ijecs
open access
www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 5 may, 2014 Page No. 5891-5896

Improving Efficiency of IDS using alert Correlation

Thakar Vivek R, Prof. Vrushank Shah, Prof. Yatin Patel

Department of computer science Rollwala computer center *Gujarat University* Ahmedbad, India

Vthakar77@gmail.com

Electronics & Communication Department Indus University Ahmedabad , India

vrushankshah.ec@indusuni.ac.in

Department Of Computer Engineering Faculty of Engineering, SSESGI Gujarat Technological University Rajpur, Kadi

yatin.patel7488@gmail.com

***Abstract*— Intrusion Detection Systems are designed to monitor a network environment and generate alerts whenever abnormal activities are detected. However, the number of these alerts can be very large making their evaluation a difficult task for a security analyst. Alert management techniques reduce alert volume significantly and potentially improve detection performance of an Intrusion Detection System. To Improve the effectiveness and efficiency of an Intrusion Detection System by significantly reducing the false positive alerts and increasing the ability. Proposed technique addresses the issues relating the optimality of decision-making through correlation in multiple sensors framework. The process is based on through Dempster Shafer rule. Moreover, the reliability factor for any Intrusion Detection System is also addressed accordingly in order to minimize the chance of false diagnose of the final network state. A considerable number of simulations are conducted in order to determine the optimal performance of the proposed prototype. In this paper we are introduce combines evidence from two homogenous and one heterogeneous ids using dempster-shafer algorithm**

I. Introduction

Firewalls are made to stop unnecessary network traffic into or out of any network. Packet filtering firewalls typically will scan a packet for layer 3(ip layer) and layer 4 (transport layer) protocol information. There are not work on application layer semantics .

In contrast to firewalls, IDS will scan all packets at layers 3 and 4 header information as well as the application level protocols looking for back door Trojans, Denial of Service attacks, worms, buffer overflow attacks, detect scans against the network etc. An IDS provides much greater visibility to detect signs of attacks and compromised hosts. There is still the need for a firewall to block traffic before it enters the network; but, an IDS is also needed to make sure that the traffic that gets past the firewall will be monitored. Intrusion detection systems are gather or collected information from a computer or network of computers and attempt to detect intruders or system abuse. Generally, an intrusion detection system will check a human analyst of a possible intrusion and take no further action, but some newer systems take active steps to stop an intruder at the time of detection. IDSs can be categorized into two classes, anomaly based IDSs and misuse based IDSs. Anomaly Based IDSs look for deviations from normal usage behaviour to identify abnormal behaviour. Misuse based, on the other hand, recognizes patterns of attack. Anomaly detection techniques rely on models of the normal behaviour of a computer system. These models may focus on the users, the applications, or the Network. Behaviour profiles are built by performing statistical analysis on historical data [1, 2], or by using rule based approaches to specify behaviour patterns [3,4,5]. A basic assumption of anomaly detection is that attacks differ from normal behaviour in type and amount. By defining what's normal, any violation can be identified, whether it is part of threat model or not. However, the advantage of detecting previously unknown attacks is paid for in terms of high false-positive rates in anomaly detection systems. It is also difficult to train an anomaly detection system in highly dynamic environments. The anomaly detection systems are intrinsically complex and also there is some difficulty in determining which specific event triggered the alarms.

