Securing IoT Network against DDoS Attacks using Multi-agent IDS

Bedine Kerim
Department of Information Technology, College of Computer Science and Information Technology Albaha University, Saudi Arabia
bkerim@bu.edu.sa

Abstract. The crucial issue of Internet of Things (IoT) is vulnerable towards various kinds of security threats, especially on denial-of-service (DoS) attacks as IoT network consists of millions of devices attached to the network. There are plenty of intrusion detection systems (IDSs) available for IoT networks, however, the accuracy detection yet still a big problem. To address the problem, this paper proposes an ensemble IDS for IoT networks. The proposed IDS uses Multi-agent System (MAS) concept and ensemble the Information Gain feature selection algorithm with J48 classifier algorithm for the proposed IDS. Experimental results show the proposed MAS-J48-IDS provides the best accuracy performance of 99.8% for all selected features compared to IDSs that use Naïve Bayesian (NB) and Random Forest (RF) classifiers. Besides, the use of MAS contributes towards the load balancing among the nodes in the network itself.

1. Introduction
Traffic data in IoT network is created by sensors and then transmitted using wireless or wired communication channel. Thus, IoT communication channel should be able to deal with gigantic traffic volumes produced by a massive collection of devices/sensors with almost zero dropped packets during the transmission and protection on external edges [1,2]. Security/protection mechanisms to such system/network require must be efficient and effective as the nature of the IoT system/network consists of resource limited devices and the environment is unattended operationally. In addition, IoT system/network uses the Internet platform for exchanging information between heterogeneous edge devices, thus, it is susceptible to different security issues [3,4]. The most needed security service in IoT system is the availability of objects’ services. Denial-of-service (DoS) or distributed DoS (DDoS) attacks launch the outbreak to the targeted network with unwanted traffic to affect the services availability. Thus, we need robust IDS to detect early this most common attack on the IoT’s Network Layer [5].

Umar et al. [6] have discussed that IDS is timely possible to detect DDoS attack. In this paper, the IDS uses J48 classifier algorithm and is implemented as multi-agent system (MAS), where the agent as a software entity can perform autonomous activities in the environment. The agents perform different task, i.e.: data acquisition and traffic monitoring. The agents cooperate through communication. The proposed IDS is experimented using CICIDS-2017 dataset.
2. Related Work

DoS or DDoS is considered as the most dangerous type of attack in IoT networks/systems, because this attack may disrupt the services availability of an IoT systems/network. DoS launches attack by flooding targeted network with a massive and integrated traffics with the aim is to consume targeted system’s resources, causing legitimate users cannot access to the system services [7],[8]. Two main techniques to launch DDoS attacks in IoT networks/systems, i.e: by sending some crafted packets to the target hosts/nodes to manipulate any running applications or even protocols, or by performing one either: (i) network DDoS attacks that disrupting users on the connectivity [7], or (ii) application-layer DDoS attacks that draining the server resources such as: memory, CPU, sockets, and bandwidth for database accessing and Input/output processing [8], Thus, protecting IoT networks/systems against DDoS attacks becomes remarkable interests for security experts.

Many research works on IoT security have been carried out. Table 1 summarizes some of them that very close to the work in this paper with the consideration of their IoT vision and security aspect they focus on.

| Authors          | Year | IoT vision                                      | Security aspect |
|------------------|------|------------------------------------------------|-----------------|
| Mehmoed et al [9] | 2018 | Multi-agent system (MAS) and                    | Id  | √  | √  | √  |
|                  |      | Feature selection/classification                | Au  | √  |    |    |
| Zouai et al [10] | 2017 | MAS & Ambient Intelligence                     | In  |    | √  |    |
| Hasan et al [11] | 2017 | MAS & Encryption                               | Pr  |    |    |    |
| Ali et al [12]   | 2016 | IoT security                                   | Tr  | √  |    |    |
| Granjal et al [13]| 2015 | 5-Layer architecture                           | AC  |    |    |    |
|                  |      |                                                 | Co  |    |    |    |

Note:  
Id = Identification; Au = Authentication; In = Integrity; Pr = Privacy; Tr = Trust;  
AC = Access Control; Co = Confidentiality.

Furthermore, Mehmoed et al. [9] have combined MAS and Naive Bayesian feature classification to develop IDS that protects the IoT networks/systems against the DDoS attacks, and showed that it has better performance compared to the conventional IDS.

