A Novel IDS Technique to detect DDoS and Sniffers in Smart Grid

S.Shitharth
Kamaraj College of Engineering and Technology
Virudhunagar,India

Dr.D.Prince Winston
Kamaraj College of Engineering and Technology
Virudhunagar,India

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 analysing the TTL values, DDoS attack is been identified and isolated. The proposed technique is also compared with a real time his electronic document is a “live” template. The various components of your paper [title, text, heads, etc.] are already defined on the style sheet, as illustrated by the portions given in this document. Do not use special characters, symbols, or math in your title or abstract. The authors must follow the instructions given in the document for the papers to be published. You can use this document as both an instruction set and as a template into which you can type your own text.

Keywords: *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 possess 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. On utility side, smart grid also gives instantaneous information on system operations, power failures and power outages.

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 behavior in handling the power resources reflects in their billing. 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.

3. SCADA SYSTEM

3.1 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.

3.2 Attacks in SCADA system

In SCADA 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 many 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

Table 1. Table captions should be placed above the table

Graphics	Top	In-between	Bottom
Tables	End	Last	First
Figures	Good	Similar	Very well

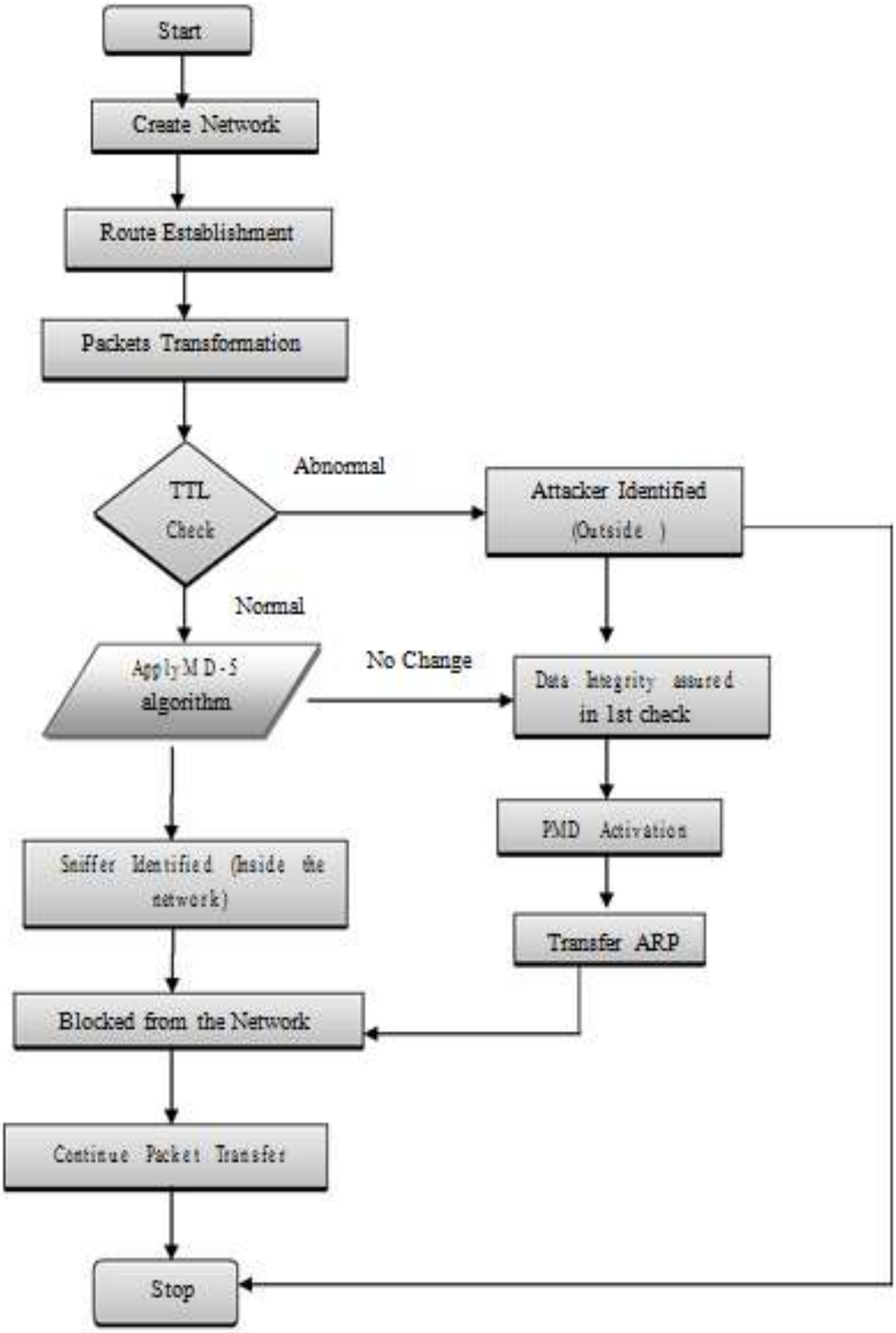


Fig. 1. Flowchart for Proposed Work

3.3 Promiscuous Mode

Promiscuous Mode [6] is a mode for a wireless network controller (WNIC) that passes a controller to pass all traffic it receives to the CPU rather than the frames that the controller is intended to receive. This mode is normally used for packet sniffing This mode is normally used for packet sniffing that takes place on a router or on a computer connected to a hub or being a part of WLAN. It allows a network device. It allows a network device to intercept and read the packets in the entry point itself.

4. 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. In fig 1.the flowchart explains about the proposed work. It explains the flow of detection of intruders in both inside and outside the network.

4.1 Using MD-5 algorithm in the First layer detection

MD-5 (Message Digest) algorithm is always preferred for preserving the data integrity. Initially, MD -5 fixes the output length of 128 bits in spite of any variable length input message. The original 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. This algorithm is used to produce 128 bit hash value.MD-5 algorithm has the following steps :

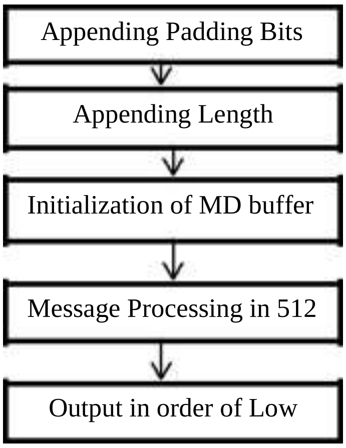


Fig. 2. Steps in MD-5 Algorithm

The MD -5 algorithm uses 512 message block to alter the state of the constants based on a non linear function F. For each block of input, four round operations are performed with 16 operations in each round.

