Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

# Detection of Intrusion through Big data Analytics for Wireless Sensor Networks

[1]Anitha J, [2]Anil Kumar B

**Abstract**

Wireless Sensor Networks are vulnerable to network attacks compared to any other network. WSNs are resource constraints in form of energy and computational resources. With these limitations Intrusion Detection is a challenging approach to equip WSN. However, the Big Data across today's networks has less security with respect to various resources available in the WSN, to work out a collaborative solution to equip such resource poor networks with an ability to detect and fight against intrusions. WSNs are severely memory constrained which makes misuse-detection based IDSs in WSNs difficult to implement, as they need to store attack signatures.

Keywords: Big Data, Intrusion Detection. Sensor Networks, Attack Patterns

## Introduction

Big data with a backbone of cloud computing is the state of art method to offload considerable computation requirements from both data centers and terminal sensing devices. These are all the more lucrative due to the inherent qualities of flexibility and scalability[1]. However, cloud computing may not be directly suitable for all applications such as WSN (Wireless Sensor Network) for its high requirement on real time latency, immediate response requirements which may be associated with geographic mobility. For WSN, area of operation is in the physical world, while cloud computes towards the edge of the network.

Big Data is a large-scale information management and analysis technology. Big Data can be differentiated in four ways:

- The amount of data (volume).
- The rate of data generation and transmission (velocity).
- The types of structured and unstructured data (variety).
- The Data Variability

Big Data technologies can be divided into two groups: batch processing, which are analytics on data at rest, and stream processing, which are analytics on data in motion.

Intrusion Detection Scheme (IDS) schemes have been implemented in wired and semi-wired networks. These systems look for certain misbehaviour patterns in the network which would give a whiff of a malicious act and thereby trigger attack mitigating mechanism. WSNs have an inherent drawback of limited resource availability in form of energy as well as computing capabilities. IDS thus have a significant contribution towards Detecting malicious nodes in WSNs from both internal and external attacks. [1]An IDS would look for an anomaly in node behaviour and once found would re-configure the network to by- pass the malicious node and thus prevent a network attack.

Wireless sensor networks have found rapidly growing applications in areas such as environmental monitoring, automated data collection and surveillance. One of the significant uses of sensor networks is the tracking of a mobile target (point source) by the network. Mobile target tracking has a number of sensible applications, including search-rescue, wildlife monitoring, robotic navigation and autonomous surveillance. To keep check on movement of suspicious people and activities monitored using surveillance, tracking system and video monitoring. Usually, target tracking involves two steps. At first, it needs to estimate or predict target positions from noisy sensor data

measurements. Then, it needs to control mobile sensor tracker to follow or capture the moving target. As a result the problem of mobile target positioning in a sensor network consists of stationary sensors and a mobile sensor.

***Material and Methodology***

The concept of alert Correlation in Distributed Environment for developing the cloud and Big data based IDS for WSN was [1] proposed by Suresh Chandra Satapathy etal .[2] The method intend to use a Big data based fuzzy logic algorithm, which would help in identifying intrusions through pattern matching and thereby reduce false alarms. Fuzzy logic dealing with vagueness and imprecision has a capability to represent exact forms of reasoning in areas where firm decisions have to be made characterized This is found to be appropriate for intrusion detection.

The detection schemes used to detect an intruder in a WSN environment are single-sensing detection and other is multiple or k-Sensing detection. In the first type, intrusion detection model, intruder must be recognize by a single sensor in a WSN domain. On the other side, in k-sensing detection, an intruder will be recognized from the collaboration of the k sensors (k is defined by the specific application requirements).The sensed information given by a single sensor might not be efficient for identifying the intruder.

Proposing a new technique of energy efficient intrusion detection, which maximize the network life time and its probability analysis considering the static sensors. The intruder is considered as a moving object and every node has Omni antenna properties for sensing. [6]The sink node knows each nodes location and its neighbor list. The algorithm is implemented at the sink node and its sends packet to the selected nodes to activate its IDS module.

***Research Methodology***

The proposed research work is to analyze the data provided through the various sensors in the wireless sensor network. Identify and detect the malicious node through IDS and bypass the malicious node from the network attack. The IDS detection is based on Anamoly detection by comparing the action or the behaviour of the node data bank and attack patterns. To provide security to the data through cryptographic algorithm and also provides reliability and robustness.

Analysing the possible problems associated with Big data Analytics for Intrusion Detection in heterogeneous wireless sensor networks and evaluate the status of current standardization and available devices. Data Collection from various sources and studying various research papers in this field. [8]Developing a framework to detect the malicious node from the big data analytics and evaluate wireless sensor network deployments with respect to the average number of sensor nodes, transmission range. Designing the simulating module to evaluate the performance metrics related to energy efficiency. Comparing the performances with the Single sensing detection with the multiple sensing detection for Big data analytics in wireless sensor networks.

