©2019 Published in 7th International Symposium on Innovative Technologies in Engineering and Science 22-24 November 2019 (ISITES2019 SanliUrfa - Turkey)
https://doi.org/10.33793/acperpro.02.03.18

Distributed Intrusion Detection Systems: A Review

*[1]Murat Özalp, [2]Cihan Karakuzu, [3]Ahmet Zengin
[1] IT Department, Bilecik Seyh Edebali University, Turkey
[2] Faculty of Engineering, Department of Computer Engineering, Bilecik Seyh Edebali University, Turkey
[3] Faculty of Computer and Information Sciences, Department of Computer Engineering, Sakarya University, Turkey

Abstract

In this paper, distributed intrusion detection systems (IDSs) in the literature are reviewed. There are two types of IDS, depending on the interoperability. Stand-alone systems decide on their own. Distributed systems are composed of multiple components processing different data and work together to make a global decision. Distributed IDSs present some difficulties compared to stand-alone systems. For example, problems such as the structure of message communication, establishment of a trust mechanism, joint decision making are the issues discussed in the studies related to such systems. A detailed literature review has been made for the distributed IDSs which are the focus of our study. The studies considered to be within the scope of our study were investigated and presented. Although the initial studies on interoperable systems began in the 1990s, the issue is still open to improvement, as there is no widespread system that has become "product". On the other hand, due to the development of artificial intelligence systems, innovative studies are being conducted on cyber threat detection. Therefore, the subject is thought to be open to improvement and in the last part of the study, suggestions are given for those who want to work on the subject.

Key words: IDS, DIDS, distributed IDS

1. Introduction

New risks arise every day in computer systems. For large networks (governments, corporations, companies, etc.), cyber security risks are becoming more and more serious threats. Multiple IDS can be used to protect such large networks. In this study, we focused on the interoperability of a large number of IDS.

In the literature review; DIDS (Distributed Intrusion Detection System), CIDS (Collaborative Intrusion Detection System) and CIDN (Collaborative Intrusion Detection Network) studies have been seen. All of these terms refer to cases where more than one IDS is used. IDSs that work independently are called stand-alone (isolated) IDS. DIDS is the general definition for IDSs consisting of multiple components. CIDS refers to IDSs that work in communication and collaboration with each other. CIDN refers to IDS networks that are composed of CIDSs. In some studies; It has been found that non-IDS tools (firewalls, log analysis systems, honeypot etc.) can also be included in CIDN systems.

*Corresponding author: Address: IT Department, Bilecik Seyh Edebali University, Turkey

2. Types of studies seen in literature review

In the literature review, systems with multiple IDS were examined. The main issues discussed in these studies are summarized below:

1. Classification studies:
   a) Signature based / anomaly based / hybrid systems
   b) NIDS / HIDS (network IDS / host -computer- IDS)
   c) Systems studied in terms of physical topology. Classifications such as central systems, distributed systems, hierarchical systems have been made.
2. Studies on the common language in which different security systems can speak. Some important studies on this subject can be summarized as follows:
   a) Lambda (a language to model a database for detection of attacks). Cuppens and Ortalo published this work in 2000. The stages of the attack can be defined as events. In this way, it is aimed to identify attacks using algebraic operators. [1]
   b) Mirador. It was published in 2002 by Cuppens and Miege. A common module for IDSs was proposed in the project. This module; provides functions for managing, clustering, merging, and associating alerts. Clustering and merging functions recognize alerts corresponding to the same attack event and generate a new alert that combines data from these various alerts. [2]
   c) STATL (An Attack Language for State-based Intrusion Detection). It was published in 2002 by Eckman et al. The language designed in the study; allows the attack phases to be defined as sequences of events. A STATL expression can be used by an IDS to analyze an event stream and detect potential ongoing attacks. [3]
   d) IDMEF (Intrusion Detection Message Exchange Format). It was studied in 2007 by Debar et al. Published by RFC 4765. The purpose of IDMEF is to define data formats and exchange procedures to share information of interest to IDSs and systems that may need to interact with them. [4]
   e) IODEF (Incident Object Description Exchange Format). It was studied in 2007 by Danyliw et al. Published by RFC 5070. IODEF is based on IDMEF and provides backward compatibility. Unlike IDMEF; It is designed for CSIRTs (computer security incident response teams) to share information, not IDSs. It is in a form that the machine can handle, but people can read. [5]
   f) ADeLe (an attack description language for knowledge-based intrusion detection). This attack description language was made by Michel and Me in 2001. The ADeLe language was developed simultaneously with the Lambda language in the Mirador project. Both languages allow detection and correlation rules as well as expression of attack code. However, while Lambda uses a declarative approach, ADeLe uses a more procedural approach. [6]

g) STIX (structured threat information expression) and TAXII™ (trusted automated exchange of intelligence information) systems are presented by the non-profit organization MITRE. TAXII is a study conducted by the US Department of National Security that makes it possible to share threat information between trusted assets. Threat information that can be shared in TAXII; IP addresses, e-mail headers and malicious software discovered vulnerabilities and even defense action plans can be. The exchanged TAXII information is represented in the XML-based STIX language. [7]
h) IDEA (Intrusion Detection Extensible Alert). Published by Kácha in 2013. JSON format is preferred in IDEA system instead of XML based systems like IDMEF and IODEF. [8]

