Journal of Theoretical and Applied Information Technology
10th November 2014. Vol. 69 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DRPGAC: DETECTING AND PREVENTING MALICIOUS ACTIVITIES IN WIRELESS SENSOR NETWORKS

A. THOMAS PAUL ROY[1], Dr.K.BALASUBADRA[2]

[1]Associate Professor, Dept. of CSE., P.S.N.A. College of Engineering and Technology
Dindigul-624 622, TamilNadu, India
[2]Professor, Dept. of CSE., R.M.D. Engineering College,
Kavaraipettai, Tiruvallur Dt., Tamil Nadu – 601 206, India
E-mail: [1]pauli.dgl@gmail.com , [2]balasubadra@yahoo.com

ABSTRACT

One of a most familiar countermeasure against Network attacks is an efficient Intrusion Detection System. In order to improve efficiency of the intrusion detection system and prevention using various methods, techniques and procedures are discussed in the earlier studies. Many procedures generally try to assuage specific weaknesses of intrusion detection. The main objective of this paper is to decrease the malicious activities by providing prevention in terms of Identity based Authentication. In the existing system LBIDS system is applied to detect the malicious node in WSN where the IDS are deployed in the leader. If the malicious node occur far from leader's place then it is difficult to detect the malicious activity. In this paper **DRPGAC**- [Dynamic Random Password Generation and Comparison] approach is proposed for detecting and preventing malicious activities in each stage of the network functionality. DRPGAC is a pre, post-processing solution for malicious activities. A sequence of DRP is generated automatically and assign to the network users. Whenever the users enter into the network, while data transmission and communication should be start to each other, their password is verified and validated to check the user is an innocent or malicious. The DRPGAC approach has been simulated and tested using a set of nodes deployed in Network Simulator Environment and the result shows better performance comparatively than the existing approaches.

KEYWORDS: *Intrusion Detection System; Wireless Networks; Random Password Generation; Malicious Activities; Prevention; Attacker Node.*

1. NOMENCLATURE

To understand and have better readability of this paper the symbols used are given in the following table with its description.

Symbols	Description
DRP	Dynamic Random Password
DRPGAC	Dynamic Random Password Generation and Comparison
IDS	Intrusion Detection System
IaaS	Infrastructure as a service
DDoS	Distributed Denial of Service
UAV	Un-named Air Vehicles
BRUIDS	behavior rule-based unmanned air vehicles IDS
LBIDS	Leader Based IDS
SOA	Service Oriented Architecture

2. INTRODUCTION

One of the main instruments for skirmishing against various attacks is IDS. IDS are a vital part of a complete security policy in information system. They are enormous in generating a huge number of alerts which are outmoded and bogus. Emerging Technologies are extremely developing in mobile devices performance and their activities. Notebooks, smart phones and iPads are used for email, document sharing, chatting and recording and playing audio, videos. These devices also used for lot of personal information. Since various kinds and numerous numbers of attackers appear

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

frequently in internet based applications, it is necessary to protect the devices and communication using these devices. Various types of IDS are available nowadays such as misuse detection and anomaly detection.

A wireless network uses radio waves to connect devices such as laptops to the Internet and to our business network and its applications. A wireless sensor network refers to a group of spatially distributed autonomous sensors to monitor environmental and physical conditions. Wireless sensor networks measure environmental conditions like pollution levels, wind speed, wind direction, temperature, sound, pressure, humidity, etc. In earlier days wireless sensor networks were designed for the military operations. But now its application has since been extended to traffic, health and many other industrial and customer areas. A wireless sensor network consists of few hundred nodes to thousands of nodes. The sensor node includes the equipment of an interfacing electronic circuit, a microcontroller, radio transceiver with an antenna, an energy source(battery) the price of the sensor node is vary depending on the functionality parameters of bandwidth, energy consumption, memory and computational speed rate. Security is a broadly used term encompassing the characteristics of authentication, confidentiality, robustness, integrity, freshness and survivability. For this reason, many different methods for network security have been developed.

