ISSN:0975-9646
Ashish K. Uplenchwar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3778-3783

Intrusion Detection System (IDS) framework for Digital Network

Mr. Ashish K. Uplenchwar,
M.E. Student,
G. H. Raisoni College of Engineering and Management,
Wagholi, Pune, India

Dr. Tanuja Dhope
Associate Professor,
G. H. Raisoni College of Engineering and Management,
Wagholi, Pune, India

Abstract: Cyber security has become high priority in Industrial Automation (IA). Here dependable operation is to ensure the security, stability and reliability in power delivery system. Anonymity progress can be easily removed by using the Intrusion Detection System (IDS) framework. In this paper Supervisory Control and Data Acquisition (SCADA)-IDS with protocol based and behavior based analysis is proposed and exemplified in order to detect known and unknown cyber-attacks from inside or outside SCADA systems. This framework provides a hierarchical approach for an integrated security system, comprising distributed IDSs to prevent the anomalous attacks due to access control process. In this article we have compare three methods viz access control, protocol base and behavior based whitelist technique. In behavior based there are two techniques used viz length detector and digital signature. However, for research in the community to progress, such a dataset would be valuable. The proposed system creates new datasets to mitigate vulnerable attacks from cyber-crime side to save the higher level records and system. The simulation result shows that behavior based method outperforms the other two methods with respect to time efficiency and accuracy.

Keywords: Cyber security; intrusion detection; smart grid; supervisory control and data acquisition (SCADA); digital signature technique

I. INTRODUCTION

Securing the advanced substation environment is simply piece of a more extensive and significant exertion that is obliged to guarantee the safe operation of cutting edge power frameworks. There are system based (NIDS) [1] and host based (HIDS) interruption recognition frameworks. A few frameworks may to stop an interruption, yet this is not obliged or expected of a checking framework. Interruption identification and aversion frameworks (IDPS) are basically centered on distinguishing conceivable episodes, logging data about them, and reporting activities. Likewise, associations use IPsec for different purposes, for example, distinguishing issues with security arrangements, archiving existing dangers and preventing people from damaging security approaches. System interruption recognition frameworks NIDS [1] are set at a vital point or indicates inside the system screen activity to and from all gadgets on the system. It performs an investigation for a passing movement on the whole subnet, lives up to expectations in an indiscriminate mode, and matches the activity that is passed on the subnets to the library of known assaults. When the assault is recognized, or strange conduct is sensed, the alarm can be sent to the manager.

Case of the NIDS would be introducing it on the subnet where firewalls are placed to check whether somebody is attempting to break into the firewall. Conceivably one would filter all inbound and outbound movement, however doing so may make a bottleneck that would hinder the general pace of the system. An IDS which is abnormality based have screen system movement and measure up it against a secured gauge. The gauge recognize what is "ordinary" for that system what kind of transfer speed is by and large utilized, what conventions are utilized, what ports and gadgets for the most part associate with one another and alarm the manager or client when activity is caught which is irregular, or fundamentally distinctive, than the pattern. The supervisory framework may be joined with an information obtaining framework by including the utilization of coded flag over correspondence channels to secure data about the status of the remote gear for showcase or for recording capacities. It is a type of industrial control system (ICS).

Current security countermeasures in SCADA (supervisory control and data acquisition) frameworks predominantly concentrate on ensuring frameworks from outer interruptions or vindictive assaults. For instance, approaching movement to substations, control focuses, and corporate systems investigated by business firewalls or IDS. Nonetheless, this security approach just considers edge safeguards and overlooks inner part location inside a substation system or a control focus. For example, an architect can enter a substation and associate his or her smart phone to the local area network (LAN). A purposeful or unintended assault by means of a contaminated smart phone now has an enhanced shot of achievement in light of the fact that edge resistances have been avoided. In practice and in most detrimental possibility situations, the greater part of the digital holdings in SCADA frameworks should be viewed as defenseless. Be that as it may, we unable to demand that all cyber assets meet the most noteworthy security necessities because of budgetary cost, time and framework requirements.