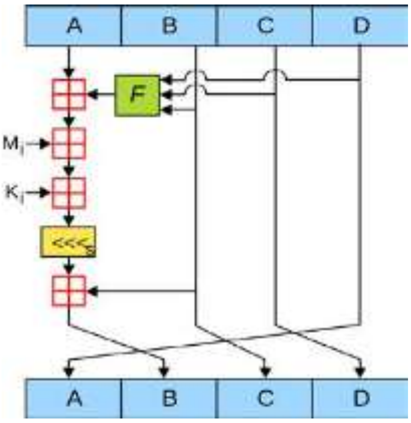


Fig. 3. Sample MD-5 operation

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

$\boxplus$ 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 : For i 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 + left rotate((A + F + K[i] +
 M[g]), s[i]) A :=dTemp
 end for
```

The steps and the sample MD-5 algorithm is shown in Fig. 2 and Fig. 3 respectively. 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.

4.2 Detection of sniffer using PMD technique in second layer detection

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.

5. 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 are 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. The comparative values of normal and abnormal TTL is given as :

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

Table 1. 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

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. To preserve privacy, TTL analysis is one of the efficient method but not the only method since equally enriched methods have also been proposed[15]. But particularly in this tool, the packet tracer uses statements such as ACCPET and DENY to create a access list for filtering the packets .Such as simulation setup is shown in fig.7

5.1 Access list for ip packets based on TTL filtering

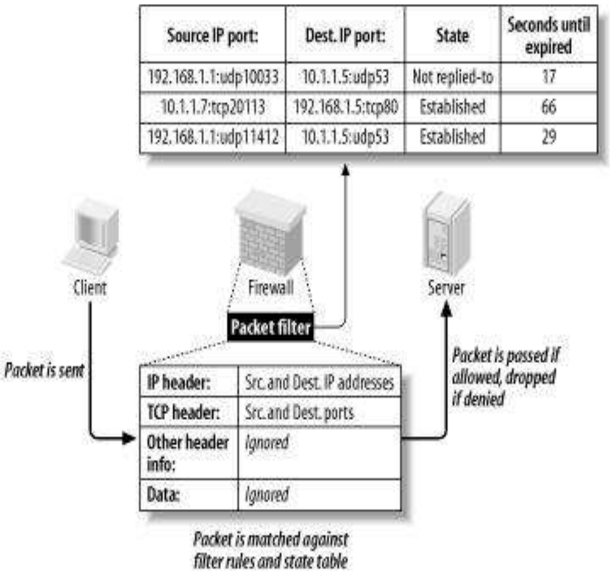
Here Cisco Packet Tracer is used for the simulation. By pinging the nodes of the network, the TTL value decrementation is tested. There should be some filtering mechanism for TTL values created by the access list in Cisco packet tracer. The following access list contain TOS level 3 to filter IP packets 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 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

5.2 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 fulfills our filtering criteria.



Source IP port:	Dest. IP port:	State	Seconds until expired
192.168.1.1:udp10033	10.1.1.5:udp53	Not replied-to	17
10.1.1.7:tcp20113	192.168.1.5:tcp80	Established	66
192.168.1.1:udp11412	10.1.1.5:udp53	Established	29

IP header:	Src. and Dest. IP addresses
TCP header:	Src. and Dest. ports
Other header info:	Ignored
Data:	Ignored

Client
Firewall
Server
Packet filter
Packet is sent
Packet is passed if allowed, dropped if denied
Packet is matched against filter rules and state table

Fig. 4. Structure showing how the packet filter works

5.3 Summary Steps

1. enable
2. configure terminal
3. ip access-*List extended* access-Ordering by name basis ip access is being defined

list-name - To filter the desired TTL value the access list has to be extended.

4. [*sequence-number*] permit *protocol source-wildcard destination destination-wildcard* [option *option-name*] [precedence *precedence*] [tos *tos*] [TTL *operator value*] [log] [time-range *time-range-name*] [fragments] - Sets conditions to allow a packet to pass a named IP access list.To clear the IP accessed named list, a set of conditions si to framed for the incoming packets. At least one permit statement is mandatory for an access list.
