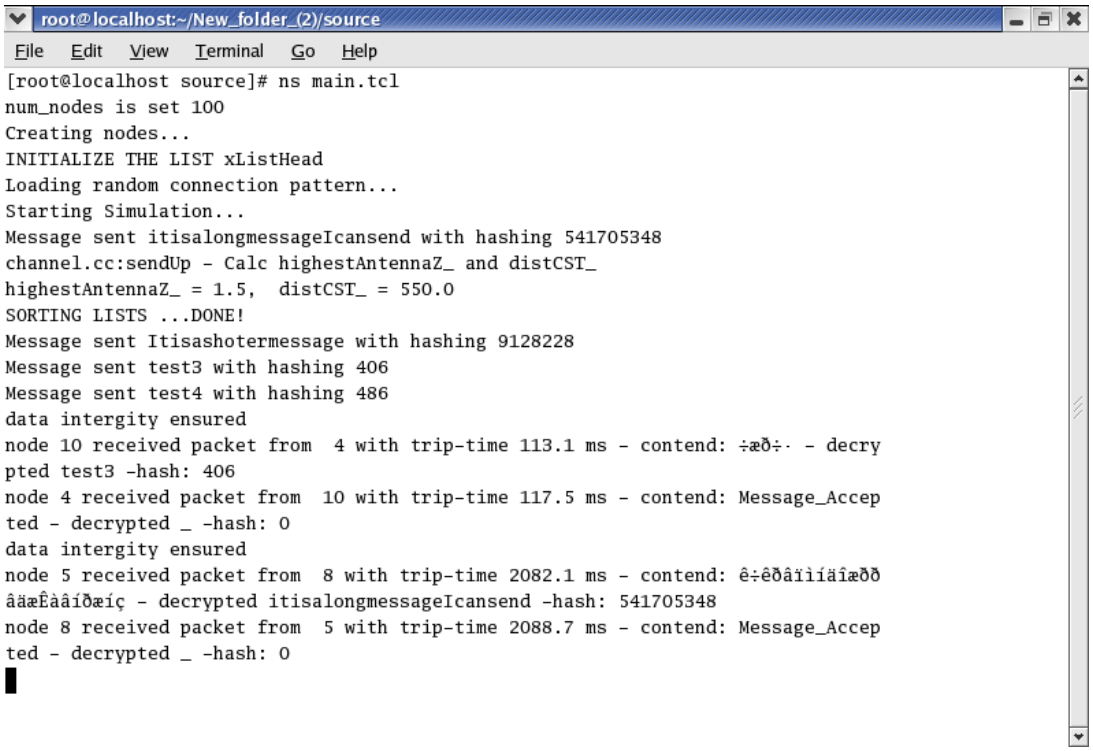

Fig 6. Screen shot of 1st layer protection of data by encryption and decryption

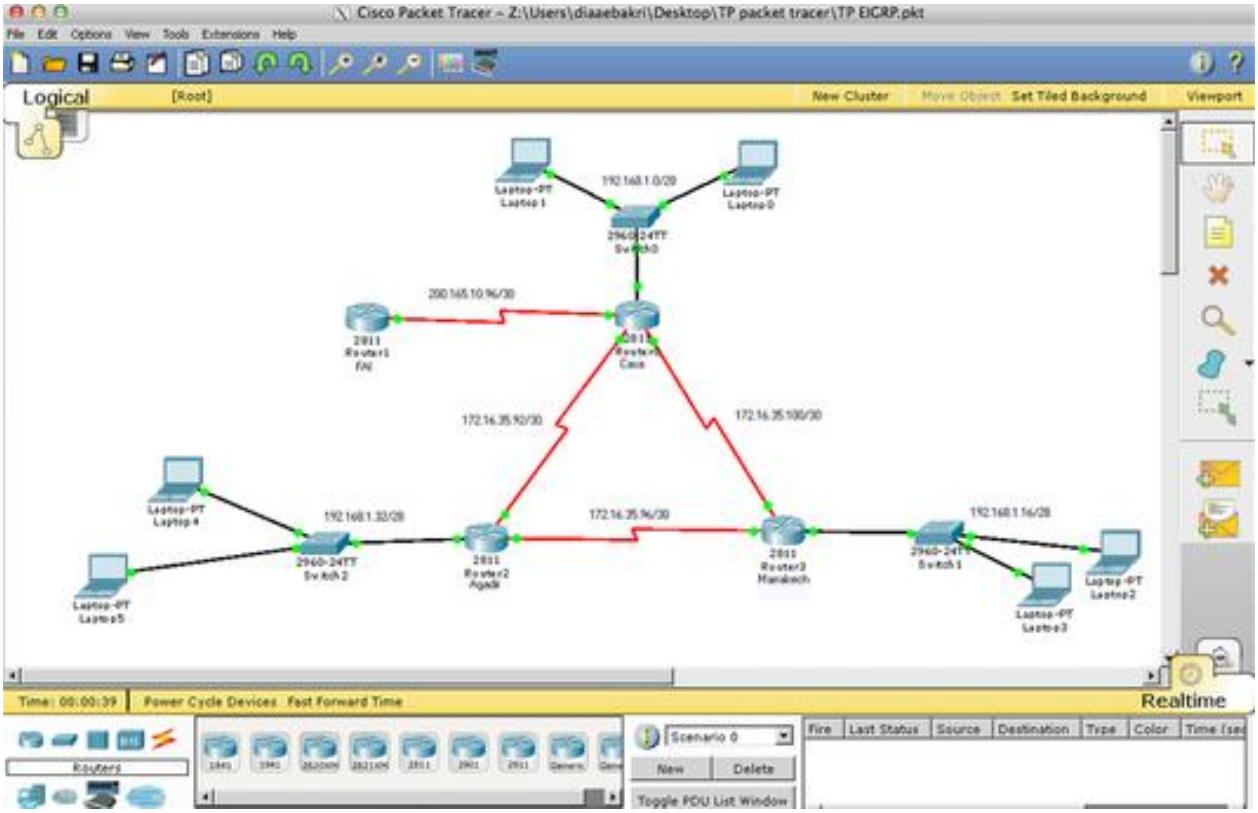

Fig. 7. Screen shot of Packet Tracer setup and analysis