3. Data privacy studies. IDSs, by nature, monitor corporate data (traffic, behavior, etc.). It is possible to transfer data out of the organization via IDS designed by a malicious person. Even if there is no malicious intent, weaknesses or errors in the systems may pose a security risk. On the other hand, for distributed systems; IDSs must already communicate with each other. There are risks related to the privacy of the systems that will work in different institutions and communicate with each other. [9], [10]
4. Studies on CIDN threats. In CIDN systems, if one or more IDS itself has become "bad"; attack traffic can be interpreted as normal traffic, and vice versa. Some types of threats have been identified (sybil, newcomer, betreyal, collusion, etc.). In the academic review studies, it was interpreted whether the systems examined were vulnerable to these threats. [11]
5. Studies on alarm correlation methods. The topic of how to evaluate the alarms from multiple nodes together. Techniques for reducing false positives are also considered in this context.

Within the scope of this study, review studies on the subject in the literature have been examined. There are two review / surveys conducted in 2010 and 2011. Again in the same scope; there is a book chapter published in 2006 and a book published in 2014. These studies are presented under the next title in chronological order. [10]–[13]

3. Distributed intrusion detection systems in the literature

Studies on DIDS in the literature started in the 1990s and continued extensively until 2009, but then decreased. After these years, it has been seen that IDS studies are mostly focused on wireless sensor networks and cloud. Important studies in the context of DIDS are presented chronologically below.

The first study in the literature about the subject; It is an early prototype design called DIDS (Distributed Intrusion Detection System) by Snapp et al. In this study, components were applied both on the multi-user server system and on the network monitoring system. [14], [15]

In 1999, Huang and colleagues designed large-scale and distributed IDS based on attack strategy analysis. In the study, the difficulties of such studies are stated as: Working with heterogeneous systems, working with voluminous and noisy data, insufficient data for easy decision making, different sensor technologies, trust relationship between IDS agents, different attack patterns. [16]

In 2001, a hierarchical structure was designed by Frincke and Wilhite. In this structure, agents were provided to work with an IDS at the center. This ensures that the agents remain lightweight, while ensuring no compromise on IDS performance. [17]

In 2003, Wu et al. Designed a CIDS. In this study; There are three layers: network, core and application. There is also a separate layer in the center. The central layer processes alarms from other components using a Bayesian algorithm to generate a common alarm. [18]

In 2004, DIDS was designed by Wang et al. based on the “data fusion” method. In the first layer of the system; local NIDS/HIDS components that are used to make decisions about attacks that can be easily detected. The second layer is where the data is combined and global decisions are made. [19]

In 2004, Yegneswaran and his colleagues designed a DIDS called DOMINO (Distributed Overlay For Monitoring Internet Outbreaks). This system; is an IDS architecture that enables the collaboration of heterogeneous nodes organized into a network layer. The capabilities and performance of the system have been tested with numerous systems. Attack records were collected over four months from more than 1600 providers on the Internet. [20]

In 2004, Locasto and colleagues proposed a completely distributed system that transmits alarms to each node. This system consists essentially of two components. The first component extracts the necessary information from the alert streams and sends it to Bloom filters that function as a probabilistic database. The second component is responsible for timing the correlation relationships between the ends. The reason for using Bloom filters is to provide privacy for this study. These filters offer only insert and validation features. [9]

In 2005, Yu et al proposed the use of multiple IDS agents working in collaborative architecture to detect real-time attacks. There are three sections in the architecture: common alert aggregation, alert assessment based on knowledge base, alert correlation. IDMEF is the preferred messaging format. [4], [21]

In 2005, Zhang and his colleagues designed a decision-making DIDS with a two-tiered clustering. In the first layer, clustering is performed on agents operating on the nodes. These clustering results are passed through the re-clustering algorithm on the IDS running at the center. [22]

In 2005, Zhou et al. Designed a DIDS that worked as P2P (peer to peer). The motivation of this study; the single point of failure in centralized managed DIDS. In the system designed in the study, there is no central control system. A large number of nodes (computers) in different networks directly share the information of attacks that they receive with other nodes. Communication of the nodes is provided by Chord, a DHT (Distributed Hash Table) based protocol. [23]