Security mechanisms that provide confidentiality and authentication are critical for the operation of many sensor applications. For this reason, variety of protocols has been developed to provide authentication and confidentiality. WSN have more number of nodes and computational competencies, memory and security policy. To achieve more security in WSN using random password methods are used. By generating password randomly it increases the security levels of the system and prevent from the out breaks. It is highly secure and extremely difficult to guess the password. Because this key has a combination of number, alphabetic with lower and upper case and alpha-numerical characters.

3. LITERATURE REVIEW

Various attacks and challenges are discussed here for review the earlier literature. A score-based multi cyclic intrusion detection algorithm was proposed to detect the changes quickly among the nodes according to their properties [1]. This method is also called Shiryaev-Roberts procedure which performs better than the other detection schemes. The problem of IDS in distributed WSN is analyzed by categorizing the detection probability in terms of sensing scenarios [2]. Various network parameters are examined and compared for verifying the uniformity of the network users. A DDoS attacks appears in IaaS clouds is controlled using a multiphase distributed vulnerability detection mechanism [3]. A NIDS system was proposed for smart-sensor inspired devices using under SOA. This NIDS can detect anomaly based intrusions [4]. FPGA based NIDS was proposed in [5], to investigate the hardware based attacks. Well defined IDS for Jamming attack, anomaly detection and some new types of attacks are monitored and detected in CRN [6]. To minimize compromised attack and evade detection a hybrid detection framework was proposed, which can investigate the FDI attack and is also controlled by CONSUMER attack model [7]. Various kinds of attacks appear in the network layer and the solutions are discussed briefly in [8]. An adaptive scientific based IDS for detecting malicious activity in VANET is experimented in [9]. The results were compared with BRUIDS which provides secure UAV applications. An agent based threat model was introduced against file access right system [10].

All the routing protocols follow a standard routing mechanism such as IEEE - 802.11, IEEE-802.15.4 and WiMAX. A cyber security attack model was introduced for distributed smart grid applications in [11]. General IDS were proposed to exploit the weakness of IDS in each abstraction level and a critical investigation based solution is provided [12]. SCADA system was proposed for controlling distributed infrastructures like power plants, water distribution system [13]. A novel anomaly detection mechanism was proposed for situational aware of cyber attacks [14] which checks the identity. A post –processing solution was applied which has a set of multiple IDS sensor indication system [15]. Every set of indication system is aggregated into a single indication to improve the quality. Whenever a critical event occur this indication system create a relevant alert to all other nodes in the network for security. A hybrid anomaly detection

Journal of Theoretical and Applied Information Technology
10th November 2014. Vol. 69 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

framework was developed and deployed for detecting injecting attacks [16] into uncertain data. One such challenge method for intrusion severity analysis is discussed in [17] where the significance of the intrusion severity is analyzed in overall clouds. An IDS/IPS method was proposed and it is positioned in cloud environment to achieve desired security in the next generation networks [18]. In [19] a novel IDS for IoT was proposed and it was named as SVELTE which detects all malicious nodes like sinkhole, Sybil, and/or selective forwarding attacks.

3.1. Existing System

A Leader Based Intrusion Detection System [20] was proposed to detect and prevent malicious activities in WSN. A Leader was elected statically in the network for a group of nodes and it monitors those nodes comes under their control. Whenever a node gets activated it informs its status to the leader, so the leader knows about all the nodes information. But the entire new node should be informed about the leader and it takes time. To solve this kind of issues DRPGAC is proposed in this paper.

4. PROBLEM STATEMENT

Devices used under wireless networks mostly access internet based applications like reservation, enquiry, billing, online payment and online transaction etc. Since, most of the vulnerability appears via internet it is necessary to provide a security mechanism for communication elements. The main objective of this paper is to design a mechanism for detecting malicious activity in terms of their Identity.