Liao et al. [14] define the intrusion detection as a method implemented to protect systems/networks from the outsider threats. Basically, the method works by matching the captured traffic’s feature and features/signatures already stored in a database. If certain features/signatures matched, then trigger an alert. Based on the techniques used for comparing the features, the IDS is categorized into five types, i.e.: statistical/Bayesian, heuristics, pattern matching, rule-based, and state-based. The IDSs should be able to identify distinctive characteristics/features of the intrusion malware, specifically in term, when and where it happened as well as the intrusion variety. Thus, IDS is deployed to enable identification and access prevention of unauthorized as well as misusing and abusing privileges of legitimate users.

The performance of the IDS depends on the classification algorithm used. J48 classifier is a decision tree-based machine learning algorithm. J48 classifier uses the entropy concept in creating its decision tree from a set of training data [15]. The basic steps of J48 classifier are as follows.

- Produce a leaf if the instances fall to the same class, returns the leaf with labeled with the same class.
- Calculates the gain in information of every attribute, using the attributes’ entropy.
- Determine the best attribute(s) based on the selection criterion and do the branching.

Researchers in [16] have reported that J48 provides high accuracy in detecting malicious activities in a network.

With regards to the intrusion detection, implementation of multi agent system (MAS) may decrease dramatically the nodes’ workload by allocating the loads among the nodes, as agents in MAS collaborate independently in gathering and communicating the data in the systems/networks. MASs gives autonomic self-management characteristic to sensors attached to IoT systems/networks.
3. Methodology
Figure 1 illustrates the overall architecture of the experimentation on the proposed IDS.

- **CICIDS-2017 Dataset**
The Canadian Institute for Cybersecurity Intrusion Detection System 2017 (CICIDS-2017) dataset is developed at ISCX Consortium. The dataset consists of eight traffic monitoring sessions, each is in the form of a comma separated value (CSV) file. The dataset has two types of traffic: normal traffic (Benign) and anomaly traffic (Attacks). The CICIDS-2017 dataset consists of 128,027 records of DoS/DDoS out of 2,830,743 total records with 77 features and 14 types of attacks.

- **Information Gain feature selection**
Information gain transforms a dataset with the aim to reduce entropy or surprise and calculated by comparing the entropy of the dataset before and after a transformation. It is often used in training decision trees.

- **Pre-processing**
The pre-processing operations on raw dataset of CICIDS-2017 include data creation, features construction and features reduction, data transferring, replace missing values and discretization, data normalization, and feature selection. The output of this pre-processing is clean dataset. For the experiment purpose, this work use 70% of the data as training dataset and 30% of the data as testing dataset (30%). The algorithm1 illustrates the preliminary stage, consists of pre-processing and the classification steps (adopted from [9]).

**Algorithm1: Preliminary stages**

**Input:** Dataset, Traffic Attributes, Record, Agent-ID, Actuator-Task;

**Output:** Features, label

**Start**
Perform Feature Extraction on Dataset using Information Gain;
   /select set of features from attributes/
Perform Feature Classification using J48;
   **if** RF = Normal **then**
      Execute Actuator-Task;
   **else**
      Continue gathering more Record of information from other Agents;
   **End-if**
**End**

- **Training the IDS with J48 classifier**
The next step is to train the IDS with the J48 classifier using training dataset. The output of this process is the trained IDS. Lastly, the trained IDS is tested on the testing dataset, and the performances are measured.

![Figure 1. Overall System Architecture](image-url)
The implementation of the MAS is illustrated in Figure 2. Four types of agents are implemented. Acquisition Agent that collects the traffic attributes from the dataset and then distributes traffic features. Monitoring Agent controls any information on anomaly/irregularity. Communication Agent is responsible on communication among the agents, and Actuator Agent is an executor for updating occurred events.

![Figure 2. MAS implementation](image)

The flowchart of the proposed IDS is shown in Figure 3. It starts with classifying the traffic information. If anomaly/irregular behaviour is identified then more detail analysis is performed to clarify further the circumstances. At the same time, the system will trigger alert and take suitable action to avoid the attacks. The detected attacks information then is dispatched to other agents/routers for the purposed of updating information.

![Figure 3. Flowchart of the detection process](image)

4. Experimental Setup, Results and Discussion
The J48 feature selection is implemented using WEKA Tool version 3.9 and the whole IDS is implemented in Python Language program on computer with the following specification. Processor: Intel Core i7, RAM: 16 GB, and Operating System: Windows 10. Experiment was conducted and the proposed MAS-J48-IDS performances are recorded.

