ORIGINAL RESEARCH PAPER
Volume - 11 | Issue - 08 | August - 2022 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

# ENHANCEMENT INTRUSION DETECTION MODEL IN WIRELESS SENSOR NETWORKS

Computer Science

**Dr. P. E. Elango** Assistant Professor, Department of Information Technology, Gobi Arts & Science College, Gobichettipalayam, Tamilnadu, India

**Mr. R. Naleiny** Assistant Professor, Department of Information Technology, Gobi Arts & Science College, Gobichettipalayam, Tamilnadu, India

**Dr. R. Prabahari** Assistant Professor, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, Tamilnadu, India

## ABSTRACT

Wireless Sensor Network (WSN) consist of spatially distributed such autonomous wireless sensors (also called nodes or motes) to cooperatively monitor physical or environmental conditions such as temperature, humidity, light intensity, sound, vibration, pressure, motion etc, A vision is emerging of the convergence of wireless communications, embedded sensing and processing devices with distributed algorithms into the field of wireless sensor networks (WSNs). The proponents of this emerging technology envision a future in which environments from nature reserves to cities are instrumented with disposable computing nodes, each with an onboard radio transceiver, battery, environmental sensors and processing capabilities. Wireless sensor network research grew out of the distributed sensor networks project at the Defence Advanced Projects Research Agency (DARPA), although the technology of the 1970s limited processing and communications and restricted the nodes to large form factors. With the exponential progress and cost reduction in micro-processing during the 1990s and 2000s, many new applications for WSN deployment emerged. The Amorphous Computing project envisioned highly generic, cheap and indistinguishable miniature devices, operating by analogy to the individual cells of biological systems. Since then, deployment of wireless sensor networks has been considered for diverse spectrum domains, including logistics, medicine, environmental monitoring, military monitoring and surveillance.

## KEYWORDS

Wireless, Intrusion, Detection, Nodes

## INTRODUCTION

Intrusion Detection has, in the route of the most recent couple of years, accepted vital significance inside the wide domain of network security, all the more so on account of wireless sensor networks. These are networks that don't have a hidden framework; the network topology is continually evolving. As we portrayed in the past section, their intrinsically helpless qualities make them powerless to a wide scope of attacks that once applied, it might be past the point of no return before any counter move can make impact. This makes it critical to continually (or if nothing else occasionally) screen all network action so as to recognize any suspicious conduct. Intrusion Detection Networks (IDS) do only that; screen review date, search for intrusions to the framework and start a legitimate reaction (e.g., start a programmed counter). In that bandwidth, there is a need to supplement customary anticipation instruments with proficient intrusion discovery and reaction.

### Background In Intrusion Detection

In intrusion detection we wish to provide an automated mechanism that identifies the source of an attack, once an intrusion attempt has occurred, and generates an alarm to notify the network or the administrator, so that appropriate preventive actions can take place. As an intrusion we consider any set of actions that can lead to an unauthorized access or alteration of the network's functionality.

### Intrusion Detection Policies

So as to identify a gatecrasher, we have to utilize a model of intrusion detection. We have to realize what an IDS framework should pay special mind to. Specifically, an IDS framework must have the option to recognize ordinary and unusual exercises so as to find malicious endeavors in time. Anyway this can be troublesome since numerous personal

conduct standards can be capricious and muddled. There are three fundamental methods that an intrusion location framework can use to group action:

### Abuse detection

In abuse recognition or mark based discovery frameworks, the watched conduct is contrasted and realized attack designs (marks). In this way, activity designs that may represent a security risk must be characterized and given to the framework. The abuse discovery framework attempts to perceive any "awful" conduct as indicated by these examples. Any activity that can't restricted is permitted. This network may display low bogus positives, however doesn't perform well at recognizing already obscure attacks.

Anomaly Detection. It solves the restrictions of abuse location by concentrating on ordinary practices, instead of assault practices. This method initially portrays what comprises an ordinary "conduct (typically settled via computerized preparing) and afterward signals as interruption endeavors any activity shifting from this conduct by a measurably critical sum. In this way there is a considerable possibility to detect novel attacks as intrusions. There are two problems associated with this approach: First, a network can exhibit legitimate but previously unseen behavior. This would prompt a generous bogus caution rate, where anomalous actions that are not intrusive are flagged as intrusive. Second, and even worse, an intrusion that does not exhibit anomalous behavior may not be detected, resulting in false negatives.

### Intrusion Detection Architectures

Traditionally, intrusion detection networks for fixed networks were divided into two categories: host-based and network-based. The host-based architecture was the first architecture to be explored in intrusion detection. A Host-Based Intrusion Detection Network (HIDS) is designed to monitor, detect, and respond to network activity and attacks on a given host (node). Any decision made is based on date collected at that host by reviewing audit logs for suspicious activity. This contradicts the distributed nature of sensor networks and makes it impossible to detect network attacks. A network-based architecture is clearly more appropriate here. Network-Based Intrusion Detection Networks (NIDS) use raw network packets as the data source. A network-based IDS typically listens on the network, and captures and examines individual packets in real time. It can analyze the entire packet, not just the header. In wired networks, active scanning of packets from a network- based intrusion detection network is usually done at specific traffic concentration points, such as switches, routers or gateways. On the other hand, wireless sensor networks do not have such bottlenecks. Any node can go about as a switch and traffic is typically dispersed for load adjusting purposes. In this way, it is difficult to screen the traffic at specific focuses. So, it is impossible to monitor the traffic at certain points. Therefore, when designing IDS for sensor networks, we must carefully locate the detection agents. Usually, due to the distributed nature of this type of networking and the traffic routed within, identical IDS clients must be installed in several nodes.