4.1.Proposed System

DRPGAC has three modules such as Node identification, Mutual Authentication and Secret Key updating. The overall functionality of DRPGAC is depicted clearly in Figure-1. Some of the assumptions are made for simulating the DRPGAC approach where the network G is a wireless network. The node may be of any type [laptop, mobile, PC etc.] which can communicate using wireless communication medium. Base station BS is the responsible administrator for the entire network can assign ID, key, key-verification etc, in the network.

4.2.Node-Id Preparation

Initially when a new created the BS prepares the NODE-ID based on the characteristics, type of communication and type of the instrument. Example if the first node created is laptop then the ID is TALTA0001. If the second node created is mobile then the ID is SAMEA0002.

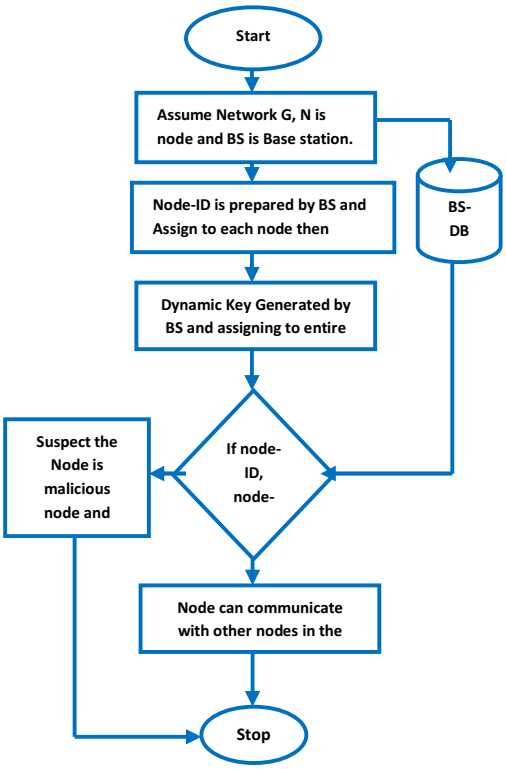

Figure-1: Overall System Model

Table-1: Id For Laptop As A Node

company Name	Device Type	Series	Auto Gen Number
ToshibA	LapTop	A	0001
ID is			TALTA0001

Table-2: ID For Mobile As A Node

company Name	Device Type	Series	Auto Gen Number
ToshibA	LapTop	A	0001
ID is			TALTA0001

Journal of Theoretical and Applied Information Technology
10th November 2014. Vol. 69 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Where,**TA** indicates the company **T**oshibA;

LT indicates the device is **L**ap**T**op

A is the series number according to the generation features added in the device. And 0001 is a unique number generated automatically. Also a 9 digit pseudo random number [IMEI] is generated mod with 2 and stored in the BS-DB.

4.3. Dynamic Key Generation

A dynamic number is generated using KeyGEN method where the IMEI number is added and appends at last with the node-ID.

$\boldsymbol{KeyGEN}$ ( )

{

- $For\ I\ =\ 1\ to\ N$
  - $Vi\ =\ substring\ (Node-ID, 4)$;
  - key_i =append(Vi, Node-ID + Vi)
  - for i = 1 to length(key_i)
  - $IMEI_i = IMEI_i \oplus 2$
  - end i
- $End\ i$

}

Example for Node-1 the key is

IMEI = 278373612 ⊕ 2 = 010111010

Key (Node1) = 010111010TALTA010111010.

This key is stored in the BS-DB for further verification and node validation. The size of the key is up to 32 [bits] where if the size increased means the series of the device gets upgraded like 'A' to 'B'. Since the key is unique and less in size the time taken for key submission and key verification is very less. Also it is not necessary that BS can spend more time on the key verification.

4.4. Secured Communication

In network G consists of N number of nodes where any node can communicate with any other node in the network. Let S be the source node and D be the destination node and the node-1 to node-3 are the intermediate nodes among the source and destination. If the intermediate nodes information is available in the BS-DB then the data transmitted else it suspects that node is malicious node.

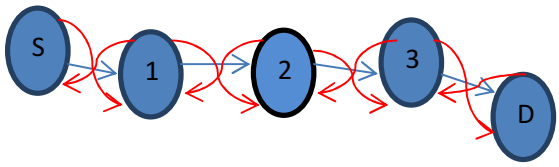

Figure-2: Pair Wise Node Validation

Table-3: Simulation Parameters

PARAMETER	LEVEL
Area	1000m x 1000m
Speed	1 to 15 m/s
Radio Propagation Model	Two − ray ground reflection
Radio Range	250 m
Number of Nodes	20 to 100
MAC	802.11
Application	CBR, 100 to 500
Packet size	50
Simulation Time	100 s
Placement	Random
Malicious Population	Upto 5%
Sybil Ids per malicious node	2

The overall functionality of the DRPGAC approach is discussed above and written as an algorithm below.

Algorithm_DRPGAC ( )

{

- $Initialize\ G, BS, Node, N\ are\ Network, Base\ Station,$
- $Node\ and\ N: Number\ of\ nodes\ in\ the\ network$
  .
- $For\ i\ =\ 1\ to\ N$

Journal of Theoretical and Applied Information Technology
10th November 2014. Vol. 69 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- $Node - ID = ConCat(CompanyName, DeviceType, Series, Auto Number)$;
- $End\ i$
- $For\ I = 1\ to\ N$
  - $Vi = substring\ (Node - ID, 4)$;
  - key_i =append(Vi, Node-ID + Vi)
  - for i = 1 to length(key_i)
  - $IMEI_i = IMEI_i \oplus 2$
  - end i
- $End\ i$
- For i=S to D
- If $(Node_i == D)\ then\ stop$
- Else
- If$(Node_i \cdot ID, Node_i \cdot Key \cdot exists$(BS-DB.record))
- $node_{i+1}.data = node_i.data$
- Else
- Next **I** }

4.5. Simulation Setup

In order to implement and evaluate our scheme, we use Network Simulator NS-2.34 using the parameters listed in Table 1.

To investigate the DRPGAC approach efficiency it is simulated in NS2. Where the area of the network size is 1500 x 1500 and the number of nodes deployed in simulation is 10, 20, 30, 40 and 50 in 5 rounds. The front end of the simulation is developed in TCL and the protocol configuration is implemented in C++ code.

5. RESULTS AND DISCUSSION

The simulation results include the number of malicious activity before and after deploying the DRPGAC approach. Initially a visual interface for network topology is presented. In this interface, the DRPGAC algorithm confirmed and detects the malicious node according to the node behavior.

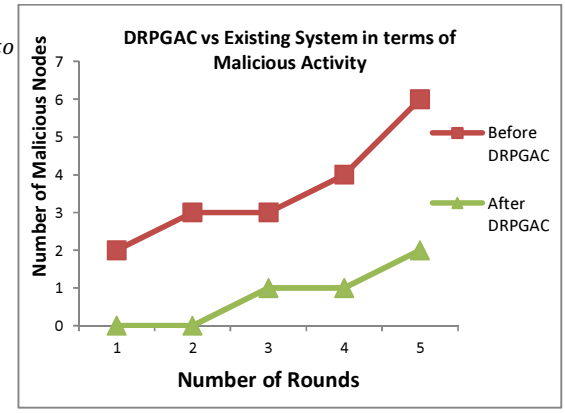

Figure-3: DRPGAC Vs. Existing System Comparison In Malicious Activity

Figure-3 shows the number of malicious behavior occur in the network before implementing DRPGAC algorithm and after implementing DRPGAC algorithm. In order to detect malicious node the ID, key of each node is verified while transmitting and receiving a data packet. The proposed system maintains and compares a DB to compare the ID, key for each node in the network. When a node is detected as malicious then the node is blocked. The malicious is reduced 10% lesser than the existing approach because DRPGAC provide more preventing instead of detection.