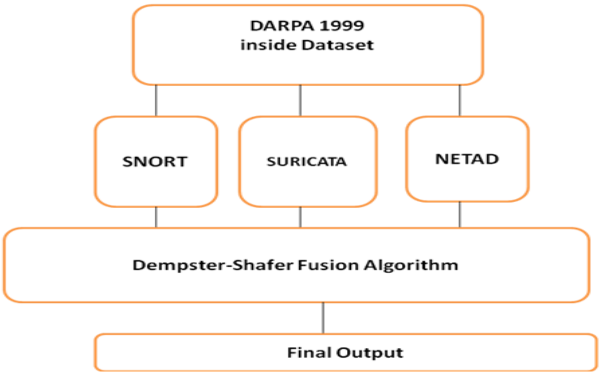
On the other hand, misuse detection systems essentially contain attack descriptions or signatures and match them against the audit data stream, looking for evidence of known attacks [6,7]. The main advantage of misuse detection systems is that they focus analysis on the audit data and typically produce few false positives. The main disadvantage of misuse detection systems is that they can detect only known attacks for which they have a defined signature. As new attacks are discovered, developers must model and add them to the signature database. In addition, signature-based IDSs are more vulnerable to attacks aimed at triggering a high volume of detection alerts by injecting traffic that has been specifically crafted to match the signatures used in the analysis process. This type of attack can be used to exhaust the resources on the IDS computing platform and to hide attacks within the large number of alerts produced.

II. RELATED WORK

Julien Corsini was worked on analysis and evaluation of network intrusion detection method to uncover data theft but one NIDS is not efficient to detect to whole categories of darpa (dos,r2l,u2r,probe).we can not depends on single type of NIDS detection rate and uncertainty rate. Ciza Thomas was worked on Performance Enhancement of Intrusion Detection Systems using Advances in Sensor Fusion .she was taken three IDS PHAD,ALAD,SNORT .first two are anamoly based and last one signature based and passed to fusion algorithm and prove the PHAD exhibits superior performance in detecting the probes and the DoS attacks. On the other hand, it exhibits sub-optimal performance in detecting the attacks belonging toR2L and U2R classes. the fusion results in a detection better than the best detector if the detectors are uncorrelated. Otherwise, as the worst case, at least the performance of the best IDS results from fusion.Faisal Mahmood was worked on Minimization of DDoS false alarm rate in Network Security. Deployment of an Intrusion Detection System is not sufficient for detecting a real intrusion. The issue of managing large number of generated alerts is a challenging task for any security analyst. The goal of this work, as stated earlier, is to propose, design and develop architecture for a fusion-based false alarm reduction module that work with existing Intrusion Detection Systems. He was worked on minimization of SYN flooding ,ICMP flooding, UDP flooding attacks for DDos category using Dempster-Shafer algorithm.two signature based IDS bro and snort was used.in this paper our approach to use three IDS combination of signature based and anamoly based and fuse to Dempster-Shafer algorithm to different to other.

III.CURRENT ISUES

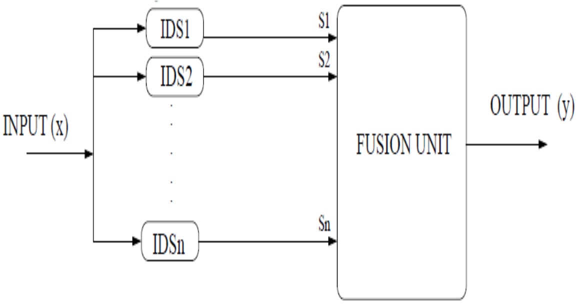
One IDS is not efficient to detect all type of attack. (R2L, DOS, Probe, U2R)[15] .We cannot depend on any single IDS (Signature or Anomaly) to detect all kind of attack. Different kinds of IDS are suitable for different Attacks. For example: SNORT detects U2R and DOS very well.SURI CATA detect R2L and DOS very well. NETAD detect DOS very well.IDS Generates sometimes unnecessary large amounts of false alerts. It is very hard to manage by network administrator [8,9,10]. detection systems must be more effective, detecting wider range of attacks with fewer false positives. intrusion detection must keep pace with modern networks' increased size, speed and dynamics. Intrusion detection must keep up with the input-event stream generated by high-speed networks and high-performance network nodes. Additionally, there is the need for analysis techniques that support the identification of attacks against whole networks. The challenge for increased system effectiveness is to develop a system that



detects close to 100 percent of attacks with minimal false positives.[11]

IV. PROPOSED SOLUTION:

We are collecting evidences different types of heterogonous and homogenous ids to passes into fusion unit. In fusion unit we are using Dempster -shafer Combination Rule. In ids1 we take snort(signature based) ,ids2 suricata(signature based), ids3 netad (anamoly based) then applying Dempster -shafer Combination Rule .