In the book chapter published by Abraham and Thomas in 2006, the history of IDS and DIDS is mentioned. In the study, which gives examples on KDD Cup data set, the methods such as how to reduce the data to be processed and how to make IDS modeling are also emphasized. [12]

In 2009, Zhu et al. Applied the game theory on CIDS. It is a study of mathematics rather than computer. IDS is not the main scope of the study, but IDS is used as an example in the theory studied. [24]

In 2009, Dastjerdi et al. Designed cloud-based DIDS using mobile clients. The advantages of the study are: high scalability, low network latency, reduced network load and consequently reduced network operating costs, asynchronous and autonomous operation, ability to work in a heterogeneous cloud environment. [25]

In 2010, Zhou et al. Conducted studies on coordinated attacks and CIDS. It is reported that co-ordinated attacks (large-scale scans, worm attacks, DoS attacks, etc.) affect multiple different networks at the same time. With isolated IDSs (stand-alone, listening only to a specific area), it is emphasized that such large-scale attacks are difficult to detect and identify. For this reason, CIDS architectures and alarm correlation methods are discussed. The four important and distinctive issues in CIDS systems are: system architecture (how to correlate and how sensors will be planned?), Alarm correlation (how to actually detect intrusion records?), Privacy (sensors in different institutions need to protect confidential information), data security and trust principle (confidential communication and trust infrastructure between different sensors). In this study, a detailed literature review was made and related studies were examined in detail in terms of the titles listed above. [10]

In a study conducted by Fung in 2011, CIDSs in the literature were investigated for possible attacks from within the IDS network itself. Insider attacks are described as follows: Sybil (node that tries to join the network with different fake identities by creating multiple identities), Newcomer (a bad node that wants to be included as a good node in the network), Betrayal (when a good node starts to do bad things after a while), Collusion (multiple bad nodes working together) [11]

The work published by Fung and Boutaba in 2013 focused on CIDN design and management. CIDN is the name given to a network consisting of a combination of CIDS and usually designed as a separate layer. The presence of bad members in CIDNs is reported to be a risk, and studies have been conducted to reduce this risk. In this study; CIDNs focus on four main topics: trust

management, collaborative intrusion detection, resource management, collaborative node selection. In this study, it is designed to run IDSs belonging to different manufacturers together as P2P. [26]

In 2014, Hu and his colleagues designed a distributed IDS framework. According to this system; the classification algorithm is run on each node, and the global attack classification algorithm is executed after the nodes. Adaboost, online GMM (Gaussian Mixture Model), PSO and SVM based algorithms were used. [27]

In 2014, Fung and Boutaba published the book "Intrusion Detection Networks - A Key to Collaborative Security". The basis of cyber-attacks, IDS types and important IDSs in the literature are mentioned. Advanced topics such as CIDN architectural design are also explained in detail. In the annexes section, sample IDS (Snort) rules and sample IDMEF messages are given. [13]

4. Results and discussion

Today, it is seen that security cannot be provided with a single device or software. Especially in large or critical networks, even a single IDS may be insufficient. Running multiple IDS together is still open to academic studies. Since the computing power of the processors is increasing day by day, systems that can be imagined a few years ago can now be designed. Even IDS can be made with small systems called single card computers.[28]

There are many different types of security systems used today. It is a necessity that the data obtained and processed by these different types of systems can be evaluated with a higher intelligence. At this point, cloud-based systems should also be evaluated from this perspective. In addition to the automatic evaluation of the data generated by security systems, studies can be conducted to make recommendations to each other. Re-evaluation of the recent studies on machine learning from the perspective of safety will also make a significant contribution to the literature.

References

[1] F. Cuppens and R. Ortalo, "LAMBDA: A Language to Model a Database for Detection of Attacks," Springer, Berlin, Heidelberg, 2000, pp. 197–216.

[2] F. Cuppens and A. Miege, "Alert correlation in a cooperative intrusion detection framework," in *Proceedings 2002 IEEE Symposium on Security and Privacy*, pp. 202–215.

[3] S. T. Eckmann, G. Vigna, and R. A. Kemmerer, "STATL: An attack language for state-based intrusion detection," *J. Comput. Secur.*, vol. 10, no. 1–2, pp. 71–103, Jan. 2002.

[4] H. Debar, D. Curry, and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)," *RFC*, Mar-2007.

[5] R. Danyliw, J. Meijer, and Y. Demchenko, "RFC5070 - The Incident Object Description Exchange Format," *IETF*, 2007.

[6] C. Michel and L. Mé, "ADeLe: An Attack Description Language for Knowledge-Based Intrusion Detection," Springer, Boston, MA, 2001, pp. 353–368.

[7] P. Kampanakis, "Security Automation and Threat Information-Sharing Options," *IEEE Secur. Priv.*, vol. 12, no. 5, pp. 42–51, Sep. 2014.