Industrial control frameworks are machine based frameworks that screen and control modern methodologies that exist in the physical world. Current security countermeasures in SCADA [2] frameworks mainly concentrate on securing frameworks from outside interruptions or malicious attacks. Case in point, approaching activity to substations, control focuses, and corporate systems reviewed by business firewalls or IDS. On the other hand, this security approach just considers border resistances and disregards inside identification inside a substation system or a control focus. There-fore, an architect can enter a substation and join his or her portable computer to the LAN. With the application of IT innovations, new digital vulnerabilities develop in keen lattices and comparative basic bases. These vulnerabilities could be misused, not just from outside sources, for example, terrorists, programmers, contenders, or mechanical surveillance, additionally from inside dangers, for example, ex-workers, displeased representatives, outsider merchants, or site engineers. Security for protecting the entire smart-grid techno-logical environment requires the consideration of many subsystems that make up the smart grid, for example, wide-area monitoring protection and control (WAMPAC), distribution-management system (DMS), advanced metering infrastructure (AMI), and higher level communication architectures at the grid system level. The scope of this paper is to focus on one important sub-system level of the smart grid environment, specifically cyber-security for digital substations.

II. RELATED WORK

The IDS of this paper is developed by using data collected by simulating attacks on IEDs and launching packet smelling attacks using forged address resolution protocol (ARP) packets. The uncovering ability of the system is then tested by simulating attacks and through genuine user activity. Intrusion detection is an effective countermeasure that is yet to be deployed in IEC61850 networks [3]. It's capable of actively countering attacks instead of passive blocking as in a firewall. Compared to a conventional computer network, the threats and countermeasures for an IEC61850 network are different. There-fore, the IDS for IEC61850 has to be developed by using experimental data based upon simulated attacks and packet sniffing [3].

In order to improve the cyber-security of the smart grid by utilizing a hierarchical and distributed intrusion detection system in the wireless mesh network. Security is improved via the classification of intrusion data using the support vector machine (SVM) and artificial immune system (AIS) algorithms. The effectiveness of the new model for improving security is demonstrated through multiple simulations [3].

To avoid the cyber-security threats, [3] proposes a distributed intrusion detection system for smart grids (SGDIDS) by developing and deploying an intelligent module, the analyzing module (AM), in multiple layers of the smart grid. Multiple AMs have been embedded at each level of the smart grid - the home area networks (HANs), neighborhood area networks (NANs), and wide area networks (WANs), where they had used the support vector machine (SVM) and artificial immune system (AIS) to detect and classify malicious data and possible cyber-attacks [3].

A methodology for the discovery of digital attacks are against mechanical establishments. The key components of this strategy are the idea of Critical State, and the presumption that an attacker going for harming a mechanical establishment (like a Power Plant) and have to alter for accomplishing that come about the state of the framework from protected to basic selective state approval, scarcely material in conventional ICT frameworks, thinks that its regular application in the mechanical control field, where the basic states are by and large well-known and restricted in number. Since the discovery is focused around the investigation of the framework development, and not on the dissection of the attack advancement the IDS for known selective states, can distinguish likewise "zero day attacks" [4]. The paper has proposed multi-dimensional metric giving a parametric measure of the separation between a given state and the set of selective states. This metric can be utilized for following the development of a framework, showing its nearness to the set of predefined selective states [4].

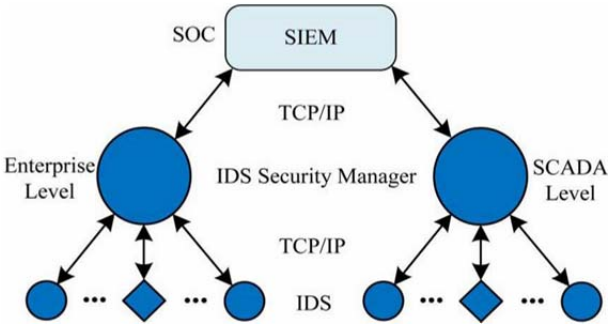

Fig.1 SCADA-IDS security-management system

The principal contribution of this paper [5] is a demonstration that anomaly detection, and specifically methods based on adaptive learning, can provide a useful intrusion detection capability in process control networks. To evaluate two anomaly detection techniques, namely, pattern based detection for communication patterns among hosts, and flow-based detection for traffic patterns for individual flows. These techniques were able to detect some basic attacks launched against the MODBUS servers in our DCS test-bed. Pattern based & flow based anomaly detection has proposed here to improve rate of detection.