Dempster -shafer algorithm:It is a generalization of probability Algorithm.Dempster-Shafer theory has ability to combine evidences provided by different observers in an intrusion detection environment. The most important part of this theory is Dempster's rule of combination which combines evidence from two or more Homogeneous or Heterogeneous IDS.

Important Parameters Of D-S Algorithm:(1)BPA (Basic Probability Assignment): It is a positive number between 0 and 1. It exists in the form of a probability value. It is also called a mass(m)

. (2) Belief (Bel) :Body of empirical evidence

{m (B1), m (B2), m (B3)….}

Bel (A) = Σ m (Bi).

(3)Plausibility Function (Pl)

The plausibility (Pl) is the sum of all the masses

Pl (A) = 1 – Bel (Ā)

4.) The Frame of Discernment (Ω)

Ω =Uncertainty

Bel(A)+ Bel(-A)+Uncertainty(Ω)= 1

[12,13,14]

r-s rule: Case I) For Number of Alerts (NOA) < 1 r = 1 Case II) For Number of Alerts (NOA) >10, *r =(Number of detected Alerts / 50)* +2 Drop all digits after decimal point For Example, r=(40/50)+2 = 2.8 ,r = 2 (by dropping 0.8 i.e. drop all digits after decimal point)

mapping alert to masses.Jøsang[1999] for collecting our parameters for belief, disbelief and uncertainty;

b = r /(r+s+c) ,

d= s /(r+s+c) ,

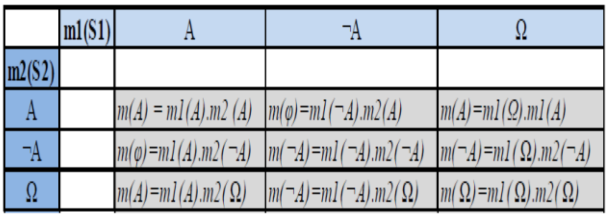
u = 2/(r+s+c)

Where b=belief, d=disbelief u=uncertainty, r= amount of evidence supporting actual event, s=amount of evidence supporting its negative c= constant=2 The combination called the joint mass (m12) is calculated from the two sets of masses m1 and m2.

$$m12\ (A) = \frac{B \cap C = A,\ \Sigma\ m1(B)\ m2(C)}{1 - [B \cap C = \emptyset,\ \Sigma\ m1(B)\ m2(C)]}\ ,\ m12\ (A) \neq \emptyset$$

Where,m12 (A) = Combined belief of the hypothesis A,m1 (B) = Belief committed to B as seen by the first observer,m2 (C) =Belief committed to C as seen by the second observer [B ∩ C = ∅, Σ m1(B) m2(C)]= K [12,13,14]

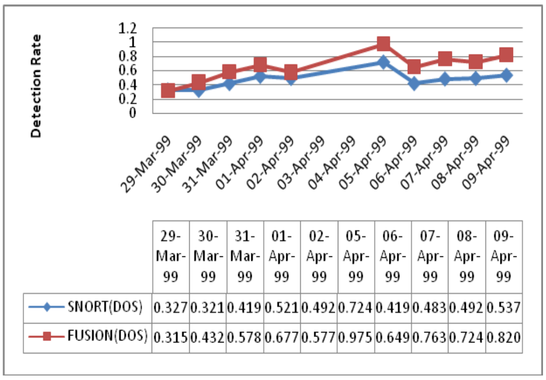
The reassignment of mass function between two ids



	m1(S1)	A	¬A	Ω
m2(S2)				
A		m(A) = m1(A).m2 (A)	m(φ)=m1(¬A).m2(A)	m(A)=m1(Ω).m1(A)
¬A		m(φ)=m1(A).m2(¬A)	m(¬A)=m1(¬A).m2(¬A)	m(¬A)=m1(Ω).m2(¬A)
Ω		m(A)=m1(A).m2(Ω)	m(¬A)=m1(¬A).m2(Ω)	m(Ω)=m1(Ω).m2(Ω)

