A novel scheme to Identify Intrusions by using ASVM Algorithm in WSN

S. Ramesh[1]
Research Scholar,
Manonmaniam Sundaranar University,Tirunelveli, T.N, India
ramesh20062000@gmail.com

Dr. H. Abdul Rauf [2]
Dean & Professor, Department of CS & IT
Sri Sastha Institute of Engineering and Technology, Chennai, T.N, India
harauf@yahoo.com

Dr. S.P. Victor [3]
Dean of Science & Associate Professor of Computer Science
St. Xavier's College, Palayamkottai, T.N, India
drspvictor@gmail.com

Abstract: Due to the enormous development of network expertise and also the significant growth in hacking tools and new attacking methods, the Wireless Sensor Networks (WSN) is in need to identify intrusions efficiently and effectively. Wireless Sensor Networks (WSNs) consist of sensor nodes deployed in a manner to collect information about surrounding environment. The limitations such as distributed nature, multi hop data forwarding, limited battery life time, memory space, computing capability and open wireless medium are the factors that make WSNs highly vulnerable to security attacks at various levels. Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing security attacks. This paper presents current Intrusion Detection Systems and some open research problems related to WSN security. In this paper we propose a new Advance Support Vector Machine Algorithm (ASVM) to eliminate the existing drawbacks. Through the ASVM algorithm we can prevent malicious attacks and the overall system acts as Intelligent Intrusion Detection System (IIDS). The ASVM is used as a set of training mechanism which invoke Network security to monitor and alert the malicious entry in WSN. Through the ASVM algorithm we can find malicious nodes by identifying misbehaviour in the data report.. The ASVM algorithm is experimented using an experimental setup. The test result shows that our proposed algorithm can give an effective intrusion detection performance with reduced amount of network load.
Keywords: WSN, MANET, IIDS, ASVM, VoIP

1. Introduction

Wireless Sensor Networks (WSN) have been widely used in various monitoring applications including virtual fencing. With the integration of Internet of Things (IoT) in which millions of devices, systems and services will be interconnected online, it brings high capabilities for sensing, intercommunication and actuation. The Internet of Things (IoT) is a heterogeneous network of objects that communicate with each other and their owners over the Internet. [1]

The IoT standards must exhibit efficient self-reliant management and monitoring capability, which in a hierarchical topology is the role of cluster heads. IoT standards must be robust, scalable, adaptable, reliable, and trustworthy. These criteria are predicated upon the limited lifetime, and the autonomous nature, of wireless personal area networks (WPANs), of which wireless sensor networks (WSNs) are a major technological solution and research area in the IoT.[2]

To safeguard networks, unauthorized intruders must be detected within the constraints of each type of device or subnetwork before any system information can be disseminated. To understand and illustrate IDS platform differences and the current research trend towards a universal, cross-platform distributed approach, the survey starts with an historical examination of intrusion detection systems.[4]

Wireless Sensor Networks development has always been driven by the complexity and diversity of modern military applications. From simple intrusion detection to complex border surveillance and monitoring integrated systems, target location and tracking, WSNs have been included in all types of military scenarios. Military live simulation systems are part of complex integrated tactical training environments used by many military powers, including North Atlantic Treaty Organization (NATO) joint armed forces, and, in the past few years, they have begun to show their technical limitations and also given alternatives for a military live simulation training system.[5]

Data transfer rate is more in wireless networks as compared to wired networks. Wireless networks are of more advantages because its support feature such as versatility, portability, open medium, simple to design. MANETs and WSN are the most common forms of Wireless media. In MANETs, nodes are deployed or distributed in Ad-hoc way and they are Communicating or exchanging messages using wireless Transmission. Security is an important concern in Mobile Ad-hoc Networks because MANETs having wide distribution are vulnerable to more malicious attackers.[6]

2. Literature Survey

In 2011, **Mohsen Estiri, Ahademzadeh** et al. concluded that they look at the issue of security in WSN based on the approach of game theory. WSNs are established on the nature of strategic interactions among nodes. So game theory can be an applicable approach for this area. The paper presents a game-theoretical model to detect intrusions and leading to a defence strategy for the WSNs. Here the authors proposed a new novel repeated game theoretical model to periodically punish a malicious node, and try to exploit the malicious node in favour of improving overall throughput of wireless sensor network.