III. PROPOSED SYSTEM

Proposing SCADA-IDS framework for detecting unwanted user on router, by extracting information about access control white list, protocol based white list and behavior base rule from the network. The source and destination IDS are all the major attributes going to use in our entire system. Below Architecture shows the system architecture of our SCADA IDS system. In the given above

Architecture there are operators which are legal users and someone may be attacker. Packets are exchanging through LAN network. There are huge chances of suspicious packets attack into the LAN. Intrusion detection system is fixed into the network as we can see it into the figure.

When packets enter into the network Intrusion Detection System starts its working. Our IDS system is structured of 3 techniques.

1. **ACW (Access Control Whitelist):** In this IDS check whitelist of MAC and IP pair which are present in our LAN. If corresponding packet doesn't have MAC-IP pair which belongs to whitelist then it will be detected as attack packet and which will be stored into Log file for future reference. Otherwise packets are not suspicious packets.

2. **PBW (Protocol Based Whitelist):** If packet belongs to whitelist then protocol based whitelist will check that packet. If corresponding packets matches any of the rule which belongs to protocol based whitelist then it will be considered as suspicious packet stored into Log file as well as database. Example.

Rule 1: if(serrr_rate= ("0.00") & login number=("1") & flag("SF")). // this is normal packet
Rule 2: if(flag=("0")) // attack
Rule 3: if(flag=("0") & fail_login1>5) // attack

3. **BBR (Behavior Based Rule):** In this method two techniques are used

- Digital signature generation: In this method if one operator wants to send any message to another operator which is confidential then for security purpose digital signature method generate keys and signature and sends encrypted data towards receiver. At the receiver end signature will be checked and if it does not match then it is suspicious packet and stored into the log file.
- Length detector: This method checks the actual payload and length of input packet if it is greater than payload then packet is suspicious and will be stored into the log file.

When attack found at that time IDS will generate alarm to know about attack detection. In this way whole architecture work and we found the packets are suspicious attack or not.

IV. PROPOSED ALGORITHM

Let S be the proposed system which we use to find the attack detection system through ACW, PBW, BBR and digital signature generation. They equip our detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively. A digital signature technique is developed to enhance and to speed up the process of SCADA.