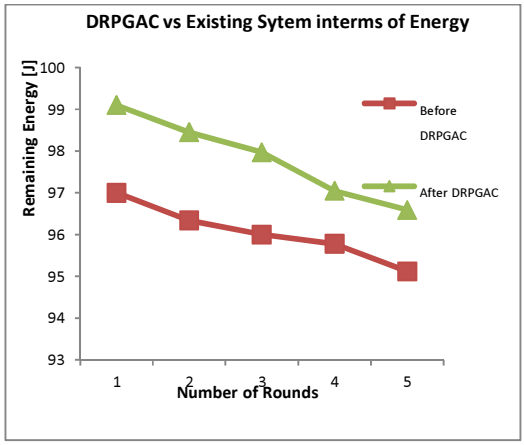

Figure-4: DRPGAC Vs. Existing System Comparison In Energy

Figure-4 shows the remaining energy of each round where the number of nodes deployed is 10, 20, 30, 40 and 50. It shows that the DRPGAC approach has longer life time then the existing system. This is because of unwanted node communication and data transmission is

Journal of Theoretical and Applied Information Technology
10th November 2014. Vol. 69 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

avoided by key comparison. Since nodes cant transmit data if they are not submitting valid ID and valid key and energy remains the same. The energy remains of the existing system in the 5th round is 95.12% where the remaining energy of DRPGAC in the 5th round is 96.59%. Hence DRPGAC saves more energy than the existing system.

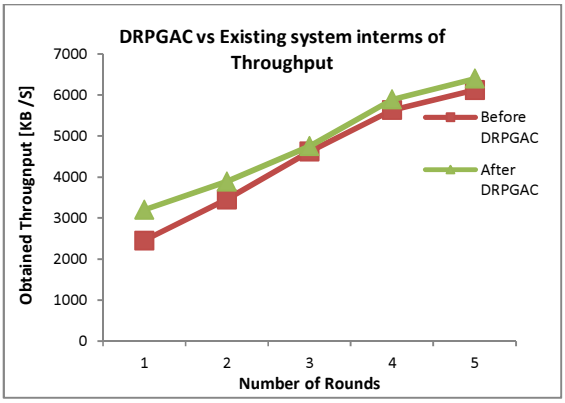

Figure-5: DRPGAC Vs. Existing System Comparison In Throughput

The data transmission successfully is sending and receiving is named as throughput. The obtained throughput using DRPGAC is better than the existing approach. Since more malicious activities occur in existing system, it spoils the data success transmission. Figure-5 shows the obtained throughput of each round. The throughput obtained by the existing system in the 5th round is 6123 packets where the DRPGAC obtained in the 5th round is 6400 packets. Hence DRPGAC obtained better throughput than the existing system.

The time taken to transmit the complete data packet from source to destination [in a route] is computed and shown in Figure-6. The time taken by DRPGCA is lesser than the existing system and which can be obtained by deploying before and after DRPGCA in the simulation. Figure-6 shows that the delay taken for transmission in each round. DRPGAC takes less time than the existing approach. The Existing approach takes 18, 27, 31, 39 and 46 ms time for each round where the DRPGAC takes 12, 15, 19, 23 and 26 ms time for each round. Totally five rounds and the number of nodes deployed are 10, 20, 30, 40 and 50 nodes.

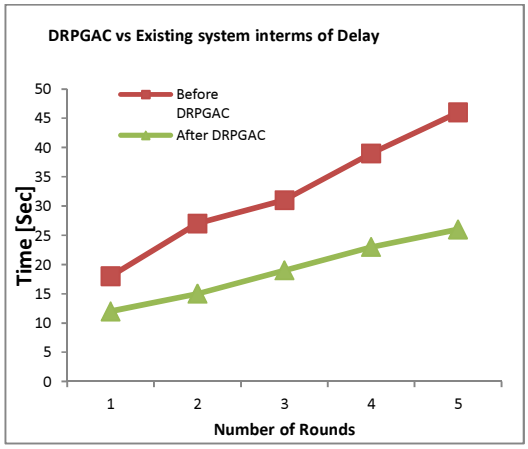

Figure-6: DRPGAC Vs. Existing System Comparison In Delay

In terms of throughput, DRPGCA is compared with various existing routing protocols is shown in Figure-7. Throughput obtained by DRPGCA is 23.45%, 36.78%, 43.21%, 54.32% and 67.89% for 10 node, 20 node, 30 nodes, 40 nodes and 50 nodes respectively. Throughput obtained by SER is 23.09%, 36.12%, 42.98%, 54.04% and 67.10% for 10 node, 20 node, 30 nodes, 40 nodes and 50 nodes respectively. Throughput obtained by LBIDS is 23.23%, 36.39%, 43.10%, 55.19% and 67.37% for 10 node, 20 node, 30 nodes, 40 nodes and 50 nodes respectively. Throughput obtained by EESRP is 23.10%, 36.58%, 43.19%, 54.28% and 67.58% for 10 node, 20 node, 30 nodes, 40 nodes and 50 nodes respectively. DRPGCA obtains maximum throughput when compared with existing protocols.

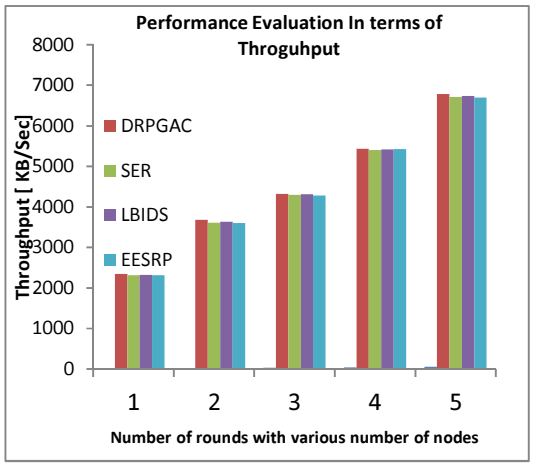

Figure-7: Performance Evaluation Of DRPGAC In Terms Of Throughput

Journal of Theoretical and Applied Information Technology
10th November 2014. Vol. 69 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Packet delivery ratio is also compared with various existing routing protocol and it is shown in Figure-8. PDR obtained by DRPGCA is 29%, 37%, 48%, 54% and 65% for 10 node, 20 node, 30 nodes, 40 nodes and 50 nodes respectively. PDR obtained by SER is 26%, 32%, 42%, 50% and 60% for 10 node, 20 node, 30 nodes, 40 nodes and 50 nodes respectively. PDR obtained by LBIDS is 27%, 34%, 45%, 52% and 62% for 10 node, 20 node, 30 nodes, 40 nodes and 50 nodes respectively. PDR obtained by EESRP is 28%, 35%, 47%, 53% and 64% for 10 node, 20 node, 30 nodes, 40 nodes and 50 nodes respectively. When compared with existing protocols, DRPGCA obtains high PDR.

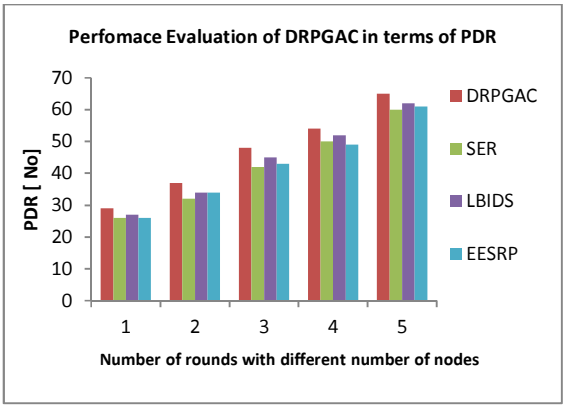

Figure-8: Performance Evaluation Of DRPGAC In Terms Of Throughput

6. CONCLUSION

DRPGCA technique is derived from an existing LBIDS approach and it is used to verify the mutual authentication among the pair of nodes, going to transmit and receive their data.

Since DRPGCA uses the unique ID from random generation method combined with node type and serial number of the node, it is a novel mechanism to create Node-ID and it makes proper authentication for nodes and it cannot be duplicated by malicious node.