In 2012, **Almir Davis, Hwa Chang** et al. concluded that an airport Perimeter Intrusion Detection System (PIDS) based on a custom designed wireless sensor network architecture. The sensing part of the network is based on accelerometers capable of detecting events such as fence climbing, fence shaking and fence kicking. The proposed security system was comprehensively tested in the simulation environment and in the open field. The open field testing proved the major concepts of the system's architecture on a small scale. The next step in the research is to expand field testing to larger areas such as to a 300 feet long chain-link fence populated with about 100 sensors per network line. The goal is to further test the reliability and soundness of the network as well as to observe the environmental impact on the network.

In 2012, **Elvni Darra, Sokratis K.Katsikas** et al. concluded that they reviewed several approaches for intrusion detection in wireless sensor networks and attributed attack detection capabilities. The paper presents that currently available proposals for intrusion detection systems for WSNs appear to be incapable of detecting a wide range of possible attacks against WSNs.

In 2013, **Amara korba Abdelaziz, Mehdi Nafaa,** et al. concluded that all routing security issues to which MANETs are vulnerable are being presented. A classification of security threats gathering selfish behaviours and malicious attacks was proposed.

In 2014, **H.T Chan, T.A.Rahuman, A.Arsad** et al. concluded that the influence of azimuth angle, height, sensitivity level, indoor and outdoor environment on the maximum sensing range of virtual fence unit has been investigated. It is found that virtual fence unit can detect movement in longer distance when it is at 0º azimuth angle, at 30cm height and in indoor

.environment. Maximum sensing range will not be affected by increased sensitivity level if it is already at its maximum value. This paper also shows that virtual fence indoor system using microwave motion detector for indoor environment could not be used in outdoor environment.

In 2015, **Audrey Ann Gendreau** et al. concluded that the energy efficiency of a virtual topology derived from an enhanced cluster head selection algorithm for situation awareness in the IoT was thoroughly tested. It showed positive results.

In 2015, **Aswathy Balakrishnan, Rino PC** et al. concluded that an anomaly detection algorithm specifically designed for cluster-based wireless sensor networks. A novel, method was defined to secure the algorithms cluster formation protocol. The tested results showed that the proposed algorithm achieves high detection accuracy.

In 2016, **Constantin Grumazescu, Valentin-Alexandru Vladuta,** et al**.** concluded that a wireless sensor network is the appropriate solution to solve several implementation issues – NLOS effects, bulky and heavy man worn equipment, low data rate, communication system deployment, high initial and maintenance costs and also presented a series of additional useful features of a future live simulation system that could be implemented by integrating many applications.

3. Objective

A significant amount of research work has been carried out in the field of intrusion detection in wireless sensor networks. Many research papers proposed a number of appropriate methods, and it is not an easy task to select the right method for Intrusion Detection in Wireless Sensor Networks. Moreover, security is one of the major significant challenges for wireless sensor networks because of their deployment in open medium and unprotected environment. As the past mechanisms such as cryptographic mechanisms are not enough to protect wireless sensor networks from external attacks, Intrusion Detection System (IDS) needs to be improved. So we propose to develop an effective, efficient novel scheme to identify intrusions by using ASVM algorithm in WSN.

4. Proposed Work

The number of intrusions are going on increasing even though, a large amount of research has been carried out in the field of intrusion detection in WSN. The paper deals with the security aspect of these IPv4-based WSNs. The proposed distributed system for malicious node detection in the IP-based WSN tends to satisfy these requirements as much as possible. It provides the possibility of connecting these sensor networks to IP based network architecture without the intermediate modules such as gateways or proxies. Unlike version 4, among other interesting features, this new IPv6 protocol offers the possibility of using extended addressing and therefore it is able to provide global reach ability to the huge number of new connected devices.

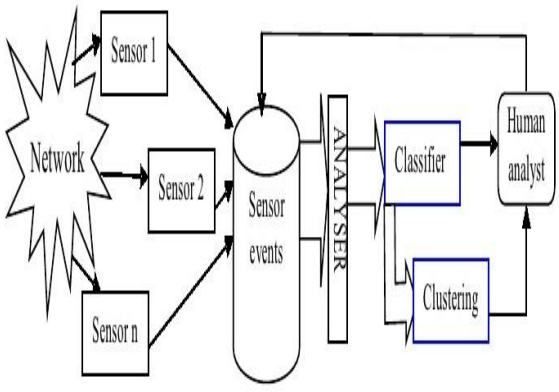

Fig:1 WSN IDS Architecture

An IDS is a device or software application that monitors systems or networks or systems for malicious activity or policy violations. Any detected abnormal activity or violation is typically reported to the administrator. An Intrusion Detection System (IDS) includes a collection of tools, methods, and resources to identify, assess, and report intrusions. Intrusion detection is typically one part of an overall protection system that is installed around a system or device and it is not a stand-alone protection measure. Intrusion is defined as "any set of actions that attempts to compromise the integrity, confidentiality, or availability of a resource.

Basically WSN networks are composed of randomly distributed collection of wireless sensors. The wireless sensors create multiple protocols for relaying detection information. The increased cluster heads within the sensor delivery area and also the increasing the transmission range of every nodes, reduces energy consumption while tracking an intrusion. So we propose a new Advance support vector machine algorithm (ASVM) to eliminate the existing drawbacks such as active and passive attacks because of its open medium, fast changing topology, lack of centralized monitoring system etc. and also they can only detect the intrusions only as per limited assumptions. Our main focus is to detect internal attacks, there is no proper implementation for internal attack, so the existing technology is not fair. Intrusion detection system (IDS) is used to monitor the malicious traffic in a particular node or network. But there is much challenge to implement the IDS in sensor Networks. Through the ASVM algorithm we can find abnormal packets based on its false misbehaviour data report and detect abnormal IP addresses and give alarm.

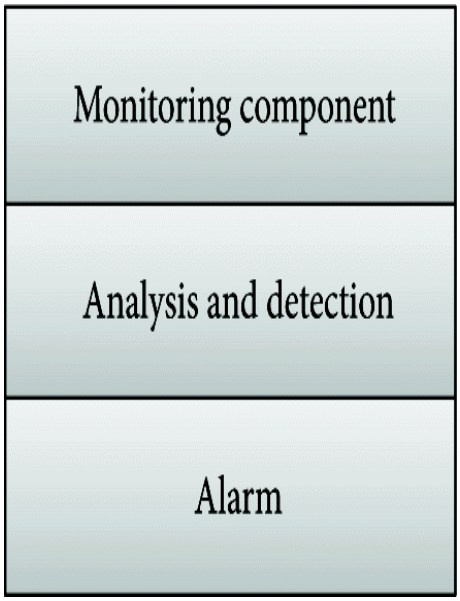

Fig: 2 The IDS three main components

Monitoring component is used for local events monitoring as well as monitoring the neighbours. This component mostly monitors traffic patterns, internal events, and resource utilization. Analysis and detection is the main component which is based on modelling algorithm. Network operations, behaviour, and activities are analyzed, and decisions are made to declare them as malicious or not. Alarm component is a response generating component, which generates an alarm in case of detection of an intrusion. It should be noted that IDSs are passive in nature and can only detect intrusion. They cannot take any preventive actions but they can generate an alarm.

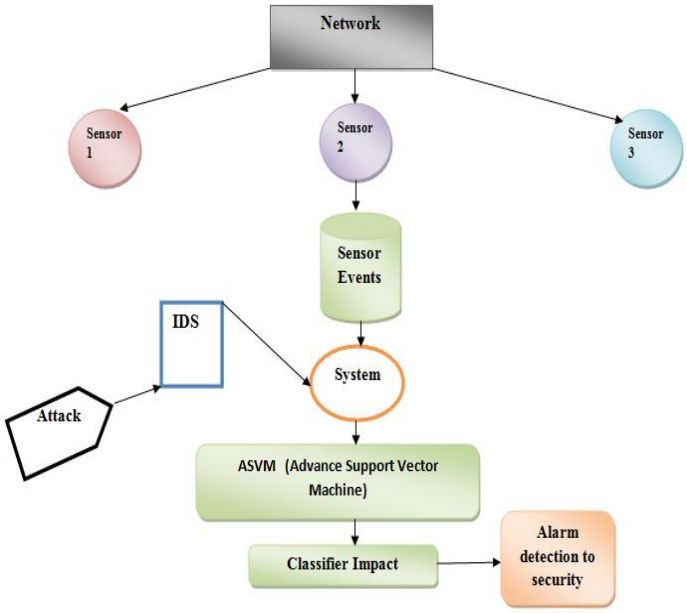

Fig: 3 ASVM Block diagram

In this proposed algorithm the block diagram showing the architectural design ASVM over WSN is given in the figure 3.

The network part in Fig 3 divides and distributes the operations to three different sensors. Due to this sensor classification the overall system runs faster for example it acts like Queue to reach destination faster. Sensor events which perform data collecting agent from sensors nodes in FIFO concept to receive the data. The external attack which arrives suddenly without any intimation which collapse the overall network topology so to avoid this situation we ensure the ASVM algorithm which plays a role like to stop the attack and alert the overall system.

The "Advance Support Vector Machine" (ASVM) is a supervised machine learning algorithm which can be used for both classification and regression challenges. However, it is mostly used in classification problems. In this proposed algorithm, we separate the normal and abnormal IP based data flow in network topology. Then, we perform classification by finding the attack plane. The Classifier acts like trigger mechanism to alert the system from the intrusion.

5. Design and Implementation

The enhanced Advance Support Vector Machine Algorithm (ASVM) is to eliminate the existing drawbacks and also it can prevent malicious attack in Mobile Adhoc Networks (MANET), so the overall system acts as Intelligent Intrusion Detection System (IIDS). The ASVM is used as a set of training mechanism which invoke in Network security area to monitor and alert the malicious entry in WSN ASVM. In real intrusion detection datasets the features classified in normal IP and Abnormal IP data set to detect the intrusion. The usual outline of scheme performance is efficient because the scheme learns the IP based performance. This type of scheme can notice unidentified attack but it exhibit high false positive rate.

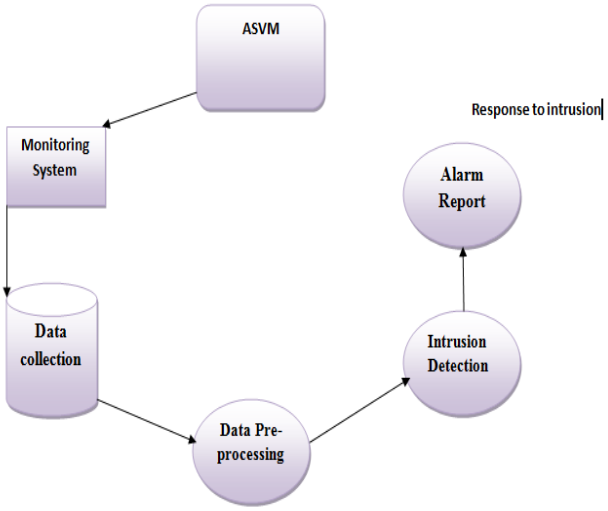

Fig: 4 ASVM cyclic flow diagram

Our ultimate aim is to bring the proposed ASVM algorithm flow which ensures efficient monitoring system as per node to node communication. Then by collecting data it analyzes and predicts the behaviors of users and then these behaviors will be distinguished as an attack or a normal behavior. We use IP based MAC address with Advance Support Vector Machine algorithm to detect network intrusions.

First, packets are captured from the Networks, SVM is used to pre-process the data and reduce the dimensions in IDS. The features selected by data pre-processing will be sent to SVM model to learn and test respectively. The method is effective to decrease the space density of data. The experiment results show that it could reduce the false positive rate and increase the accuracy and generate alarm report.

1: procedure ASVM_ Force (x, y, z, n)
//Input:
//x=array of m bytes representing the keyword
//y =integer representing the keyword length
// z= array of n bytes representing the book contribution
// n= distance between nodes
2: for j = 0 to n − m do //every quality in y
3: i = 0
4: while i < n and x[i] = y [i + j] do
5: i = i + 1 // i = add up of corresponding
6: end while
7: if i>= m then
8: output j
9: end if
10: end for
11: end process

Classification is used to determine the predetermined output. It predicts the target class for each data item. Instantly it recognize the intrusion as low, high, medium. Based on the training set which matches with the parameters of nodes with IDS technology along with ASVM algorithm, we can predict the results.

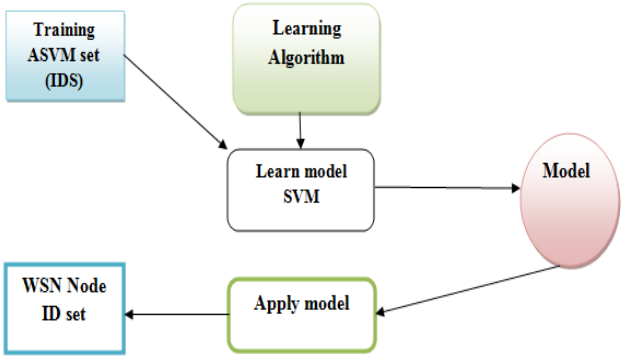

Fig: 5 ASVM classification diagram

The support vector machine acts as model for IDS in WSN nodes to develop the overall security system. ASVM uses a high dimension space to find a hyper-plane to perform binary classification, where the error rate is minimal. The IP based ASVM is trained by using reduced dataset, to find several support vectors that represent the training data. By using this model, the ASVM will classify the given unknown data and predicts the data as normal or abnormal.

In this paper we suggest a new model for IDS which concentrate on reducing power consumption of sensor nodes by distributing the work of intrusion detection to different sheet nodes with the help of security based network management system. We separated each area of sensor nodes into hexagonal region (like IDS cells). Sensor nodes in each of the hexagonal area are monitored by a cluster node. Each combined node will be monitored by a local node then, the regional nodes will be further monitored by the Base station.

6. Experimental Results

ASVM defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. When Abnormal IP enters in the IDS the IDS will filter the abnormal packets. When the number of malicious nodes increased, packet delivery system gradually slowed down. The tests are conducted based on the IP to distinguish the normal and abnormal IP's. The results were shown in table 3.

S.No	Time (ms)	Bytes	IP	Normal IDS IP	Abnormal IDS IP
1	12:31:111	74	192.168.1.1	192.168.1.1	
2	12:32:112	74	192.168.1.2	192.168.1.2	
3	12:33:114	74	192.168.1.3	192.168.1.3	
4	12:34:115	74	192.168.1.4		192.168.1.4
5	12:35:116	74	192.168.1.5	192.168.1.5	
6	12:36:117	74	192.168.1.6	192.168.1.6	
7	12:37:118	74	192.168.1.7		192.168.1.7
8	12:38:119	74	192.168.1.8	192.168.1.8	