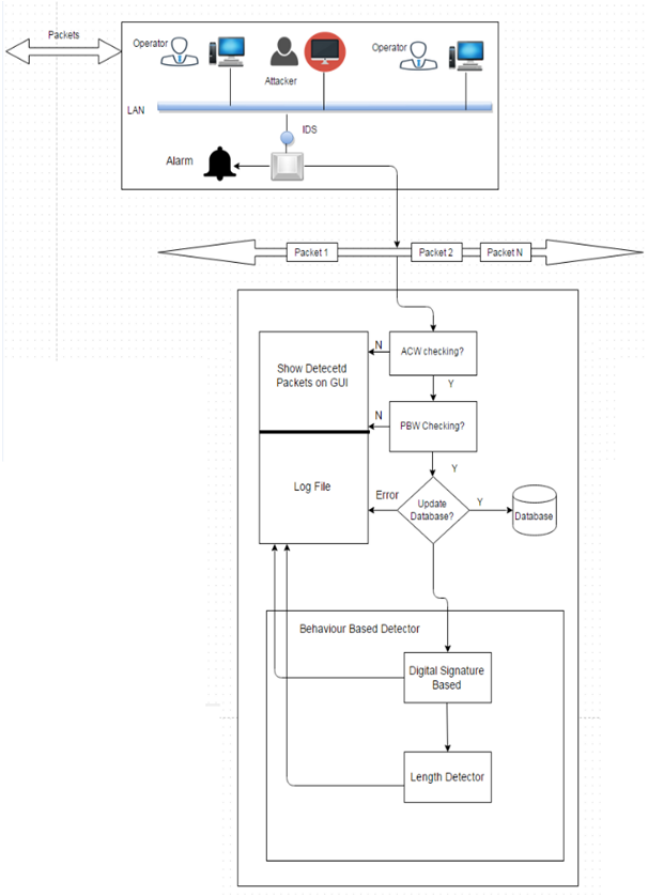

Fig.2 Proposed System Architecture

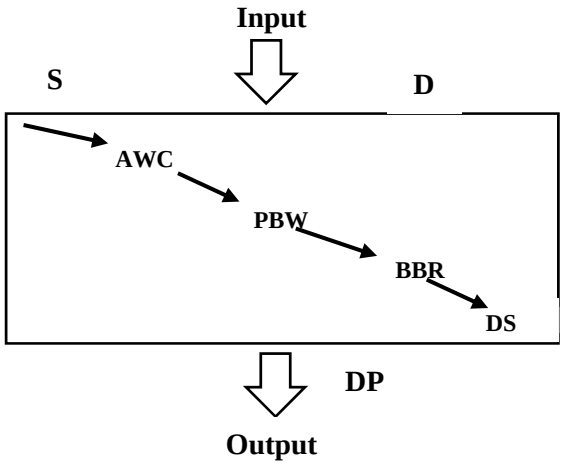

Fig 3. Processes in Detection of Intrusion attacks.

As we can see in Fig 3.
S = {D, ACW, PBW, BBW, DP}
Where, S=
System.
D= Dataset.
ACW = Access Control Whitelist.
PBW = Protocol Based Whitelist.
BBW =Behaviour Based Whitelist.
DG= Digital Signature Generation.

Input:

Given an arbitrary dataset X = {x1, x2,…., xn},

Where xi = $[f_1^i, f_2^i, \ldots., f_m^i]$T , $(1 \leq i \leq n)$ represents the ith m-dimensional traffic record.

Where x1, x2,…, xn is n number of packets flowing in the network.

ACW (Access Control Whitelist).

AC = { , $MAC_{dst}, IP_{src}, IP_{dst}$}

Where MAC_{src} = Source MAC address.

MAC_{dst} = Destination MAC addresses.

IP_{src} = Source IP address.

IP_{dst} = Destination IP address.

If any of the addresses or ports is not in the corresponding whitelist, the detector will take a predefined action, for example, it will alert in IDS mode and log the detection results. That is

AC $\notin \{AC_{wl}\} \rightarrow$ Actions (alert.log)

Where, AC= , MAC_{dst} , IP_{src} , IP_{dst} and AC_{wl} represent the corresponding whitelist set.

PBW (Protocol Based Whitelist).

Assume there are n packets coming from dataset as

D={x1, x2, …., xn},

Where xi = $[f_1^i, f_2^i, \ldots., f_m^i]$T , $(1 \leq i \leq n)$ represents the ith m-dimensional traffic record.

R = {r1, r2, …. , rn}

Where R is the set of rule for protocol based detection and r1= Rules of whitelist.

If when the IDS is deployed at the network between two control centers, the protocol-based detector only allows communication traffic complying with specific rules of protocol; otherwise, it will generate an alert message. That is,

P $\notin \{P_R\} \rightarrow$ Actions (alert.log)

Where P is the Packet and P_R is Protocol based whitelist which contains rules of detecting intrusion from corresponding traffic.

BBR(Behavior Based Rules):

Assume there are n packets coming from dataset as

D={x1, x2, · · · , xn},

Where xi = $[f_1^i, f_2^i, \ldots., f_m^i]$T , $(1 \leq i \leq n)$ represents the ith m-dimensional traffic record.

BBR = {LD, Sig}

Where, BBR is the set of methods for detection of packets belonging to attack packets.

LD=Length Detector

Sig= Signature based Detector.

LD = {P1,P2…Pn}

Where P1,.., Pn are the input packets

When packet contains bytes which indicate the length information about the packet in the payload, it is proposed that a length detector should be applied to detect that whether the number shown in the length bytes is equal to the real length of the payload, such that

$PL_l \neq \rightarrow$ Action (alert, log)

Where PL_l is the length value indicated in the length field of the payload, and PL_{rl} stands for the practical length of the payload.

If alert generated then store it into log file.

DG (Digital Signature):

i) Key Generation:

- Choose two large prime numbers p and q and calculate n= p x q
- Calculate $\emptyset(n) = (p-1)x\ (q-1)$ and Choose e such that gcd (e, $\emptyset(n)$)=1
- Calculate d such that d X e mod $\emptyset(n) = 1$
- Choose random numbers b and x. Here x should not relative prime to $\emptyset(n)$ - Calculate c such that b^x x c(mod)n=1
- Public key is (n, e, c, x) and private key is (d, b).

ii) Signature Generation:

Calculate S1 = (m) mod n if x|s1 (i.e. x is a divisor of s1) then generate s1 again.

Calculate s2 = (H(m) x b^{s1}) mod n

H (.) is a one way hash function. (s1, s2) is the signature of message m. Sender sends signature with the message m to receiver.

iii) Signature Verification:

Receiver first calculates H (m) using the received message m and check the following two conditions for signature verification:

Verify, if H(m) = s_1^e mod n

$(m)^x \equiv s_2^x$ x c^{s1} mod n **DP**

(Detected Packets) :

DP={n,m}

Where n is normal packets and

M is the malicious packets.

Log (Log File):

Log={x1, x2,.., xn}

Where Log is the set of detected packets i.e. x1, x2 etc.

If P $\notin$ ACW or PBW or BBR $\rightarrow Action\ (Log)$

Where P is the packet if it does not belongs to corresponding whitelist i.e. ACW, PBW and BBR then store that packet into log file.

V. SIMULATION RESULTS

Detecting attackers has been primarily compare among three algorithms, attackers detection precision can be assure this parameter.

We have defined the graph through calculating recall and precision values.

$$Recall = \frac{|\{relevant\ document\} \cap \{retrieved\ documents\}|}{|\{relevant\ document\}|}$$

Recall in information retrieval is the fraction of the documents that are relevant to the query that are successfully retrieved.

Precision is the probability that a (randomly selected) retrieved document is relevant.

Precision and recall are then defined as:

$$Precision = \frac{tp}{tp + fp}$$

$$Recall = \frac{tp}{tp + fn}$$

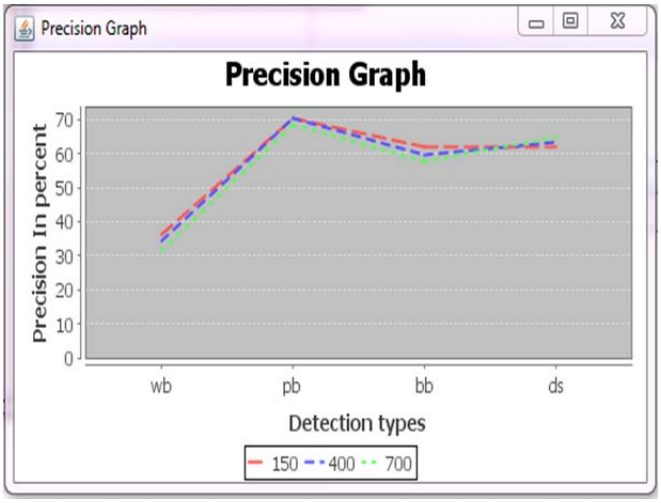

Fig 4. Precision Graph.