The output of the DRPGAC approach much more useful to the Wireless Networks based applications. This approach improves the quality of the network. The ID, Key comparison steps are preprocessing approach in a network to make the network is a trustable network and provides protection to the network. DRPGAC simulation has proved that it is a general solution which prevents the data from malicious people by transfer the data only to the authorized people. This approach can produce good result in over-sized network also. DRPGAC can give security without affecting the network quality in terms of throughput, energy and delay.

6.1.LIMITATIONS

- ✓ There is no scalability in device type.
- ✓ Data level security is also needed
- ✓ Maintenance level security is needed

REFERENCES:

[1]. Alexander G. Tartakovsky, , Aleksey S. Polunchenko, and GrigorySokolov, "Efficient Computer Network Anomaly Detection by Changepoint Detection Methods" IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, VOL. 7, NO. 1, FEBRUARY 2013

[2]. Yun Wang, Weihuang Fu, and Dharma P. Agrawal, Life Fellow, "Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 2, FEBRUARY 2013

[3] Chun-Jen Chung, PankajKhatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013

[4] Francisco Maciá-Pérez, Francisco J. Mora-Gimeno, Diego Marcos-Jorquera, , Juan Antonio Gil-Martínez-Abarca, Héctor Ramos-Morillo, and Iren Lorenzo-Fonseca, "Network Intrusion Detection System Embedded on a Smart Sensor", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 58, NO. 3, MARCH 2011

[5] Salvatore Pontarelli, Giuseppe Bianchi, and Simone Teofili," Traffic-Aware Design of a High-SpeedFPGA Network Intrusion Detection System", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 11, NOVEMBER 2013.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, Mostafa M. Fouda, "An Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks", IEEE Network Magazine, vol. 27, no. 3, pp. 51-56, May-June 2013.

[7] CHUN-HAO LO and NIRWAN ANSARI, "CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid", VOLUME 1, NO. 1, JUNE 2013

[8] Adnan Nadeem, and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013

[9] Robert Mitchell and Ing-Ray Chen, "Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications" IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS

[10] Frank Jiang, Daoyi Dong, Longbing Cao, and Michael R. Frater, "Agent-Based Self-Adaptable Context-Aware Network Vulnerability Assessment" IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 10, NO. 3, SEPTEMBER 2013

[11] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C. Green II, and MansoorAlam, "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids", IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011

[12] IginoCorona , Giorgio Giacinto,FabioRoli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues" 2013 Elsevier Inc

[13] HeshanKumarage, Ibrahim Khalil a, ZahirTari , Albert Zomaya, "Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modeling" 2013 Elsevier Inc.

[14] PanosLouvieris, NatalieClewley,XiaohuiLiu, "Effects-based featureidentificationfornetworkintrusiondetection" 2013 Elsevier B.V.

[15] Georgios P. Spathoulas, Sokratis K. Katsikas, "Enhancing IDS performance through comprehensive alert post-processing" Elsevier Ltd

[16] Reda M. Elbasiony ,Elsayed A. Sallam , Tarek E. Eltobely , Mahmoud M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means", 2013 Ain Shams University.Production and hosting by Elsevier B.V.

[17] JunaidArshad, Paul Townend, JieXu, "A novel intrusion severity analysis approach for Clouds" 2011 Elsevier B.V.

[18] ChiragModi, DhirenPatel, BhaveshBorisaniya, HirenPatel, Avi Patel, MuttukrishnanRajarajan, "A survey of intrusion detection techniques in Cloud", 2012 Elsevier Ltd.

[19] ShahidRaza, Linus Wallgren, Thiemo Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things". 2013 Elsevier B.V.

[20]. UdayaSuriyaRajkumar, D. and RajamaniVayanaperumal, "A LEADER BASED MONITORING APPROACH FOR SINKHOLE ATTACK IN WIRELESS SENSOR NETWORK", Journal of Computer Science 9 (9): 1106-1116, 2013.