Table: 1 Intrusion identification based on IP

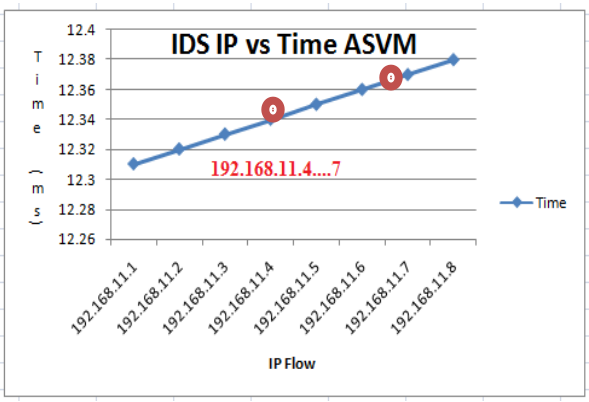

Fig: 6 Graph Analysis Flow over IDS

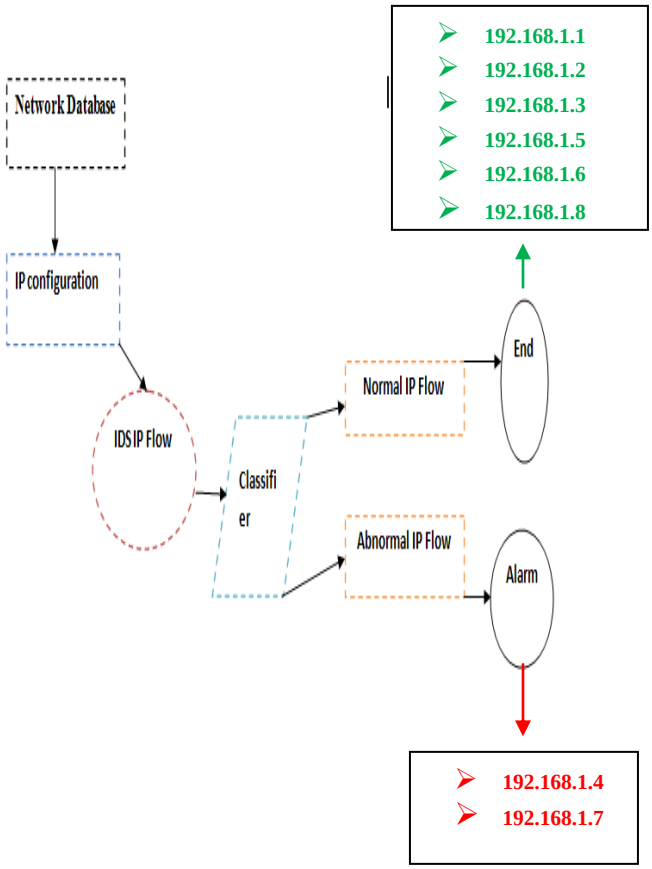

Fig: 7 Intrusion Identification Diagram based on IP

9. Conclusion

Security is the most important anxiety for WSN researchers and designer because of its serious applications in different environments. In this paper we discuss the security issues, a variety of security attacks and their counter measures. So we analyzed the review of recent work on dissimilar approaches of IP based IDS for WSN. It has been experimented that these intrusion detection systems are not sufficient for defensive WSN from intruders professionally. We found various IDS approaches to detect those internal malicious attacks. Those approaches have

some limitations for the detection of attacks. Still proper solutions can be implemented to detect internal attacks of WSN Networks. We hope our proposed real time solution will greatly help to detect internal malicious attacks. Here we presented an ASVM algorithm and implemented. The results were shown in the above figures and tables. From these results it is clear that our proposed method provides a good solution.

10. Future work

A real time Intrusion Detection system for Wireless Sensor Networks using ASVM system is examined. In future this algorithm may be improved to get better performance.

11. Reference

[1] H. T Chan, T.A Rahman, and A. Arsad "Performance study of virtual fence unit using Wireless Sensor Network in IoT environment." 2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS).

[2] Audrey Ann Gendreau. "Situation Awareness Measurement Enhanced for Efficient Monitoring in the Internet of Things. 2015 Pages: 82 - 85, DOI: 10.1109/TENSYMP.2015.13

[3] Audrey A. Gendreau, Michael Moorman, "Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things" 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) 2016 Pages: 84-90, DOI: 10.1109/FiCloud .2016.20

[4] Constantin Grumazescu, Valentin-Alexandru Vladuta, and Georgiana Subasu. "WSN solutions for communication challenges in military live simulation environments" 2016 International Conference on Communications (COMM) Pages: 319 - 322, DOI: 10.1109/ICComm.2016.7528266

IEEE Conference Publications

[5] Sharad Awatade, Shweta Joshi "Improved EAACK: Develop secure intrusion detection system for MANETs using hybrid cryptography" 2016 International Conference on Computing communication Control and automation (ICCUBEA) Year: 2016 Pages: 1 - 4, DOI: 10.1109/ICCUBEA.2016.7860076

[6] Aswathy Balakrishnan, Rino PC "A Novel Anomaly Detection Algorithm for WSN" 2015 Fifth International Conference on Advances in Computing and Communications (ICACC) Year: 2015 Pages: 118 - 121, DOI:10.1109/ICACC.2015.29

[7]. Amara Korba Abdelaziz, Mehdi Nafaa, and Ghanemi Salim "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks" 2013 UKSim 15th International Conference on Computer Modelling and Simulation Pages: 693 - 698, DOI: 10.1109/UKSim.2013.48

[8]. Almir Davis, Hwa Chang "Airport protection using wireless sensor networks" 2012 IEEE Conference on Technologies for Homeland Security (HST) Year: 2012 Pages: 36 - 42, DOI: 10.1109/THS.2012.6459823

[9]. Eleni Darra, Sokratis K. Katsikas "Attack detection capabilities of intrusion detection systems for Wireless Sensor Networks" IISA 2013 Pages: 1 - 7, DOI:10.1109/IISA.2013.6623718

[10]. Mohsen Estiri, Ahmad Khademzadeh "A game-theoretical model for intrusion detection in wireless sensor networks" CCECE 2010 Pages: 1 - 5, DOI: 10.1109/CCECE.2010.5575157

[11]. T. Eswari, V. Vanitha "A novel rule based intrusion detection framework for Wireless Sensor Networks" 2013 International Conference on Information Communication and Embedded Systems (ICICES) Pages: 1019 - 1022, DOI: 10.1109/ICICES.2013.6508172

[12] A. Babu Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, and Al-Sakib Khan Pathan "A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks" 2014 3rd International Conference on Eco-friendly Computing and Communication Systems Pages: 95 - 98, DOI: 10.1109/Eco-friendly.2014.94

[13]. Alexandre Mouradian, Isabelle Auge Blum "Formal Verification of Real-Time Wireless Sensor Networks Protocols: Scaling Up"2014 26th Euromicro Conference on Real-Time Systems Pages: 41 - 50, DOI: 10.1109/ECRTS.2014.12