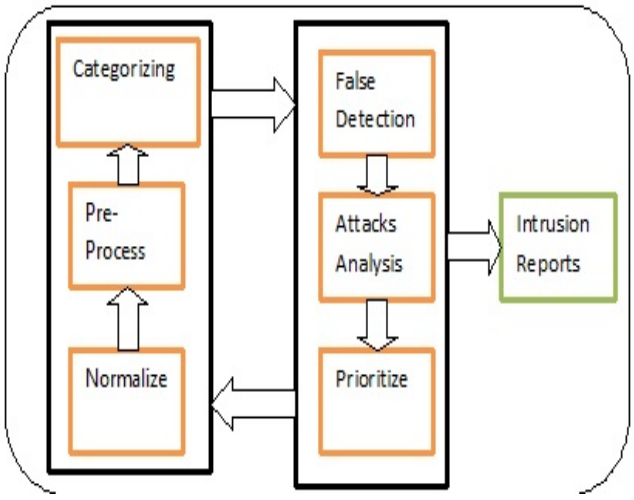


**Figure 1 : IDS Model**

Normalize : The data from the network with regards to threats and anomalies is normalized. The data from the cluster head comprises of dynamic fields like date and time stamp, username, port used, IP addresses of the source and destination etc.

Preprocessing : The main task of pre-processing component is providing alerts with missing fields which are necessary for other correlating components.

Categorize: The similar events are categorized together and the nature of occurrence on attacks at a certain time interval is studied.

Correlation :The performance of Correlation depends on combining the three tasks of normalization, preprocessing and categorization. The key step for selecting a method for correlation process is to consider nature of environment followed by more ability for reception of alerts, trace of tracks, preparation logs with simple entities and trace of events with such entities.

False Detection : [1]This component is tasked with the responsibility of distinguishing between false positive and true positive alerts. Different sensors have their own advantages and disadvantages in various attacks detection and this is a famous bottleneck for low-level sensors to generate lots of false positive alerts.

Attack analysis: The attack strategy analysis tries to comprehend the real intentions of invaders

## Conclusion

This Paper Analyses the possible problems associated with Big data Analytics for Intrusion Detection in heterogeneous wireless sensor networks and evaluate the status of current standardization and available devices through the analysis of the available technology cloud, Big data ,IDS and their applicability in WSN.

### References

[1] Pritee Parwekar & Suresh Chandra Satapathy (2015) , CSI Communications, "Leveraging Bigdata Towards Enabling Analytics Based Intrusion Detection Systems in Wireless Sensor Networks"

[2] F. Raza, S.Bashir, K. Tauseef and S. I. Shah 2015 12th International Bhurban Conference on Applied Sciences & Technology (IBCAST) "Optimizing nodes proportion for Intrusion Detection in Uniform and Gaussian distributed Heterogeneous WSN"

[3] Fu Xiao, Chongsheng Zhang and Zhijie Han (2013), "Big Data in Ubiquitous Wireless Sensor Networks".

[4] Fu Xiao, Chongsheng Zhang and Zhijie Han (2013),"An approach based on chain key predistribution against Sybil attack in wireless sensor networks"

[5] Yun Wang, Weihuang Fu, and Dharma P. Agrawal , " Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Net- works", IEEE transactions on parallel and distributed systems, vol.24, no.2 February 2013.

[6] A.Shakil Ahmed & Dr.A.Rajeswari, ISBN: 978-1-4673-1601-9/12/$31.00 ©2012 IEEE 389 ICRTIT-2012 , "Intrusion Detection in Heterogeneous Wireless Sensor Networks With an Energy Efficient Localization Algorithm "

[7] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho , IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 9, NO. 2, JUNE 2012 "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection"

[8] Hu, W., Chou, C.T., Jha, S., and Bulusu, N.: Deploying Long- Lived and Cost-effective Hybrid Sensor Networks. Elsevier Ad-Hoc Networks, Vol. 4, Issue 6. (2010) 749-767.

[9] A. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks.

[10] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," Wireless Networks, vol. 16, no. 5, pp. 1493–1510, July 2010.

### Author's Details

1.Dr. J Anitha , Professor, Department of Computer Science & Engg, Dayananda Sagar Academy of Technology and Management,Karnataka,India, anitha.jayapalan@gmail.com

2.Anil Kumar B, Asst. Professor, Department of Computer Science & Engg, Dayananda Sagar Academy of Technology and Management, Karnataka, India, anildsatm@gmail.com