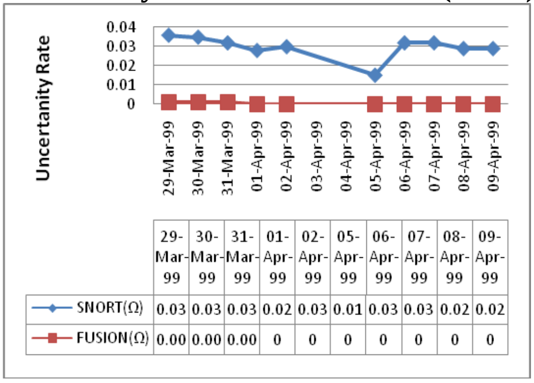
V. RESULT AND ANALYSIS

Detection Result-Snort Vs FUSION IDS(0 to 1)



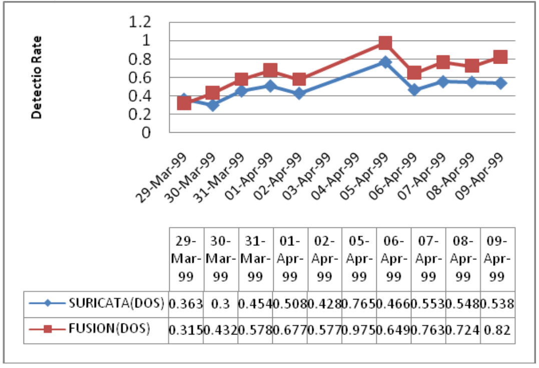
	29-Mar-99	30-Mar-99	31-Mar-99	01-Apr-99	02-Apr-99	05-Apr-99	06-Apr-99	07-Apr-99	08-Apr-99	09-Apr-99
SNORT(DOS)	0.327	0.321	0.419	0.521	0.492	0.724	0.419	0.483	0.492	0.537
FUSION(DOS)	0.315	0.432	0.578	0.677	0.577	0.975	0.649	0.763	0.724	0.820

Uncertanity-Snort Vs fusion IDS(0 to 1)



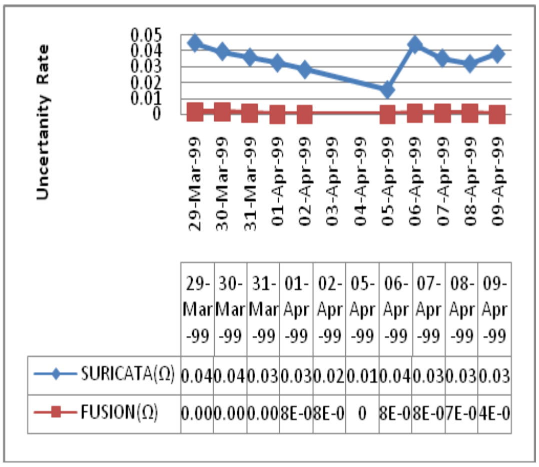
	29-Mar-99	30-Mar-99	31-Mar-99	01-Apr-99	02-Apr-99	05-Apr-99	06-Apr-99	07-Apr-99	08-Apr-99	09-Apr-99
SNORT(Ω)	0.03	0.03	0.03	0.02	0.03	0.01	0.03	0.03	0.02	0.02
FUSION(Ω)	0.00	0.00	0.00	0	0	0	0	0	0	0

Detection Result-Suricata Vs FUSION IDS(0 to 1)



