NIDS: Network intrusion detection system with Deceptive Virtual Hosts for Industrial Control Networks

R Nirmala Devi Rajesh[1], C Selvalakshmi[2]
[1] PG Student, [2]Assistant Professor, Department of Computer Science and Engineering,
PTR College of Engineering and Technology, Tamilnadu, (India)

ABSTRACT

Industrial control systems (ICS) are a distributed network most commonly used for operating the networks which are tightly coupled with physical process. In this factor a challenging issue is handling the security issues on a large distributed network. To handle this system various tools were evolved, in which effective tool is honeypot which is used for monitoring and focusing the activities of intruders according to the real world consequences. Honeypot tracks the unauthorized users accessing the information on a control system. These honeypots are self configured but it still facing the drawbacks like failure in detecting and preventing in a virtual network environment at the same time it is not accurate in detecting the attackers. In this paper we proposed a modern methodology known as NICE that is Network Intrusion detection and Countermeasure selection in virtual network systems. This proposed system uses the improvised methodology in reconfiguring the virtual network to monitor the intruders in the system. It is a multiphase distributed network intrusion detection that manages effectively the cloud traffic without interrupting users' applications and cloud services. This system is more prominent in gathering the network entity information's when considered to the traditional network security tools. The proposed system implementation results in successful consequence by achieving automatic virtual network creation by means of virtual host and also detecting malicious behaviors in a network system effectively.

Index term: Network system, cloud server, intrusion detection and network security

INTRODUCTION

Networking is the major technology is implemented for various processes like information sharing and sharing of peripheral devices by means of internet. It uses packets for sharing the information from source to the destination with the help of protocols. Network security undergoes various authentication credentials to assure that they are the real member to take part in the communications. In which privacy and network security is the major problem that makes the global utilization in an unfair manner. Because that information must be preserved from the unauthorized users in order to achieve the privacy. By this way industrial control system (ICS) is a distributed networking system which was used by many of the prominent industries like chemical, electrical, water, oil, gas and data. It is generally used for data acquisition (SCADA) systems and in other systems. It commonly receives data from the remote station such as field devices in controlling the major activities like opening, closing of valves and breakers. The thing is noted among these are public safety, network security, and industrial or economical consequences. Here also lack of authentication is one of the remaining challenges for ICS security. For this infrastructure is very important but only few systems are supporting the critical infrastructure like air-gapped. Another challenge in ICS to be discussed is procurement, installation and maintenance because the controlling equipments using which to be installed, configured and run by plant engineers on site in an effective manner. To overcome the security threats in the modern world an advanced security system should develop to overcome the critical cyber-physical system drawbacks. It was connected by means of Ethernet network and for protecting the control system the network monitoring system is the major one in providing a fine solution from network intruders.

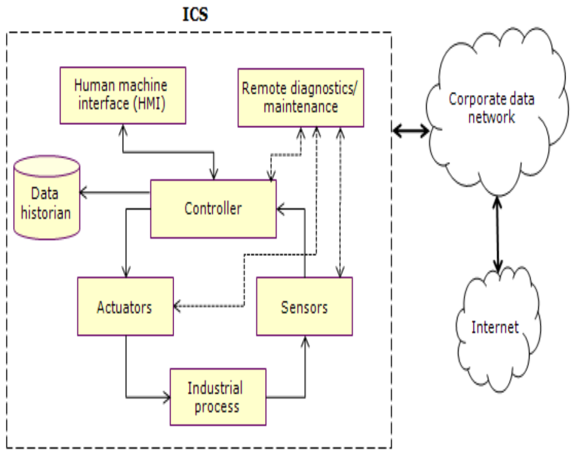


Fig 1: A common ICS System

The fig 1 shows the industrial control system and the overall process are monitored by the network monitor system through internet. In this mechanism the configuring devices are huge in number and also high in deployment. For example consider a AMI system advanced metering infrastructure in which moreover 1500 wireless sensors are to be connected to a multiple wireless access point (WAP). In this case a monitoring system should be effective in detecting the accuracy and precision rates. In this mechanism NEI (network identity information) plays a vital role in monitoring the traffics in the network, by means of gathering the information from source, destination, and port activity. That information's are useful in creating a representative virtual network.