[8] P. Kácha, "IDEA : Designing the Data Model for Security Event Exchange CESNET-CERTS Computer Security Incident Response Team," *Wseas.Us*, pp. 209–214, 2013.

[9] M. E. Locasto, J. J. Parekh, S. Stolfo, A. D. Keromytis, T. G. Malkin, and V. Misra, "Collaborative Distributed Intrusion Detection," *Columbia University Computer Science Technical Reports, CUCS-012-04*, 2004.

[10] C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection," *Comput. Secur.*, vol. 29, no. 1, pp. 124–140, 2010.

[11] C. J. Fung, "Collaborative Intrusion Detection Networks and Insider Attacks," *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 2, no. 1, pp. 63–74, 2011.

[12] A. Abraham and J. Thomas, "Distributed Intrusion Detection Systems - A Computational Intelligence Approach," in *Applications of Information Systems to Homeland Security and Defense*, IGI Global, 2006, pp. 107–137.

[13] C. Fung and R. Boutaba, *Intrusion Detection Networks A Key to Collaborative Security*. Londra: CRC Press, 2014.

[14] S. R. Snapp *et al.*, "A system for distributed intrusion detection," in *Digest of Papers - IEEE Computer Society International Conference*, 1991, pp. 170–176.

[15] S. R. Snapp *et al.*, "DIDS (Distributed Intrusion Detection System) − − Motivation, Architecture, and An Early Prototype," in *In Proceedings of the 14th National Computer Security Conference*, 1991, pp. 167--176.

[16] M. Y. Huang, R. J. Jasper, and T. M. Wicks, "Large scale distributed intrusion detection framework based on attack strategy analysis," *Comput. Networks*, vol. 31, no. 23, pp. 2465–2475, 1999.

[17] D. Frincke and E. Wilhite, "Distributed Network Defense," *Inf. Syst. Secur.*, pp. 5–6, 2001.

[18] Y. S. Wu, B. Foo, Y. Mei, and S. Bagchi, "Collaborative intrusion detection system (CIDS): A framework for accurate and efficient IDS," *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, vol. 2003-Janua, no. Acsac, pp. 234–244, 2003.

[19] Y. Wang, H. Yang, X. Wang, and R. Zhang, "Distributed intrusion detection system based on data fusion method," *Fifth World Congr. Intell. Control Autom. (IEEE Cat. No.04EX788)*, no. 2, pp. 4331–4334, 2004.

[20] V. Yegneswaran, P. Barford, and S. Jha, "Global Intrusion Detection in the DOMINO Overlay System.," *Netw. Distrib. Syst. Secur. Symp.*, 2004.

[21] J. Yu, Y. V. R. Reddy, S. Selliah, S. Reddy, V. Bharadwaj, and S. Kankanahalli, "TRINETR: An architecture for collaborative intrusion detection and knowledge-based alert evaluation," *Adv. Eng. Informatics*, vol. 19, no. 2, pp. 93–101, 2005.

[22] Y.-F. Zhang, Z.-Y. Xiong, and X.-Q. Wang, "Distributed intrusion detection based on clustering," *2005 Int. Conf. Mach. Learn. Cybern.*, vol. 4, no. August, pp. 18–21, 2005.

[23] C. V. Zhou, S. Karunasekera, and C. Leckie, "A Peer-to-Peer Collaborative Intrusion Detection System," in *2005 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf on Communic*, 2005, vol. 1, pp. 118–123.

[24] Q. Zhu, C. Fung, R. Boutaba, and T. Başar, "A game-theoretical approach to incentive design in collaborative intrusion detection networks," *Proc. 2009 Int. Conf. Game Theory Networks, GameNets '09*, pp. 384–392, 2009.

[25] A. V. Dastjerdi, K. A. Bakar, and S. G. Hassan Tabatabaei, "Distributed intrusion detection in clouds using mobile agents," *3rd Int. Conf. Adv. Eng. Comput. Appl. Sci. ADVCOMP 2009*, pp. 175–180, 2009.

[26] C. J. Fung and R. Boutaba, "Design and Management of Collaborative Intrusion Detection Networks," *2013 Ifip/Ieee Int. Symp. Integr. Netw. Manag.*, pp. 955–961, 2013.

[27] W. Hu, J. Gao, Y. Wang, O. Wu, and S. Maybank, "Online adaboost-based parameterized methods for dynamic distributed network intrusion detection," *IEEE Trans. Cybern.*, vol. 44, no. 1, pp. 66–82, 2014.

[28] M. Ozalp, C. Karakuzu, and A. Zengin, "Designing of Security Hardware for Wireless Network," in *2018 3rd International Conference on Computer Science and Engineering (UBMK)*, 2018, pp. 244–247.