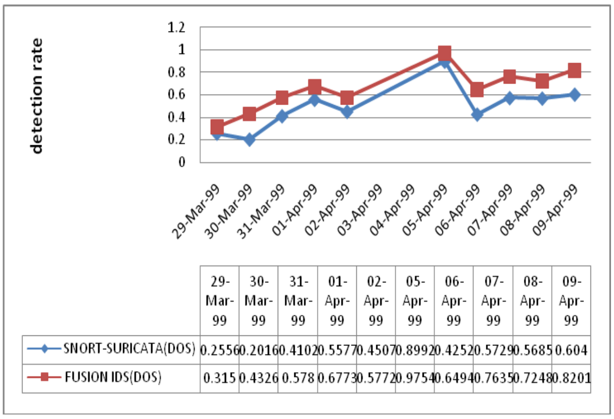
	29-Mar-99	30-Mar-99	31-Mar-99	01-Apr-99	02-Apr-99	05-Apr-99	06-Apr-99	07-Apr-99	08-Apr-99	09-Apr-99
SURICATA(DOS)	0.363	0.3	0.454	0.508	0.428	0.765	0.466	0.553	0.548	0.538
FUSION(DOS)	0.315	0.432	0.578	0.677	0.577	0.975	0.649	0.763	0.724	0.82

Uncertainty Result suricata vs fusion ids(0 to 1)



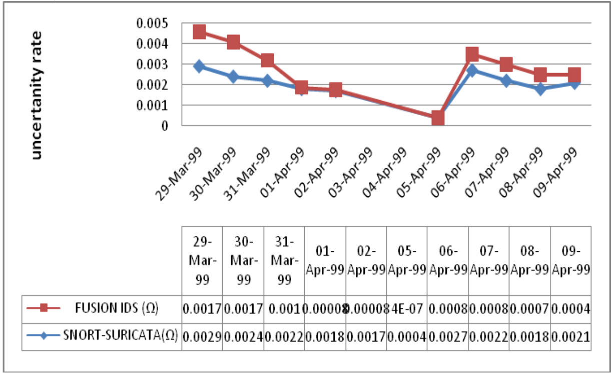
	29-Mar-99	30-Mar-99	31-Mar-99	01-Apr-99	02-Apr-99	05-Apr-99	06-Apr-99	07-Apr-99	08-Apr-99	09-Apr-99
SURICATA(Ω)	0.04	0.04	0.03	0.03	0.02	0.01	0.04	0.03	0.03	0.03
FUSION(Ω)	0.00	0.00	0.00	8E-0	8E-0	0	8E-0	8E-0	7E-0	4E-0

Detection rate of SNORT-SURICATA Vs FUSION IDS



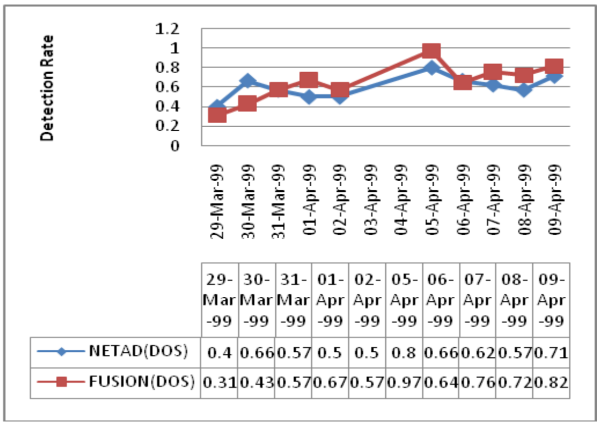
	29-Mar-99	30-Mar-99	31-Mar-99	01-Apr-99	02-Apr-99	05-Apr-99	06-Apr-99	07-Apr-99	08-Apr-99	09-Apr-99
SNORT-SURICATA(DOS)	0.2556	0.2016	0.4102	0.5577	0.4507	0.8992	0.4252	0.5729	0.5685	0.604
FUSION IDS(DOS)	0.315	0.4326	0.578	0.6773	0.5772	0.9754	0.6494	0.7635	0.7248	0.8201

Uncertainty Result snort-suricata vs fusion ids(0 to 1)



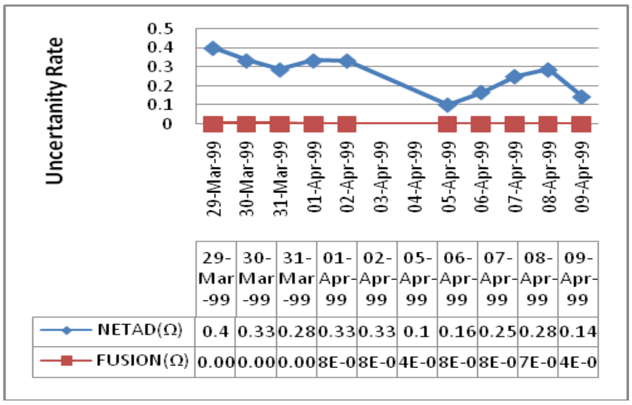
	29-Mar-99	30-Mar-99	31-Mar-99	01-Apr-99	02-Apr-99	05-Apr-99	06-Apr-99	07-Apr-99	08-Apr-99	09-Apr-99
FUSION IDS (Ω)	0.0017	0.0017	0.001	0.00008	0.00008	4E-07	0.0008	0.0008	0.0007	0.0004
SNORT-SURICATA(Ω)	0.0029	0.0024	0.0022	0.0018	0.0017	0.0004	0.0027	0.0022	0.0018	0.0021

Detection rate of NETAD Vs FUSION IDS

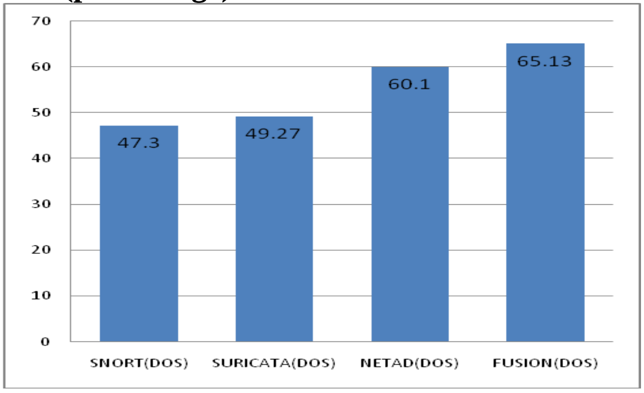


	29-Mar-99	30-Mar-99	31-Mar-99	01-Apr-99	02-Apr-99	05-Apr-99	06-Apr-99	07-Apr-99	08-Apr-99	09-Apr-99
NETAD(DOS)	0.4	0.66	0.57	0.5	0.5	0.8	0.66	0.62	0.57	0.71
FUSION(DOS)	0.31	0.43	0.57	0.67	0.57	0.97	0.64	0.76	0.72	0.82

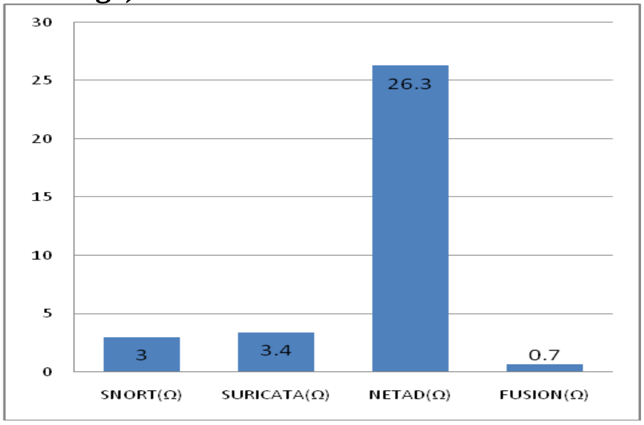
Uncertainty Result NETAD vs fusion ids(0 to 1)



Improvement in Efficiency Level Of FUSION IDS(percentage)



Decresing Uncertanity level in FUSION IDS (Percentage)



VII. CONCLUSION AND FUTURE WORK

Depending on any single type (Signature based or Anomaly based) of IDS is not advisable.Each IDS has its own specialty to detect attacks of different category (R2L,U2R,DOS,PROBE).Fusion approach to combine evidences from two or more IDS is reliable and give accurate detection rate with low uncertainty rate.We applied fusion approach on DOS category of attack, this can also be apply on remaining category. Fusion approach to combine evidences from two or more IDS is reliable and gives accurate detection rate with low uncertainty level. Using Dempster-Shafer algorithm we fused three Ids Snort,Suricata and Netad for the Denial of service attack (DOS). After fusing the IDS we found more detection rate with low false uncertainty rate against individual work of any single IDS. In our work, we used Dempster-Shafer algorithm to fuse the IDS using alert correlation for particularly Denial of Service (Dos) category attack. Remaining categories of attacks R2L, Probe and U2R can be resolved by this technique and method. Using this work improvement in efficiency of ids can be achieved and also uncertainty level of false alerts can be reduce.

VIII. REFERENCES

[1] P. Helman, G. Liepins, Statistical Foundations of Audit Trail Analysis for the Detection of Computer Misuse
In IEEE Transactions on Software Engineering volume Vol 19, No. 9, pages 886-901, 1993.

[2]H.S.Javitz, A. Valdes, The NIDES StatisticalComponent Description and Justification, Technical report, SRI International, Menlo Park, CA, March1994.

[3]C. Ko, M. Ruschitzka, K. Levitt, Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-based Approach,
In Proceedings of the 1997 IEEE Symposium on Security andPrivacy, pp. 175-187, May 1997.

[4] D. Wagner, D. Dean, Intrusion Detection via Static Analysis, In Proceedingsof the IEEE Symposium on Security and Privacy, IEEE Press, 2001

[5] C.Warrender, S. Forrest, B.A. Pearlmutter, Detecting intrusions using system calls: Alternative data modelsIn IEEE Symposium on Security andPrivacy, pages 133-145, 1999.

[6] CSI/FBI Computer Crime and Security Survey, http://www.gocsi.comipress/20020407

[7]DEF CON 8 conference. Las Vegas, NV, 2000. www.defcon.org

[8] Eugene Albin,Neil Rowe, Rex Buddenberg September 2011, A COMPARATIVE ANALYSIS OF THE SNORTANDSURICATA INTRUSION-DETECTION SYSTEMS

[9]Aleksandar Lazarevic*, Levent Ertoz*, Vipin Kumar*, Aysel Ozgur*, Jaideep Srivastava* A comparative study of anomaly detection schemes in network intrusion detection

[10] Intrusion Detection and Prevention In-sourced or Out-sourced, SANS Institute (2008).

[11] Performance Enhancement of Intrusion Detection Systems using Advances in Sensor Fusion,ciza Thomas, Supercomputer Education and Research CentreIndian Institute of Science BANGALORE – 560 012April 2009

[12]YU, D., FRINCKE, D. 2005. Alert confidence fusion in intrusion detection systems with extended Dempster-Shafer Theory.ACM-SE 43: Proceedings of the 43rd annual south- East regional conference. 2, 142 – 147

[13]Chen, Q., Aickelin, U. 2006. Dempster-Shafer for anomaly detection In Proceedings Of the International Conference on Data Mining (DMIN 2006), Las Vegas, USA.

[14]Faisal Mahmood, 2012, Windsor, Ontario, Canada, Minimization of DDOS false alarm rate in network security , Refining fusion through correlation.

[15] M. L. Laboratory, “Darpa intrusion detection data sets”, 1999. [Online]. Available: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999