### Requirements Of Intrusion Detection For Wsns

So as to expand on the prerequisites that an IDS framework for sensor networks ought to fulfill, one needs to take a gander at the particular

qualities of these networks as depicted. There are two key prerequisites that an IDS must satisfy. These are adequacy- how to make the intrusion discovery framework arrange defame and considerate action accurately - and proficiency - how to run the IDS in a practical way. These two prerequisites fundamentally recommend that IDS ought to detect a generous level of intrusions into the managed framework, while keeping the bogus alert rate at an adequate level at a lower cost. Specifically, we necessitate that an IDS for sensor networks must fulfill the accompanying properties:

**Localized Auditing**

The IDS specialists must work with confined and incomplete review information. In sensor systems there are no brought together focuses (aside from the base station) that can gather review information for the whole system, so these methodology this sort of systems administration.

**Minimal Use of Resources**

The IDS structure ought to use a limited quantity of assets. The remote network doesn't have stable associations, and physical assets of network and gadgets, for example, data transmission and force, are constrained. Separation can occur whenever. Furthermore, the communication between nodes for intrusion location purposes ought not take a lot of the accessible transmission bandwidth.

**Designing An Intrusion Detection Network For Wsns**

Intrusion recognition can't tie in with recognizing that a node has been attacked, yet in addition detecting the wellspring of an attack. For our situation, the intrusion discovery process is activated by an attack and the ensuing cautions got by the neighboring sensors.

Author discuss its logicality and efficiency, and give a brief overview of the necessary and sufficient conditions, on the behavior of the IDS agents. However, as we noted earlier, the focus of this chapter is not to give the detailed theoretical foundation of intrusion detection but to convince the reader of the practicality and effectiveness of such an approach in the extremely resource constrained environment of sensor networks. This will set the scene for the next chapters where we will prove the applicability of the presented framework by developing novel detection countermeasures that can be incorporated into it.

## REFERENCES


[1]. Anderson, J.P., Computer Security Threat Monitoring and Surveillance, Technical report, James P. Anderson Co., Fort Washington, PA., April 1980. On Software Engineering, vol. SE-13, pp. 222-232, February 1987.

[2]. Ashok Kumar, D., and Venugopalan, S.R., 2016, December. A Novel algorithm for Network Anomaly Detection using Adaptive Machine Learning. In Advanced Computing and Intelligent Technologies (ICACIE), 2016 First International Conference on. Springer

[3]. Singh, S.P. (2010) Data Clustering Using K-Mean Algorithm For Network Intrusion Detection, Thesis, Lovely Professional University, Jalandhar.

[4]. Deepthy K. Denatious, and John, A. (2012) 'Survey on data mining techniques to enhance intrusion detection', International Conference on Computer Communication and Informatics, ICCI-2012, Coimbatore, India.

[5]. C. Kruegel, F. Valeur, and G. Vigna. Intrusion Detection and Correlation: Challenges and Solutions. Springer-Verlag Telos, 2004.

[6]. L. R. Halme and R. K. Bauer. AINT misbehaving – A taxonomy of anti-intrusion techniques. In Proc. of 18th NIST-NCSC National Information Systems Security Conference, pages 163– 172, 1995.

[7]. D.E. Denning, An Intrusion-Detection Model, IEEE Transactions on Software Engineering, vol. SE-13, pp. 222-232, 1987.

[8]. Dinakara K, "Anomaly Based Network Intrusion Detection System", Thesis Report, Dept. of Computer Science and Engineering, IIT Khargpur 2008

[9]. Guy Bruneau – GSEC Version 1.2f," The History and Evolution of Intrusion Detection", SANS Institute 2001.

[10]. Ilgun, Koral, USTAT:a real time IDS for Unix, Proceedings of the 1993 IEEE Computer Society Symposium on research insecurity and privacy, 1993.

[11]. Mark Crosbie, Gene Spafford, Defending a Computer System using Autonomous Agents, Technical report No. 95-022, COAST Laboratory, Department of Computer Sciences, Purdue University, March 1994.

[12]. D. Anderson, T. Frivold, A. Valdes, Next-generation intrusion detection expert system (NIDES), Technical report, SRI-CSL95-07, SRI International, Computer Science Lab, May 1995."

[13]. Paxson, Vern, Bro: A system for detecting network intruders in real-time, Computer Network, v 31, n 23, Dec 1999.

[14]. Ning,Wang X.S, Jajodia S, Modelling requests among cooperating IDSs, Computer Communications, v 23, n 17, Nov, 2000."

[15]. J. E. Dickerson and J. A. Dickerson, "Fuzzy network profiling for intrusion detection," In Proceedings of the 19th International Conference of the North American Fuzzy Information Processing Society (NAFIPS), 13-15 July 2000, pp. 301 – 306.

[16] TEODOR-GRIGORE LUPU," Main Types of Attacks in Wireless Sensor Networks "

[17] Sunil Gupta,Authentication Framework against "Malicious Attack in Mobile Wireless Sensor Networks", Vol II, IMECS 2017, March 15 - 17, 2017

[18] Chaudhari H.C. and Kadam L.U,"Wireless Sensor Networks: Security, Attacks and Challenges International Journal of Networking" ,Volume 1, Issue 1, 2011, pp-04-16

[19] Hu, Perrig, and Johnson, "Malicious Node Detection in Wireless Sensor Networks" Waldir Ribeiro Pires J´unior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro.