International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution Systems

***[1]Tasneem Rahath,[2]Ch Anusha, [3]B Divya Sri**
[1]Assistant Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India
[2,3]Students, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

Article Info
Volume 9, Issue 5
Page Number : 306-310

Publication Issue :
September-October-2022

Article History
Accepted : 01 Oct 2022
Published: 22 Oct 2022

ABSTRACT
Networks protection against different types of attacks is one of most important posed issue into the network and information security application domains. This problem on Wireless Sensor Networks (WSNs), in attention to their special properties, has more importance. Now, there are some of proposed architectures and guide lines to protect Wireless Sensor Networks (WSNs) against different types of intrusions; but any one of them do not has a comprehensive view to this problem and they are usually designed and implemented in single-purpose; but, the proposed design in this paper tries to has been a comprehensive view to this issue by presenting a complete and comprehensive Intrusion Detection Architecture (IDA). The main contribution of this architecture is its hierarchical structure; i.e., it is designed and applicable, in one or two levels, consistent to the application domain and its required security level. Focus of this paper is on the clustering WSNs, designing and deploying Cluster-based Intrusion Detection System (CIDS) on cluster-heads and Wireless Sensor Network wide level Intrusion Detection System (WSNIDS) on the central server. Suppositions of the WSN and Intrusion Detection Architecture (IDA) are: static and heterogeneous network, hierarchical and clustering structure, clusters' overlapping and using hierarchical routing protocol such as LEACH, but along with minor changes. Finally, the proposed idea has been verified by designing a questionnaire, representing it to some (about 50 people) experts and then, analyzing and evaluating its acquired results.

Keywords : Wireless Sensor Network (WSN), Security, Routing, Intrusion Detection System (IDS), Attack, Detection, Response & Tracking.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are homogeneous or heterogeneous systems consist of many small devices, called sensor nodes, that monitoring different environments in cooperative [1, 2]; i.e. sensor nodes cooperate to each other and compose their local data to reach a global view of the operational environment; they also can operate autonomously. In WSNs there are two other components, called "aggregation points" (i.e. cluster-heads and CIDSs' deployment locations) and "base stations" (i.e. central server and the

WSNIDS's deployment location), which have more powerful resources and capabilities than normal sensor nodes [1, 2]. As shown in Figure1, aggregation points collect information from their nearby sensors, integrate and aggregate them and then forward to the base stations to process gathered data. Factors such as wireless, unsafe, unprotected and shared nature of communication channel, untrusted and broadcast transmission media, deployment in hostile and open environments, automated and unattended nature and limited resources, make WSNs vulnerable and susceptible to many types of attacks [1]. Therefore, security is a vital and complex requirement for these networks. In attending to the WSNs' constraints, their requirements and unusable traditional network security techniques on WSNs [2,3]; so the defensive-security mechanisms that can guarantee the normal functionalities of these networks, must be consistent to the WSNs' autonomous mechanisms. This paper is following a complete security mechanism to cover and establish different basic security dimensions of WSNs, like confidentiality, integrity, availability and authenticity; of course, by attending to the existent obstacles and constraints in these networks. Our proposal is adding a another defensive line, called Intrusion Detection System (IDS), as a new defensive-security level to the WSNs' security infrastructure; which it can detects unsafe activities and unauthorized login/access, and when attacks occurred, even new attacks such as anomalies, it can notifies by different warnings and operates required actions (mainly predefined actions). Therefore, the main purpose of this paper is presenting, discussing and solving the intrusion detection problem in WSNs. This paper by focus on WSNs' security follows this goal, including:

• An overview of WSNs and their security;

• Discussing Intrusion Detection System (IDS) as a new aggressive-defensive security layer for WSNs;

• Suggestion a comprehensive, hierarchical and distributed intrusion detection model and IDS architecture on WSNs (CIDS and WSNIDS architectures);

This paper makes us enable to identify the existent security challenges in WSNs and we can almost solve intrusion detection problem in these networks, by adding a new defensive-security layer, called IDS, to WSNs' security infrastructure; besides, we also can detect and manage WSNs' attacks and react to them, appropriate to attacks' type and their nature.