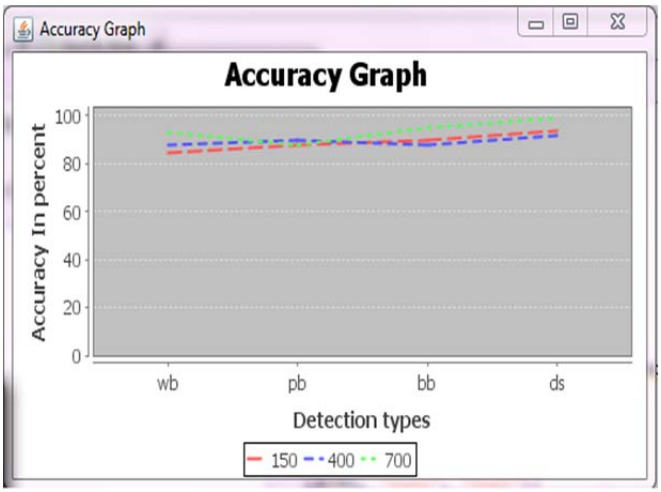

Fig 5. Accuracy Graph.

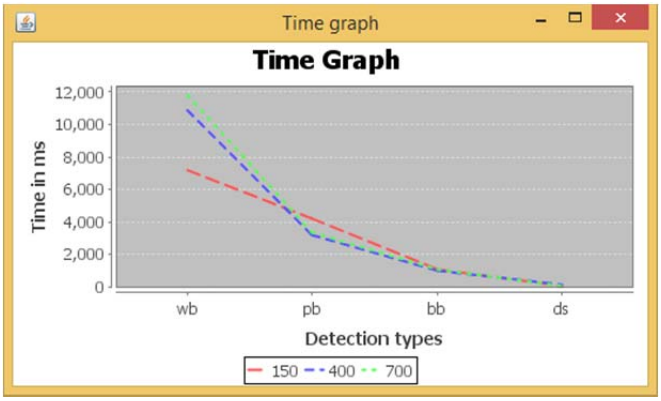

Fig 6. Time graph

For evaluating the performance of whitelists-based (wb), protocol-based (pb), behavior based (bb) and digital signature (ds). We have taken the dataset of 150,400 and 700 records. The parameters like accuracy, time required for execution and precision has been taken into considerations in simulating these algorithms' performance. For evaluating the performance of whitelists-based (wb), protocol-based (pb), behavior based (bb) and digital signature (ds). We have taken the dataset of 150,400 and 700 records .The parameters like accuracy, time required for execution and precision has been taken into considerations in simulating these algorithms' performance. As shown in above graphs, Precision of protocol and accuracy of digital signature base shows better result with respect to other techniques for the dataset 700 records and as shown in time graph digital signature requires less time to communicate for a dataset 150 records.

VI. CONCLUSION

The whitelists-based, protocol-based and behavior-based method studied & implemented the intrusion detection techniques, the behavior based algorithm method with digital signature technique is proposed in order to monitor the entire sensor network. Also based on the Simulation results as shown in (Fig. & Table) it reflects that the performance is improved in terms of accuracy & time efficiency with the help of Behavior Based Technique as compared with Access Control Whitelist & Protocol Based techniques. Thus Digital Signature Technique helps in better monitoring of cybercrime process in networking.

REFERENCES

[1] A.A.Ghorbani, W.Lu, and M.Tavallaee, Network Intrusion Detection and Prevention: Concepts and Techniques. 2010, pp. 1–20.

[2] Y. Yang, K. McLaughlin, S. Sezer, ,T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks" IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 29, NO. 3, JUNE 2014, pp. 1092-1102

[3] Upeka Kanchana Premaratne, Jagath Samarabandu ,"An Intrusion Detection System for IEC61850 Automated" IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 25, NO. 4, OCTOBER 2010,pp2376-2383

[4] A.Carcano,A. Coletta,M.Guglielmi,M. Masera "A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems" IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 7, NO. 2, MAY 2011 ppt 179-186.