14]. Qi Guo, Xiaohong Li, Zhiyong Feng, and Guangquan Xu “MPOID: Multi-protocol Oriented Intrusion Detection Method for Wireless Sensor Networks” 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems Pages: 1512 - 1517, DOI: 10.1109/HPCC-CSS-ICESS.2015.283
[15]. A. Babu Karuppiah, J. Dalfiah, K. Yuvashri, and S. Rajaram “An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks” International Confernce on Innovation Information in Computing Technologies Pages: 1 - 7, DOI: 10.1109/ICIICT.2015.7396103
[16]. Prachi S. Moon, Piyush K. Ingole “An overview on: Intrusion detection system with secure hybrid mechanism in wireless sensor network” 2015 International Conference on Advances in Computer Engineering and Applications Pages: 272 - 277, DOI: 10.1109/ICACEA.2015.7164714
[17]. Okan Can, Ozgur Koray Sahingoz “A survey of intrusion detection systems in wireless sensor networks” 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO) Pages: 1 - 6, DOI: 10.1109/ICMSAO.2015.7152200
[18]. Snehal Bhagat, Chandrabala P. Kothari, Vishram Bapat, Vaishali Kulkarni "Classification and determination of physical intrusion using Wireless Sensor Networks” 2015 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT) Pages: 1 - 5, DOI: 10.1109/ICCCNT.2015.7395165
[19]. A S M Ashraful Alam, David Eyers, and Zhiyi Huang “Helping secure robots in WSN environments by monitoring WSN software updates for intrusions” 2015 6th International Conference on Automation, Robotics and Applications (ICARA) Pages: 223 - 229, DOI: 10.1109/ICARA.2015.7081151
[20]. Lyes Bayou, Nora Cuppens-Boulahia, David Espes, Frederic Cuppen “Towards a CDS-based Intrusion Detection Deployment Scheme for Securing Industrial Wireless Sensor Networks” 2016 11th International Conference on Availability, Reliability and Security (ARES) Pages: 157 - 166, DOI: 10.1109/ARES.2016.48
[21]. Krishna Doddapaneni; Enver Ever; Orhan Gemikonakli; Leonardo Mostarda; Alfredo Navarra Effects of IDSs on the WSNs Lifetime: Evidence of the Need of New Approaches 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and CommunicationsDOI:10.1109/Trust Com.2012.137
[22]. Murat Gül Intrusion detection for Wireless Sensor Networks using ant colony 2016 24th Signal Processing and Communication Application Conference (SIU) Pages: 1453 - 1456, DOI: 10.1109/SIU.2016.7496024
[23]. Gauri Kalnoor; Jayashree Agarkhed Preventing attacks and detecting intruder for secured Wireless Sensor Networks 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) Pages: 1062 - 1067, DOI: 10.1109/WiSPNET.2016.7566300
[24]. Mounib Khanafer; Youssef Gahi; Mouhcine Guennoun; Hussein T. Mouftah A Review of Intrusion Detection in 802.15.4-Based Wireless Sensor Networks 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) Pages: 95 - 101, DOI: 10.1109/CSCloud.2016.32
[25]. S. Shanthi; E. G. Rajan Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks 2016 2nd International Conference on Next Generation Computing Technologies (NGCT) Pages: 426 - 431, DOI: 10.1109/NGCT.2016.7877454
[26]. Muhammad Usman; Vallipuram Muthukkumarasamy; Xin-Wen Wu; Surraya Khanum Wireless Smart Home Sensor Networks: Mobile Agent Based Anomaly Detection 2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing Pages: 322 - 329, DOI: 10.1109/UIC-ATC.2012.145
[27]. Udaya Suriya Rajkumar D; Rajamani Vayanaperumal Detecting and revocation the compromised node in zone - based wireless sensor network using a two stage approach 2014 Sixth International Conference on Advanced Computing (ICoAC) Pages: 7 - 13, DOI: 10.1109/ICoAC.2014.7229747
[28]. M. Surendar; A. Umamakeswari InDReS: An Intrusion Detection and response system for Internet of Things with 6LoWPAN 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) Pages: 1903 - 1908, DOI: 10.1109/WiSPNET.2016.7566473
[29]. Qixiang Yu; Zhenxing Luo; Paul Min Intrusion detection in wireless sensor networks for destructive intruders 2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA) Pages: 68 - 75, DOI: 10.1109/APSIPA.2015.7415410
[30]. Ting Sun; Xingchuan Liu Agent-based intrusion detection and self-recovery system for wireless sensor networks 2013 5th IEEE International Conference on Broadband Network & Multimedia Technology Pages: 206 - 210, DOI: 10.1109/ICBNMT.2013.6823943