II. LITERATURE SURVEY

Specification based intrusion detection looks for abnormal performance at the system level; contrast this with anomaly based intrusion detection that analyzes specific user profiles or data flows. Specification based intrusion detection approaches formally define legitimate behavior and indicate an intrusion when the system departs from this model. One major advantage of specification based intrusion detection is a low false negative rate. Only
situations that violate what a human expert previously defined as proper system behavior generate detections. By definition, these approaches only react to known bad behavior; the theoretical basis is a bad node will disrupt the formal specification of the system. Another major advantage of specification based intrusion detection is the system is immediately effective because there is no training/profiling phase. The key disadvantage of specification based intrusion detection is the effort required to generate a formal specification. Specification based intrusion detection approaches are especially effective against insider attacks as they focus on system disruption. On the other hand, they are not the best approach for outside attackers because the specification (e.g., state machine or grammar) is application-specific and pertains to actions that only an insider can take. An outsider is not capable of generating transitions in the governing state machine or transforms in the defining grammar. Specification based intrusion detection is a form of anomaly based

intrusion detection where no user, group or data profiling is used. Instead legitimate behaviors are specified by humans and a nodes misbehavior is measured by its deviation from the specification. This allows for lightweight intrusion detection to be deployed in systems with severe resource constraints where user, group or data profiling is not possible.

Signature based intrusion detection approaches look for runtime features that match a specific pattern of misbehavior. Some sources refer to this approach as misuse detection, supervised detection, pattern based detection or intruder profiling. One major advantage of this category is a low false positive rate. By definition, these approaches only react to known bad behavior; the theoretical basis is a good node will not exhibit the attack signature. The key disadvantage of this category is that the techniques must look for a specific pattern; a dictionary must specify each attack vector and stay current. An attack signature can be a univariate data sequence: for example, bytes transmitted on a network, a program's system call history or application specific information flows (sensor measurements in a WSN or CPS). One sophistication is to combine simple data sequences into a multivariate data sequence. The important research problem in this field is creating an effective attack dictionary. Signature length is a coarse indicator of efficiency for signature based approaches; longer signatures suggest a larger memory requirement and higher microprocessor use. Signature based approaches are more effective against outsider attacks; malicious outsiders presumably will exhibit well known signatures in the course of penetrating the network.

III. PROPOSED SYSTEM

Intrusion detection in WSNs has many challenges, mainly due to lack or weak of resources [5, 13]. Besides, the existent methods and protocols of traditional networks can not be used and enforced to the WSN, directly; because they need to the resources which attending to the WSNs' limitations and constraints are inaccessible. In general, WSNs are application-oriented [10, 12]; i.e. they are designed as cover the very special properties according to the target application domain. Intrusion detection process is supposing that the behavior of normal system is differentiating than the behavior of attacked system. There are several possible and different configurations for WSNs; so, it is difficult to define normal and expected behavior; since the proposed IDS should have been different characteristics on different application domains. Non-existence the unique structure for WSNs, leads to non-existence unique IDS and requiring different IDSs; so, requiring to a modular and comprehensive IDS [14, 16].

IV. APPROACHES

There are two major approaches for intrusion detection in this domain, as follows:

• Centralized approach: for applications with accessible nodes and possible to manage them, in centralize [14, 16]; else, this kind of architecture threats the entire system security.

• Distributed approach: in this approach, it is possible to have one IDS per each cluster of nodes (CIDS); in this case, cluster-heads usually make decisions autonomously and independently; in some cases about boundary nodes, they cooperate to each others for intrusion detection; so, they take decisions, cooperatively. Thus, they using a cooperative mechanism to take appropriate decisions and then, they combine the local view of neighboring cluster-heads to each other. In clustering method, all cluster-heads that place in the radio range of a node, can surveillance on that node, to identify malicious nodes accurately by using the majority rule; even though chained destruction.

The used approach is combinational; i.e. at first, the existent sensor nodes be classified in subsets, called cluster; then, a cluster-head be selected per each

cluster. Now, in low level, a series of distributed IDS, called CIDS, be installed on cluster-heads; these IDSs have communicate to each other and corresponding cluster nodes; also, they have communicate to the central server (high-level IDS: WSNIDS). Besides, there is a centralized and comprehensive IDS on high level of the WSN architecture which has been installed and deployed on the powerful central server, called WSNIDS.

V. CONCLUSION

The purpose of this paper is considering intrusion detection problem on WSNs and designing an Intrusion Detection Architecture (IDA) for these networks, of course by attending to their restrictions. The suggested system depends on situations, the WSN's application domain, the requirement security level and other things such as its cost, can be used and implemented in 1 or 2 levels; including: CIDSs (surveillance, monitoring and control in cluster-level) on cluster-heads and the WSNIDS (monitoring and control in the WSN-wide level or level of the entire WSN) on the central management system.