RELATED WORKS

For an effective control system various researchers were discussed about complex control system and their working strategies in which a compromised control system was discussed about the security, public safety, and industrial consequences [1] [2]. In which [3] [4] were discussed about the critical cyber physical system and their security threats globally. On discussing about network monitoring system a protective control system is analyzed in [5] [6]. A deceptive system for monitoring solution with enhanced approach in accuracy and precision rates were considered in [7] [8]. According to John ousterhout in a faithful honeypot automation construction there are four common factors are involved in order to turn the deployment of enemy into a friend [9]. In a network system it is difficult list the definitive attributes of a network host which are required to grab the attacker attentions. When the propose of honeypot raise there are primary aspects in gathering the information one is active scanning and another term is passive scanning. Most of the previous work were discussed about the passive scanning in which was implemented with P0f and occasionally Snort [10] [11]. A suitable tool which is commonly used for gathering passive information is Ettercap[12]. In which snort resembles the rule based introduction system but only limited amount of information can gleaned by passive scanning as the tool was restricted in collecting the information from captured stream [12]. On dealing these situations active scanning is more powerful and successful. In which Nmap is one of the active scanning tool that proved successful in interrogating hosts on a network [13]. But active scanning is also suffers from the problem of service interruption on hosts especially in most of the control systems. That pings on older system which may leads to physical damages [14]. On this Lance Spitzner has introduced a dynamic honeypot in 2004 (DHP) that is a concept of automatic configuring based on the gleaned information from the network traffic. The DHP requires two factors such as network information gathering and deploying honeypot configuration. More about DHP solution were discussed in [15] [16]. On discussed about the previous works supervisory control and data acquisition (SCADA) Honeynet project by Matthew Franz and Venkat Pothamsetty of the Cisco Critical Infrastructure Assurance Group (CIAG) were remarkable one in simulating a set of services for a PLC [17]. According to digital bond Inc is a research group for consulting the control systems which utilizes two machines one as monitoring tool such as snort and another one is for simulating the PLC [18]. In the literature review the tools which are used for providing network host identification are P0f [19], Tshark [20], Ettercap, Snort [21], Tcpdump [22], SinFP [23] and Ntop [24]. But these tools are not effective in accurate execution on the test sensor systems. In the Anomaly behavior (AB) its implementation and works are discussed by the author in [25] which configure the virtual honeypot IP addresses and send alerts based on any activity. But this approach was not effective according to the real time situations.

EXISTING SYSTEM

In order to overcome the security issues an automatic configuration is may be a solution in monitoring the control system effectively and which can be achieved by implementation of Honeyd. It is totally contrast to the other honeypot creations known as honeynet that is nothing but a network of hosts. Before discussing honeyd just look on honeypots as it can be implemented in two ways such as low interaction and high interaction. These Low-interaction virtual honeypots were work collaboratively with other agents in gathering information which are simple to deploy. High-interaction honeypot systems require complex management with wide range of software. By this honeypot with either high or low interaction but it can only detect the attack but it not effective entirely. Honeyd is created by Niels Provos is also a low interaction honeypot that has the ability to connect multiple hosts on a single host which results in minimum hardware consumptions. It quickly realize if any anomalous done by the attacker.

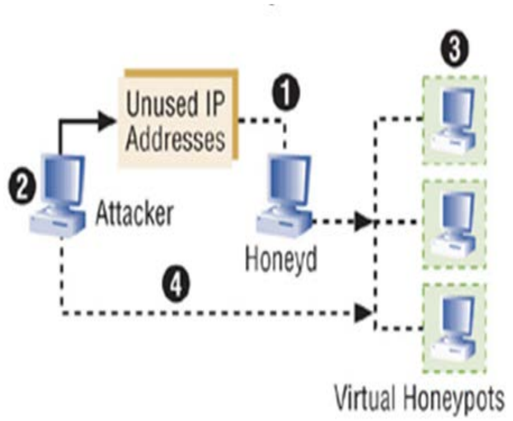


Fig 2: Working of Honeyd

As shown in fig 2 initially honeyd monitors the unused IP space in the network. If an attacker probes the unused IP it is noticed by the honeyd and detects the probe in the network by IP spoofing with the help of creating virtual honeypot for attackers. This mechanism is a concept of fooling the attacker by creating multiple virtual hosts on all unused addresses. But the attacker may thing that he is still interacting with the successful hacking system. Moreover these honeyd can automatically configure the unused IP on the system which can either add or removed by them. A sample honeyd configuration is given below;

```
Create Vh1

Set Vh1 personality “Linux 2.4.xx”

Set Vh1 default tcp action reset

Set Vh1 default udp action reset

Add Vh1 tcp port 23 “/script /router-telnet.pl”

Set Vh1 ethernet “00:00:BC:A1:00:23”

Bind 192.168.1.125 vh1
```

PROPOSED SYSTEM

In this paper we analyze NICE (Network Intrusion detection and Countermeasure selection in virtual network systems) is effectively progress against the attack detection in a network by overcoming the drawbacks faced on honeyd. The mechanism is based on defense-in-depth intrusion detection framework which implies reconfigurable virtual networking by attempting the counters in order to comprise the VM’s as preventing zombie in VM’s. The proposed system creates multi-phase distributed network which effectively suspects the cloud traffic without interrupting users’ applications and cloud services. Without disturbing the entire network it makes progress on improving the resiliency to VM exploitation attack. The major this in this proposed architecture is it reduce the resource consumptions. We had shown in our work that NICE consumes less computational by comparing proxy-based network intrusion detection solutions.

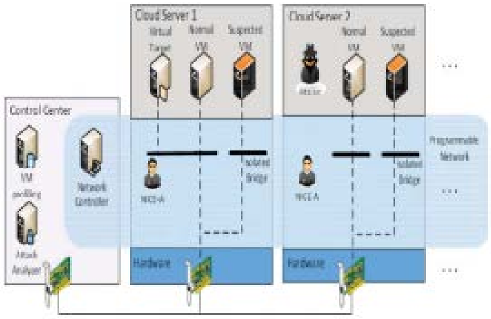


Fig 3: Architecture of NICE

The proposed system is consisting of two algorithms such as Alert Correlation Algorithm and Countermeasure Selection algorithms. The working mechanism of alert correlation algorithm is it receives the alert from the intrusion system by detecting the root cause and minimizing the false alert in order to improve the network performance. It is so predictable in maintaining the accuracy, functionality, and computation power of the system. The countermeasure selection is applied to count the overall attack in the network by applying the formula;

$$Attack\ propability = \frac{Number\ of\ attack\ packets}{Total\ number\ of\ packets}$$

IMPLEMENTATION DESIGN

The above explained proposed system is implemented by means of java with supporting software's to obtain the expected results. The modules are;

- Creation of virtual cloud servers with some VMs
- Deploy a agent (NICE-A) on each cloud server
- Scanning the virtual system vulnerabilities with in a cloud server
- Performing the counter measure actions to protect the cloud server

Initially the cloud server is configured with VM's in this the cloud does not allow to choose the specified hardware required needed for the application. So to meet the consequence we modified the application with available resources instead of customizing the infrastructure. Next we deploy the NICE and captures the suspicious aspects happened in the network. Based on that attack graph is modified by means of countermeasures. This graph plays a vital role in identifying the potential threats, possible attacks, and known vulnerabilities in a cloud system. In this section the network controller, a VM profiling server, and an attack analyzer identifies the normal data packets using OpenFlow tunneling or VLAN. The network controller organizes the attack countermeasure by means of attack analyzer decisions. Next the initial node to goal node various attack exploited and those are count by the distance of vAlert still it reaches the target node. The attack probability is calculated by means countermeasure algorithm to valid the overall performance of the network. The workflow system of the proposed system is given below;

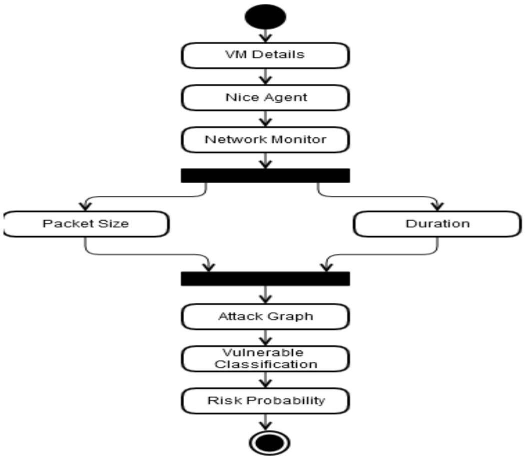
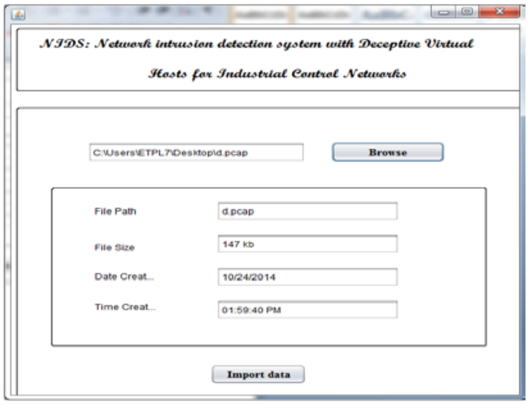


Fig 4: The workflow mechanism of the proposed system

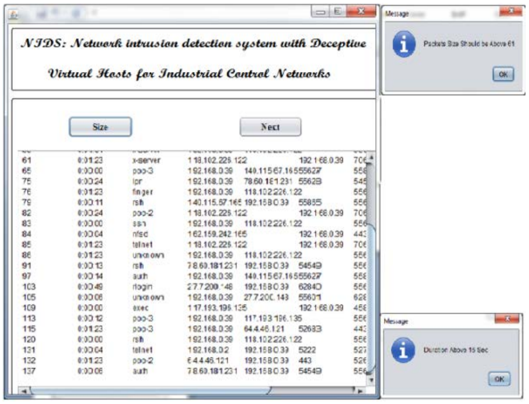
RESULT AND DISCUSSION


NIDS: Network intrusion detection system with Deceptive Virtual Hosts for Industrial Control Networks
Browse
Import data

```
C:\Users\ETPL7\Desktop\d.pcap

File Path      d.pcap
File Size      147 kb
Date Creat...  10/24/2014
Time Creat...  01:59:40 PM
```

Fig 5: Importing the data


NIDS: Network intrusion detection system with Deceptive Virtual Hosts for Industrial Control Networks
Size
Next
Message
OK

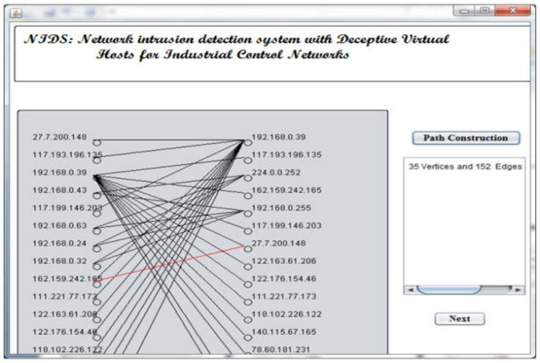
```
61   0:01:23  x-server  118.102.226.122                 192.168.0.39  706
65   0:00:00  pop-3     192.168.0.39    140.115.67.165  55627         558
75   0:00:24  lpr       192.168.0.39    78.60.181.231   55628         545
76   0:01:23  finger    192.168.0.39    118.102.226.122               556
79   0:00:11  rsh       140.115.67.165  192.168.0.39    55855         556
82   0:00:24  pop-2     118.102.226.122                 192.168.0.39  706
83   0:00:00  ssh       192.168.0.39    118.102.226.122               556
84   0:00:04  nfsd      162.159.242.165                 192.168.0.39  443
85   0:01:23  telnet    118.102.226.122                 192.168.0.39  706
86   0:01:23  unknown   192.168.0.39    118.102.226.122               556
91   0:00:13  rsh       78.60.181.231   192.168.0.39    54549         556
97   0:00:14  auth      192.168.0.39    140.115.67.165  55627         558
103  0:00:48  rlogin    27.7.200.148    192.168.0.39    62840         556
105  0:00:06  unknown   192.168.0.39    27.7.200.148    55601         628
109  0:00:00  exec      117.193.196.135                 192.168.0.39  458
113  0:00:12  pop-3     192.168.0.39    117.193.196.135               556
115  0:01:23  pop-3     192.168.0.39    64.4.46.121     52683         443
120  0:00:00  rsh       192.168.0.39    118.102.226.122               556
131  0:00:04  telnet    192.168.0.2     192.168.0.39    5222          527
132  0:01:23  pop-2     64.4.46.121     192.168.0.39    443           526
137  0:00:06  auth      78.60.181.231   192.168.0.39    54549         556
```

Packets Size Should be Above 61

Duration Above 15 Sec

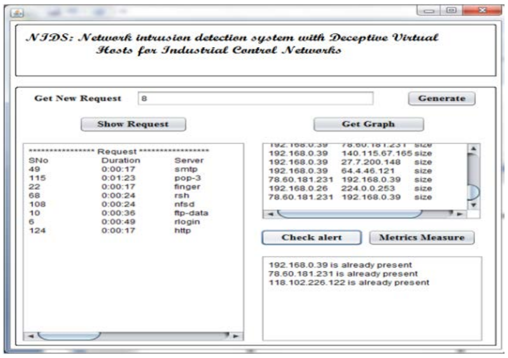
Fig 6: Analyzing network info & protocol setting

From the observation fig 5 shows the initial work in which the captured data from the control system is processed. The data is import to the frame work, in which the file path, size, create date and processing time are noted for further processing. In fig 6 the entire details like IP, from which network topology, server , the packet sent – received, size and time information are gathered based on the protocol is generated. The protocol is based on the time period and size to a certain calculation in which the node which violating the protocol is considered as the vulnerable activity in the network



35 Vertices and 152 Edges

Fig 7: Path construction


NIDS: Network intrusion detection system with Deceptive Virtual Hosts for Industrial Control Networks
Generate
Show Request
Get Graph
Check alert
Metrics Measure

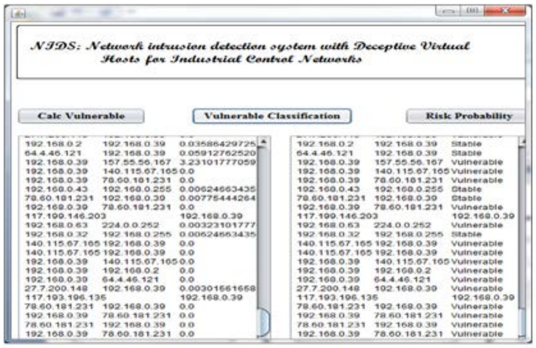
Get New Request: 8

```
**************** Request *****************
SNo       Duration    Server
49        0:00:17     smtp
115       0:01:23     pop-3
22        0:00:17     finger
68        0:00:24     rsh
108       0:00:24     nfsd
10        0:00:36     ftp-data
6         0:00:49     rlogin
124       0:00:17     http
```

```
192.168.0.39    140.115.67.165 size
192.168.0.39    27.7.200.148   size
192.168.0.39    64.4.46.121    size
78.60.181.231   192.168.0.39   size
192.168.0.26    224.0.0.253    size
78.60.181.231   192.168.0.39   size
```

```
192.168.0.39 is already present
78.60.181.231 is already present
118.102.226.122 is already present
```

