- 1175 : IoT Multimedia Applications and Services
- Published: 24 February 2021

Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things

- R. Gopi,
- V. Sathiyamoorthi,
- S. Selvakumar,
- Ramasamy Manikandan,
- Pushpita Chatterjee,
- N. Z. Jhanjhi &
- Ashish Kumar Luhach

Multimedia Tools and Applications (2021)Cite this article

Abstract

Due to the huge flow of data and complications in mutable characteristics of the data, Distributed Denial of Services attacks existed in the Multimedia Internet of Things. Attacks over the IoT have become an increasing menace in recent time, which tries to hack or illegally tamper the streaming data available over the networks. On the other hand, there has been an increase in volume in research contributions to effectively counter these attacks and implement a strong defense mechanism. There have been numerous algorithms and frameworks implemented in recent times that are intelligent and soft computing-based. These evolution-based algorithms play a vital role in self-adapting the system under attack towards increasing and new types of attacks which are increasing day by day. One such area of soft computing algorithms investigated in this paper is the Artificial Neural Network or popularly known as ANNs. It works analogously to the biological neurons in the human body. In this paper, we systematically

explain the ANN-based network model to counteract the DDoS attacks in the Multimedia Internet of Things, architecture, and implementation of ANNs, the experimental investigations and findings which help in drawing an inference of ANN-based defense models.

References

1.
Arivudainambi D, Varun Kumar KA, Chakkaravarthy SS (2019) LION IDS: a meta-heuristics approach to detect DDoS attacks against software-defined networks. Neural Comput Applic 31(5):1491–1501

Article Google Scholar

15
0
2. 5
Chhaya L, Sharma P, Bhagwatikar G, Kumar A (2017) Wireless sensor network based smart grid communications: cyber attacks, intrusion detection system and topology control. Electronics 6(1):5

Article Google Scholar

44
0
3. 19
Colom JF, Gil D, Mora H, Volckaert B, Jimeno AM (2018) Scheduling framework for distributed intrusion detection systems over heterogeneous network architectures. J Netw Comput Appl 108:76–86

Article Google Scholar

14
0
4. 4
Durairipandian M, Palanisamy C (2015) Analysis of a combined parameter-based multi-objective model for performance improvement in wireless networks. Wirel Pers Commun 83(4):2425–2437

Article Google Scholar

2
0
5. 0
Farris I et al (2018) A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Commun Surv Tutor 21(1):812–837

Article Google Scholar

99
0
6. 58
Ferrag MA, Maglaras L, Ahmim A, Derdour M, Janicke H (2020) RDTIDS: rules and decision tree-based intrusion detection system for internet-of-things networks. Futur Internet 12(3):44

Article Google Scholar

18
0
7. 10
Fu Y, et al. (2017) An automata based intrusion detection method for internet of things. Mob Inf Syst 2017

8.
Gandhi UD, Kumar PM, Varatharajan R, Manogaran G, Sundarasekar R, Kadu S (2018) HIoTPOT: surveillance on IoT devices against recent threats. Wirel Pers Commun 103(2):1179–1194

Article Google Scholar

35
0
4
9.
Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud), pp. 84–90. IEEE

10.
Golrang A, Golrang AM, Yayilgan SY, Elezaj O (2020) A novel hybrid IDS based on modified NSGAII-ANN and random forest. Electronics 9(4):577

Article Google Scholar

7
0
6
11.
Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B (2019) A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7:82721–82743

Article Google Scholar

197
0
128
12.
Hussain F, Hussain R, Hassan SA, & Hossain E (2020) Machine learning in IoT security: current solutions and future challenges. IEEE Commun Surv Tutor

13.
Khan R, Kumar P, Jayakody DNK, Liyanage M (2019) A survey on security and privacy of 5G technologies: potential solutions, recent advancements and future directions. IEEE Commun Surv Tutor

14.
Kim J, Kim J, Kim H, Shim M, Choi E (2020) CNN-based network intrusion detection against denial-of-service attacks. Electronics 9(6):916

Article Google Scholar

23
0
13
15.
Ksasy MS et al (2018) A new advanced cryptographic algorithm system for binary codes by means of mathematical equation. ICIC Exp Lett 12(2):117–125

Google Scholar

16.

Manimurugan S, Al-Mutairi S, Aborokbah MM, Chilamkurti N, Ganesan S, Patan R (2020) Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access 8:77396–77404

Article Google Scholar

21
0
25
0

17. Manso P, Moura J, Serrão C (2019) SDN-based intrusion detection system for early detection and mitigation of DDoS attacks. Information 10(3):106

Article Google Scholar

20
0
13
0

18. Napiah MN, Idris MYIB, Ramli R, Ahmedy I (2018) Compression header analyzer intrusion detection system (cha-ids) for 6lowpan communication protocol. IEEE Access 6:16623–16638

Article Google Scholar

31
0
35
0

19. Pejic D, Arsic M (2019) Minimization and maximization of functions: golden-section search in one dimension. In: Exploring the Data Flow Supercomputing Paradigm (pp. 55–90). Springer: Cham

20. Suratgar AA, Tavakoli MB, Hoseinabadi A (2005) Modified Levenberg-Marquardt method for neural networks training. World Acad Sci Eng Technol 6(1):46–48

Google Scholar

Download references

Author information

Affiliations

Department of Information Technology, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu, India

R. Gopi & S. Selvakumar

Department of CSE, Sona College of Technology, Salem, India

V. Sathiyamoorthi

School of Computing Science and Engineering, VIT Bhopal University, Bhopal, India

Ramasamy Manikandan

Future Networking Research Group, Ton Duc Thang University, Ho Chi Minh City, VA, Vietnam

Pushpita Chatterjee

School of Computer Science and Engineering SCE, Taylor's University, Subang Jaya, Malaysia

N. Z. Jhanjhi

Department of Electrical & Communication Engineering, The PNG University of Technology, Lae, Papua New Guinea

Ashish Kumar Luhach

Corresponding authors

Correspondence to Pushpita Chatterjee or N. Z. Jhanjhi.

Additional information

Publisher's note

Rights and permissions

About this article

Cite this article

Gopi, R., Sathiyamoorthi, V., Selvakumar, S. *et al.* Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. *Multimed Tools Appl* (2021). https://doi.org/10.1007/s11042-021-10640-6

Download citation

- Received29 June 2020
- Revised04 January 2021
- Accepted04 February 2021
- Published24 February 2021
- DOIhttps://doi.org/10.1007/s11042-021-10640-6

Keywords

- ANN
- DDoS attacks
- Multimedia IoT
- Network attacks
- Training