VI. REFERENCES

[1] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy; A Comparison of Routing Attacks on Wireless Sensor Networks; Journal of Information Assurance and Security (JIAS); ISSN 1554-1010 Volume 6, pp. 195-215; 2011.

[2] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy; A Comparison of Link Layer Attacks on Wireless Sensor Networks; Journal of Information Security (JIS); 2011.

[3] K. Sharma and M. K. Ghose; Wireless Sensor Networks: An Overview on its Security Threats; IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs; CSE Department, SMIT, Sikkim, India; 2010.

[4] T. A. Zia; A Security Framework for Wireless Sensor Networks; Doctor of Philosophy Thesis; The School of Information Technologies, University of Sydney; Feb 2008.

[5] M. Saxena; Security in Wireless Sensor Networks: A Layer-based Classification; Department of Computer Science, Purdue University.

[6] Z. Li and G. Gong; A Survey on Security in Wireless Sensor Networks; Department of Electrical and Computer Engineering, University of Waterloo, Canada.

[7] A. Dimitrievski, V. Pejovska and D. Davcev; Security Issues and Approaches in WSN; Department of computer science, Faculty of Electrical Engineering and Information Technology; Skopje, Republic of Macedonia.

[8] J. Yick, B. Mukherjee and D. Ghosal; Wireless Sensor Network Survey; Elsevier's Computer Networks Journal 52 (2292-2330); Department of Computer Science, University of California; 2008.

[9] C. Karlof and D. Wagner; Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures; Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols; In First IEEE International Workshop on Sensor Network Protocols and Applications; University of California at Berkeley, Berkeley, USA; 2003.

[10] A. Perrig, R. Szewczyk, V. Wen, D. culler and D. Tygar; SPINS: Security Protocols for Sensor Networks; Wireless Networking ACM CCS; 2003.

[11] B. Krishnamachari, D. Estrin, and S. Wicker; The Impact of Data Aggregation in Wireless Sensor Networks; International Workshop on Distributed Event-Based Systems, (DEBS '02), p 457-458; 2002.

[12] V. Handziski, A. K¨opke, H Karl, C. Frank, and W. Drytkiewicz; Improving The Energy

Efficiency of Directed Diffusion Using Passive Clustering; in Proc. 1st European Workshop on Wireless Sensor Networks, pp. 172 – 187, Berlin, Germany; 2004.

[13] K. Scarfone and P. Mell; Guide to Intrusion Detection and Prevention Systems (IDPS); NIST 800-94; Feb 2007.

[14] G. Maselli, L. Deri and S. Suin; Design and Implementation of an Anomaly Detection System: an Empirical Approach; University of Pisa, Italy; 2002.

[15] V. Chandala, A. Banerjee and V. Kumar; Anomaly Detection: A Survey; ACM Computing Surveys; University of Minnesota; Sep 2009.

[16] Ch. Krügel and Th. Toth; A Survey on Intrusion Detection Systems; TU Vienna , Austria; 2000.

[17] J. Molina and M. Cukier; Evaluating Attack Resiliency for Host Intrusion Detection Systems; Information Assurance and Security Journal; 2009.

[18] S. Selliah; Mobile Agent-Based Attack Resistant Architecture for Distributed Intrusion Detection System; MSc Thesis, College of Engineering and Mineral Resources at West Virginia University; 2001.

[19] A. K. Jones and R. S. Sielken; Computer System Intrusion Detection: A Survey; University of Virginia, USA.

[20] S. Northcutt and J. Novak; Network Intrusion Detection: An Analyst's Handbook; New Riders Publishing; Thousand Oaks, CA, USA; 2002.

[21] S. Zanero and S. M. Savaresi; Unsupervised Learning Techniques for an Intrusion Detection System; ACM Symposium on Applied Computing; 2004.

[22] O. Depren, M. Topallar, E. narim and M. K. Ciliz; An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks; 2005.

[23] R. A. Kemmerer and G. Vigna; Intrusion Detection: A Brief History and Overview; 2002

Cite this article as :

Tasneem Rahath, Ch Anusha, B Divya Sri, "Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution Systems", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 5, pp. 306-310, September-October 2022.

Journal URL : https://ijsrset.com/IJSRSET229639