Fig 8: Analyzing intruder possibilities

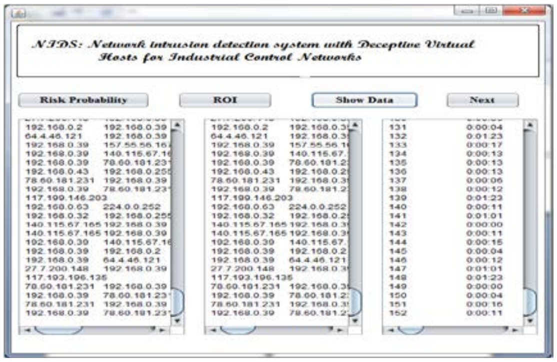

NIDS: Network intrusion detection system with Deceptive Virtual Hosts for Industrial Control Networks
Calc Vulnerable
Vulnerable Classification
Risk Probability

```
192.168.0.2      192.168.0.39    0.03586429725
64.4.46.121      192.168.0.39    0.05912762520
192.168.0.39     157.55.56.167   3.23101777059
192.168.0.39     140.115.67.165  0.0
192.168.0.39     78.60.181.231   0.0
192.168.0.43     192.168.0.255   0.00624663435
78.60.181.231    192.168.0.39    0.00775444264
192.168.0.39     78.60.181.231   0.0
117.199.146.203                  192.168.0.39
192.168.0.63     224.0.0.252     0.00323101777
192.168.0.32     192.168.0.255   0.00624663435
140.115.67.165   192.168.0.39    0.0
140.115.67.165   192.168.0.39    0.0
192.168.0.39     140.115.67.165  0.0
192.168.0.39     192.168.0.2     0.0
192.168.0.39     64.4.46.121     0.0
27.7.200.148     192.168.0.39    0.00301661658
117.193.196.135                  192.168.0.39
78.60.181.231    192.168.0.39    0.0
192.168.0.39     78.60.181.231   0.0
78.60.181.231    192.168.0.39    0.0
192.168.0.39     78.60.181.231   0.0
```

```
192.168.0.2      192.168.0.39    Stable
64.4.46.121      192.168.0.39    Stable
192.168.0.39     157.55.56.167   Vulnerable
192.168.0.39     140.115.67.165  Vulnerable
192.168.0.39     78.60.181.231   Vulnerable
192.168.0.43     192.168.0.255   Stable
78.60.181.231    192.168.0.39    Stable
192.168.0.39     78.60.181.231   Vulnerable
117.199.146.203                  192.168.0.39
192.168.0.63     224.0.0.252     Vulnerable
192.168.0.32     192.168.0.255   Stable
140.115.67.165   192.168.0.39    Vulnerable
140.115.67.165   192.168.0.39    Vulnerable
192.168.0.39     140.115.67.165  Vulnerable
192.168.0.39     192.168.0.2     Vulnerable
192.168.0.39     64.4.46.121     Vulnerable
27.7.200.148     192.168.0.39    Vulnerable
117.193.196.135                  192.168.0.39
78.60.181.231    192.168.0.39    Vulnerable
192.168.0.39     78.60.181.231   Vulnerable
78.60.181.231    192.168.0.39    Vulnerable
192.168.0.39     78.60.181.231   Vulnerable
```

Fig 9: Classifying the vulnerable in the network

From the fig 7 we can see how the network communication is established, which is the source node and destination node along with the packet transformation. In this network the red line showing a node attempting a vulnerable activity during the communication based on that fig 8 gives the details about number request for transferring the packet. And the possible vulnerable nodes already in the network are shown to be the continuation the fig 9 shows the risk possibility by calculating the activities of vulnerable nodes in the network.



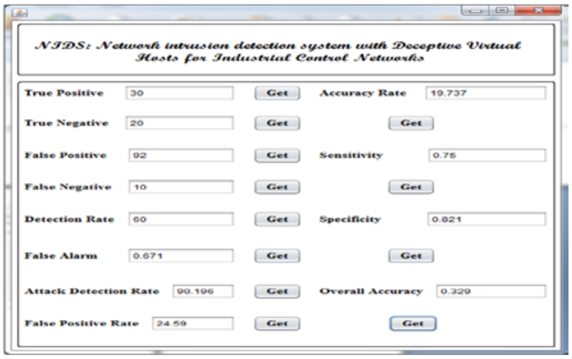
NIDS: Network intrusion detection system with Deceptive Virtual Hosts for Industrial Control Networks

```
192.168.0.2     192.168.0.39
64.4.46.121     192.168.0.39
192.168.0.39    157.55.56.16
192.168.0.39    140.115.67.16
192.168.0.39    78.60.181.231
192.168.0.43    192.168.0.255
78.60.181.231   192.168.0.39
192.168.0.39    78.60.181.231
117.199.146.203
192.168.0.63    224.0.0.252
192.168.0.32    192.168.0.255
140.115.67.165 192.168.0.39
140.115.67.165 192.168.0.39
192.168.0.39    140.115.67.16
192.168.0.39    192.168.0.2
192.168.0.39    64.4.46.121
27.7.200.148    192.168.0.39
117.193.196.135
78.60.181.231   192.168.0.39
192.168.0.39    78.60.181.231
78.60.181.231   192.168.0.39
192.168.0.39    78.60.181.231
```

```
192.168.0.2     192.168.0.3
64.4.46.121     192.168.0.3
192.168.0.39    157.55.56.1
192.168.0.39    140.115.67.
192.168.0.39    78.60.181.2
192.168.0.43    192.168.0.2
78.60.181.231   192.168.0.3
192.168.0.39    78.60.181.2
117.199.146.203
192.168.0.63    224.0.0.252
192.168.0.32    192.168.0.2
140.115.67.165 192.168.0.3
140.115.67.165 192.168.0.3
192.168.0.39    140.115.67.
192.168.0.39    192.168.0.2
192.168.0.39    64.4.46.121
27.7.200.148    192.168.0.3
117.193.196.135
78.60.181.231   192.168.0.3
192.168.0.39    78.60.181.2
78.60.181.231   192.168.0.3
192.168.0.39    78.60.181.2
```

```
131     0:00:04
132     0:01:23
133     0:00:17
134     0:00:13
135     0:00:13
136     0:00:13
137     0:00:06
138     0:00:12
139     0:01:23
140     0:00:11
141     0:01:01
142     0:00:00
143     0:00:11
144     0:00:15
145     0:00:04
146     0:00:12
147     0:01:01
148     0:01:23
149     0:00:00
150     0:00:04
151     0:00:16
152     0:00:11
```

Fig 10: Calculating the risk probability



NIDS: Network intrusion detection system with Deceptive Virtual Hosts for Industrial Control Networks

True Positive 30

True Negative 20

False Positive 92

False Negative 10

Detection Rate 60

False Alarm 0.671

Attack Detection Rate 90.196

False Positive Rate 24.59

Accuracy Rate 19.737

Sensitivity 0.75

Specificity 0.821

Overall Accuracy 0.329

Fig 11: Performance analysis

From fig 10 and 11 we can say the confirmation risk attempted by the node and who are the intruders along with overall performance by calculating number of users to the intruders their negatives and positives. The accuracy and sensitivity is calculated as per given;

Average = True positive /total count – True Negative/ total count

Sensitivity = = True positive /total count – True Negative/ total count

$$Attack\ propability = \frac{Number\ of\ attack\ packets}{Total\ number\ of\ packets}$$

Based on the above calculation, attack happened in the network and detection on analyzing the intruder is estimated. By which the overall accuracy of the network is examined.

CONCLUSION & FUTURE ENHANCEMENT

In this work we discussed some of the draw backs of existing system regarding monitoring and preventing the vulnerable of virtual machines from being compromised in the cloud server. These are effectively handled by our proposed systems and the justifications of these works are discussed in the result section. For a better attack detection in a distributed network our NICE incorporates attack graph analytical procedures into the intrusion detection processes by employs a reconfigurable virtual networking system. Further this work can be implemented in wide network with large distributed mechanism along with customized cloud architecture to suspect the intrusion detection and to be controlled with limited power consumption in future.

REFERENCE

1) D. A. Shea, “Critical infrastructure: Control systems and the terrorist threat,” Libr. Congr., Rep. Congr. RL31534, Jan. 2004.

2) Y. Huang et al., “Understanding the physical and economic consequences of attacks on control systems,” Int. J. Crit.

Infrastruct. Prot., vol. 2, no. 3, pp. 73–83, Oct. 2009.

3) C. Rieger, D. Gertman, and M. McQueen, "Resilient control systems: Next generation design research," in Proc. 2nd IEEE Conf. Human Syst. Interact., Catania, Italy, May 2009, pp. 632–636.

4) G. Rueff, B. Wheeler, T. Vollmer, and T. McJunkin, "INL control system situational awareness technology final report," INL, Idaho Falls, ID, USA, Rep. EXT-11-23408, Jan. 2013.

5) A. Carcano et al., "A multidimenisonal critical state analysis for detecting intrusions in SCADA systems," IEEE Trans. Ind. Informat., vol. 7, no. 2, pp. 179–186, May 2011.

6) R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security Privacy. Oakland, CA, USA, May 2010, pp. 305–316.

7) L. Chao, M. Sumiko, and K. Hirotsugu, "Dynamic hybrid system of honeypot and IDS for network security analysis," IPSJ SIG Notes, vol. 2013, no. 26, pp. 1–5, Dec. 2013.

8) M. A. McQueen and W. F. Boyer, "Deception used for cyber defense of control systems," in Proc. 2nd IEEE Conf. Human Syst. Interact. Catania, Italy, May 2009, pp. 624–631.

9) J. Ousterhout, "Is scale your enemy, or is scale your friend?" Commun. ACM, vol. 54, no. 7, pp. 110–111, Jul. 2011.

10) J. Hieb and J. H. Graham, "Anomaly-based intrusion detection for network monitoring using a dynamic honeypot," Intell. Syst. Res. Lab., Univ. Louisville, Louisville, KY, TR-ISRL-04–03, Dec. 2004.

11) N. Provos and T. Holz, Virtual Honeypots. Reading, MA, USA: Addison- Wesley, 2007.

12) C. Hecker and B. Hay, "Securing E-government assets through automating deployment of honeynets for IDS support," in Proc. 43rd Hawaii Int. Conf. Syst. Sci., Koloa, Kauai, HI, USA, 2010, pp. 1–10.

13) F. Gagnon and B. Esfandiari, "A hybrid approach to operating system discovery based on diagnosis," Int. J. Netw. Manage., vol. 21, pp. 106–119, Mar. 2011.

14) G. Lyon, Nmap Network Scanning. Palo Alto, CA, USA: Insecure.org, 2008 [Online]. Available: www.nmap.org

15) D. P. Duggan, "Penetration testing of industrial control systems," Sandia National Lab., Albuquerque, NM, USA, Tech. Rep. SAND2005-2846P, Mar. 2005.

16) C. Hecker, K. L. Nance, and B. Hay, "Dynamic honeypot construction," in Proc. 10th Coll. Inf. Syst. Secur. Educ., Adelphi, MD, USA, 2006, pp. 4880–4889.

17) X. Jiang and D. Xu. (2004). BAIT-TRAP: A Catering Honeypot Framework [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.84.3

18) V. Pothamsetty and M. Franz. SCADA Honeynet Project [Online]. Available: http://scadahoneynet.sourceforge.net/

19) Digital Bond Incorporated. SCADA Honeynet [Online]. Available: http:// www.digitalbond.com/tools/scada-honeynet/

20) P0f [Online]. Available: http://lcamtuf.coredump.cx/p0f.shtml

21) Tshark Network Analyzer [Online]. Available: http://www.wireshark.org/

22) M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. 13th Conf. Syst. Admin., Berkeley, CA, USA, Nov. 7–12, 1999, pp. 229–238.

23) Tcpdump Packet Analyzer [Online]. Available: http://www.tcpdump.org/

24) Ntop Network Traffic Probe [Online]. Available: http://www.ntop.org/

25) P. Auffret, "SinFP, unification of active and passive operating system fingerprinting," J. Comput. Virol., vol. 6, no. 3, pp. 197–205, Aug. 2010

26) O. Linda, T. Vollmer, and M. Manic, "Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge," in Proc. IEEE Symp. Resilience Control Syst., Salt Lake City, UT, USA, Aug. 2012