[5] T. Morris, R. Vaughn, and Y. Dandass, "A retrofit network intrusion detection system for MODBUSRTU and ASCII industrial control systems,"inProc.,2012,pp.2338–2345

[6] Z. Trabelsi and K. Shuaib, "Man in the middle intrusion detection," in Proc. IEEE Global Telecommun. Conf., 2006, pp. 1–6.

[7] E. D. Knapp, Industrial Network Security: Securing Critical Infra-structure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 2011, pp. 60–61.

[8] J. Hurley, A. Munoz, and S. Sezer, "ITACA: Flexible, scalable net-work analysis," in 2012, pp. 1084–1088.

[9] IBM, "IBM security QRadar SIEM," Somers, NY, USA, Tech. rep.WGD03021-USEN-00, Jan. 2013.

[10] Z. Yichi, W. Lingfeng, S. Weiqing, R. C. Green, and M. Alam, Distributed intrusion detection system in a multi-layer network architecture of smartgrids," vol.2,no.4,pp.796–808, Dec. 2011.

[11] M. Crosbie and G. Spafford, "Applying genetic programming to ntrusion detection," presented at the AAAI Fall Symp. Series, AAAI Press, MenloPark, CA, Tech. Rep. FS-95-01, 1995

[12] W. Lu and I. Traore, "Detecting new forms of network intrusion using genetic programming,"Comput. Intell., vol. 20, no. 3, pp. 474–494,2004.

[13] "Communication Pattern Anomaly Detection In Process Control Systems" Alfonso Valdes, Steven Cheung 22 - 29 11-12 May 2009 978-1-4244-4178-5

[14] P. Gross, J. Parekh, and G. Kaiser, "Secure selecticast for collaborative intrusion detection systems," inProc. Int. Workshop on DEBS, 2004

[15] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Q. Yao, B.Pranggono, and H. F. Wang, "Man-in-the-middle attack testbed inves-tigating cyber-security vulnerabilities in smart grid SCADA systems,"inProc. IET Int. Conf. Sustain. Power Gen. Supply, 2012, pp. 1–8.

[16] IEEE Standard Communication Delivery Time Performance Require-ments for Electric Power Substation Automation, IEEE Standard 1646–2004, Feb. 2005.

[17] De Ocampo, Frances Bernadette C, Del Castillo, Trisha Mari L Gomez, Miguel Alberto N "AUTOMATED SIGNATURE CREATOR FOR A SIGNATURE BASED INTRUSION DETECTION SYSTEM WITH NETWORK ATTACK DETECTION CAPABILITIES (PANCAKES)" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(1): 25-35 , 2013 (ISSN: 2305-0012)

[18] Huang Lu, Jie Li, and Hisao Kameda "A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature"This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceeding.

AUTHORS

Mr. Ashish K. Uplenchwar is a P. G. Scholar in the Computer Engineering Department, G. H. Raisoni College of Engineering and Management, Wagholi, Pune. He has received Bachelor of Technology degree (BTech) in Computer Science and Engineering in 2012 from MIT, Aurangabad, India. His research interests are Wireless Networks, Computer Networks, Database management etc.

Dr.Tanuja Satish Dhope (Shendkar) is a full time Associate Professor at Department of Computer , G.H.Raisoni College of engineering, Pune India. She has acquired her Ph.D in wireless communication at University of Zagreb, Croatia under Erasmus Mundus Mobility for Life Project in 2012. She graduated in Electronics and Telecommunication engineering at Cummins College of Engineering, University of Pune in 1999. She has received Master in Electronics Engineering from Walchand college of Engineering, Sangli, Shivaji University in 2007. Her research focus is on cognitive radio network optimization with spectrum sensing algorithms, radio channel modelling for cognitive radio, wireless sensor network, cooperative spectrum sensing, Direction of arrival (DoA) Estimation algorithms in Cognitive Radio and in SDMA. She published 24 scientific papers in journals and conference proceedings. She has reviewed 7 IEEE conference papers and honoured as 'Session Chair' at ICACCI 2013 conference in Mysore.