5. Continue to add permit or deny statements to achieve the filtering you want.
6. exit- Exits any configuration mod
7. interface *type number*- Gets into interface config mode. Prior to that interface type is configured.
8. ip access-group *access-list-name* {in | out}

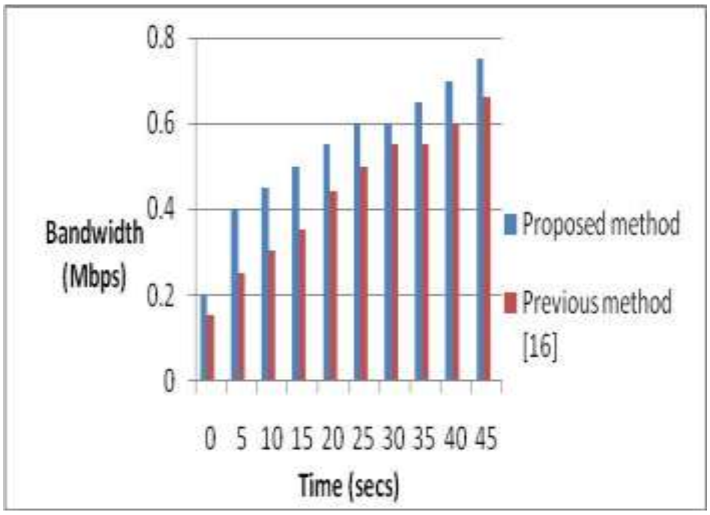


Fig. 5. Comparison of Bandwidth in previous and proposed method

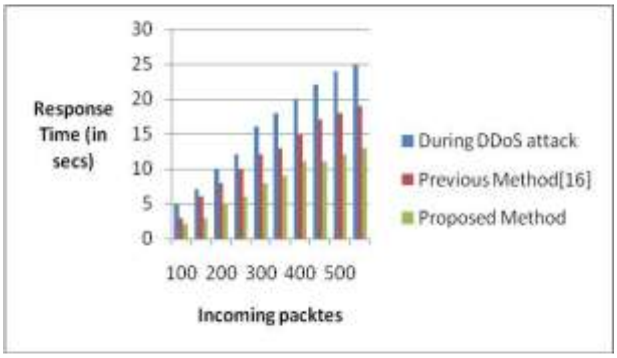
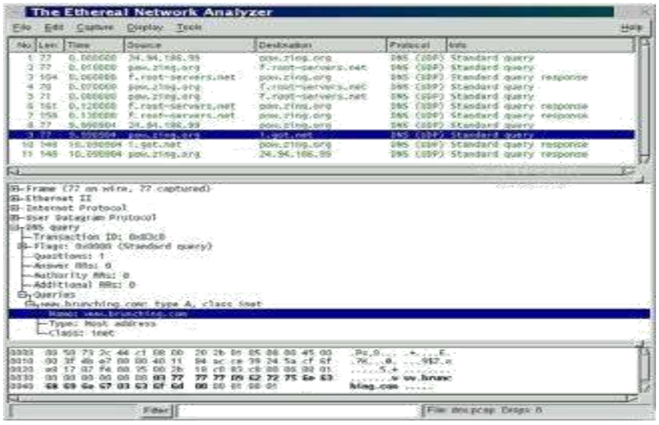


Fig. 6. Comparison of Response time with incoming packets

6. Comparison of proposed technique with Ethereal tool

This proposed technique is also compared with the existing IDS tool to show a better bandwidth. This proposed technique detect sniffers by using very less bandwidth . Unlike the other systems, SCADA systems would be more conscious on the bandwidth they consume. Remote SCADA is polled by a host system in different locations but one at a time i.e. Only one remote station answers at a time. Data traffic is either a poll from the host to the remote or a response to a poll from the remote RTU to the host computer. Therefore either of the communication should not lag even a minute delay because of high bandwidth consumption.

Even though tools like wire shark may show a better performance in throughput than the proposed method, they lag in bandwidth. They consume more bandwidth for the detection of DDoS and Sniffers. In Fig. 7, sample traffic is analyzed and in Fig.8 the bandwidth of ethereal is recorded. Then in Fig. 9, the IDS tool(ethereal) bandwidth is compared with the proposed work bandwidth. TTL analysis and PMD technique combinedly use less bandwidth. The resultant graph clearly shows the efficient use of bandwidth that obviously suits the SCADA security system.


The Ethereal Network Analyzer
File Edit Capture Display Tools Help
Filter

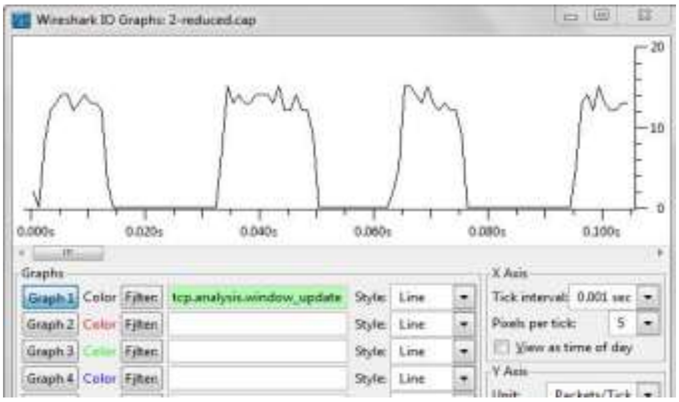
```
No Len Time      Source               Destination          Protocol  Info
 1  77 0.000000  24.94.186.99         pow.zing.org         DNS (UDP) Standard query
 2  77 0.010000  pow.zing.org         f.root-servers.net   DNS (UDP) Standard query
 3 104 0.060000  f.root-servers.net   pow.zing.org         DNS (UDP) Standard query response
 4  70 0.070000  pow.zing.org         f.root-servers.net   DNS (UDP) Standard query
 5  71 0.080000  pow.zing.org         f.root-servers.net   DNS (UDP) Standard query
 6 161 0.120000  f.root-servers.net   pow.zing.org         DNS (UDP) Standard query response
 7 158 0.130000  f.root-servers.net   pow.zing.org         DNS (UDP) Standard query response
 8  77 5.990904  24.94.186.99         pow.zing.org         DNS (UDP) Standard query
 9  77 5.990904  pow.zing.org         i.gst.net            DNS (UDP) Standard query
10 148 10.090904 i.gst.net            pow.zing.org         DNS (UDP) Standard query response
11 148 10.090904 pow.zing.org         24.94.186.99         DNS (UDP) Standard query response

⊞-Frame (77 on wire, 77 captured)
⊞-Ethernet II
⊞-Internet Protocol
⊞-User Datagram Protocol
⊟-DNS query
  ├─Transaction ID: 0x03c8
  ⊞-Flags: 0x0000 (Standard query)
  ├─Questions: 1
  ├─Answer RRs: 0
  ├─Authority RRs: 0
  ├─Additional RRs: 0
  ⊟-Queries
    ⊟-www.brunching.com: type A, class inet
       ├─Name: www.brunching.com
       ├─Type: Host address
       └─Class: inet

0000  00 50 73 2c 44 c1 08 00  20 2b 0e 85 08 00 45 00   .Ps,D... .+....E.
0010  00 3f 4b e7 00 00 40 11  94 ac ce 39 24 5a cf 6f   .?K...@. ...9$Z.o
0020  a0 17 07 f6 00 35 00 2b  18 c0 03 c8 00 00 00 01   .....5.+ ........
0030  00 00 00 00 00 00 03 77  77 77 09 62 72 75 6e 63   .......w ww.brunc
0040  68 69 6e 67 03 63 6f 6d  00 00 01 00 01            hing.com .....

File: dns.pcap Drops: 0
```

Fig. 7. Traffic analyzer in Ethereal network analyzer



Graph 1 Filter: tcp.analysis.window_update Style: Line
Graph 2 Style: Line
Graph 3 Style: Line
Graph 4 Style: Line
Tick interval: 0.001 sec
Pixels per tick: 5
☐ View as time of day
Unit: Packets/Tick

Fig. 8. Bandwidth analyzer of ethereal with traffic by analyzing tcp and udp data.

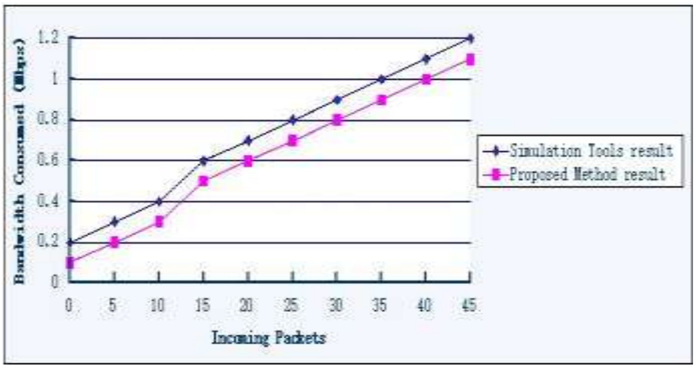


Fig. 9. Bandwidth comparison of proposed method and the IDS tool.

7. 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 network analyzer are the tools used for result comparison.

Important thing to be perceived is that the TTL technique used here is to detect only 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 scenarios with high efficiency.

8. 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 2009 on System Sciences, vol. 0, pp. 1-10.

[3] NIST,\Guidelines for Smart Grid Cyber Security Smart Grid Cyber Security Strategy '10 , Architecture and High-Level Requirement Vol 1, NISTIR 7628,".

[4] CNN, \Staged cyber attack reveals vulnerability power grid,"2007 in. [Online] Available: http://www.youtube.com/watch?v=fJyWngDco3g

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

[6] Daiji Sanai, "Detection of Promiscuous mode using ARP packets," 2001. [Online] Available: http://www.securefriday.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 Grid Communications, 2010, pp. 220-225.

[9] S.Shitharth, D.Prince Winston, “An Appraisal on Security Challenges and Countermeasures in Smart Grid.” International Journal of Applied Engineering Research, Vol.10, No.20, 2015, pp. 16591-16597.

[10] Fengun Li, Lawerence KS, Bo Luo,"Preserving Integrity for Smart Grid data aggregation." in Smart Grid Comm, 2012 .

[11] David K. Yau, John C. S. Lui, and Feng Liang,“Defending Against Distributed Denial of Service Attacks with Max-min Fair Server-centric Router Throttles”, Quality of Service, 2002 Tenth IEEE International Workshop, pp. 35-44.

[12] David Mankins, Rajesh Krishnan, Ceilyn Boyd, John Zao, and Michael Frentz, “Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing”, ComputerSecurity Applications Conference, 2001.ACSAC Proc17th Annual, pp.411-421.

[13] Joao B. D. Cabrera, Lundy Lewis, Xinzhou Qin, Wenke Lee, Ravi K. Prasanth, B. Ravichandran, and Ramon K. Mehra, “Proactive Detection of Distributed Denial of Service Attacks Using MIB Traffic Variables – A Feasibility Study”, Integrated Network Management Proceedings 2001, pp. 609-622.

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

[15] S.Shitharth, D.Prince Winston, “A New Probablistic Relavancy Classification (PRC) based Intrusion Detection System(IDS) for SCADA network.” Journal of Electrical Engineering, Vol.16, No.3, 2016, pp. 278-288.

[16] S.A Arunmozhi ,Y.Venkataramani, "DDoS Attack and Defence Scheme in Wireless Ad Hoc Networks." in International journal of Network Security and Communications Vol 3, No 3, May 2011, pp. 182-187.

[17] Sakthivel, K. and Prince Winston, D. “Application of Optimization Techniques in Smart Grids” International Journal of Science, Engineering and Technology Research (IJSETR), Vol.3, 2014, pp. 32-36.

[18] S.Shitharth, D.Prince Winston, “A Comparative Analysis between Two Countermeasure Techniques to Detect DDoS with Sniffers in a SCADA Network” Procedia Technology, Vol.21, 2015, pp.179-186.

[19] Praveen, S. and Prince Winston, D. “Protection and Performance Improvement of a Photovoltaic Power System. Advances in Electronic and Electric Engineering” Vol.4, 2014, pp.41-48.