J48 feature selection produces 15, 23, 34, 52 and 57 features that provide optimum criteria. Table 2 lists the performance in term of accuracy of the proposed IDS compared to IDSs’ that use Naïve Bayesian (NB) and Random Forest (RF) feature selection algorithm, for different number of selected features. A screenshot of running J48 classifier on Weka Tool is shown in Figure 4.
Table 2. Detection Performance & Comparison

| Feature Selection Algorithm | Normal | DDoS | Normal | DDoS | Normal | DDoS | Normal | DDoS | Normal | DDoS |
|-----------------------------|--------|------|--------|------|--------|------|--------|------|--------|------|
| NB                          | 0.305  | **0.965** | 0.359  | 0.723 | 0.692  | 0.673 | 0.357  | 0.724 | 0.4    | 0.715 |
| RF                          | 0.998  | **0.998** | 0.998  | **0.998** | 0.997  | 0.997 | 0.998  | 0.997 | 0.998  | 0.997 |
| J48                         | 0.978  | 0.97 | 0.981  | **0.998** | 0.983  | **0.998** | 0.978  | **0.998** | 0.973 | **0.998** |

Figure 4. Screenshot of the running J48 on Weka Tool

Experiment on observing the performance with considering the traffic load also was carried out. Figure 5 depicts the comparison of detection rate performances against the throughput. The figure shows that he proposed IDS outperforms the other IDSs that use Naïve Bayesian and Random Forest feature selection algorithms. The results also show that the higher the throughput, the higher the performance.
Figure 5. Comparison of the Detection Performance vs. Throughput

The experimental results displayed on Table 2 exhibit that the proposed MAS-J48-IDS performs better compared to Naïve Bayesian-based IDS and only slightly better compare to Random Forest-based IDS. The proposed IDS also is able to detect the DoS/DDoS attacks consistently using different number of features.

5. Conclusions and Future Work

Experimental results show that the proposed MAS-J48-IDS is a promising tool for detecting intrusions in IoT system/network. Intrusion Detection System with ensemble of Information Gain feature selection and J48 classifier, then incorporated into multi-agent system outperforms the IDSs with Naïve Bayesian or Random Forest classifiers. The proposed IDS achieves 99.8% accuracy detection for almost all of the selected feature numbers. The implementation of the MAS as distributed agents on the IDS balances the energy/power consumption as the overall computation load is distributed among all the nodes in the network. This advantage addresses the issue of limited energy/power of devices attached to IoT system/network.

In the future, the author plans to expand the work through an implementation of ensemble IDS using combination of several classifier algorithms. Furthermore, the number, the types, and the natures of the agent can be further elaborated.

References
[1] Ullah I, Shah MA, Wahid A, Mehmood A, Song H 2018 ESOT: a new privacy model for preserving location privacy in Internet of Things. *Telecommun. Syst.* 67 4 p.553–575
[2] Khan R et al. 2012 Future internet: the Internet of Things architecture, possible applications and key challenges. *Proc. of 10th IEEE International Conference on Frontiers of Information Technology (FIT).*
[3] Mehmood A, Lloret J, Sendra S 2016 A secure and low energy zone-based wireless sensor networks routing protocol for pollution monitoring. *Wirel Commun Mob Comput* 16 17 p. 869–2883.
[4] Borgohain T, Kumar U, Sanyal S. 2015. Survey of security and privacy issues of Internet of Things. *arXiv preprint arXiv:1501.02211. *
[5] Fremantle P, Scott P. 2015. A security survey of middleware for the Internet of Things. *PeerJ PrePrints*, 3:e1521.
[6] Prasad KM, Reddy ARM, Rao KV 2014 DoS and DDoS attacks: defense, detection and traceback mechanisms—a survey. *Global J. Comput. Sci. Technol.* 14 7 p.1–19
[7] Zargar ST, Jyoti J, Tipper D 2013 A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Commun. Surv. Tutor* 15 4 p. 2046–2069
[8] Umar MM, Mehmood A, Song H. 2016. SeCRoP: secure cluster head centered multihop routing protocol for mobile ad hoc networks. *Secur. Commun. Netw.* 9 16 p. 3378–3387.
[9] Mehmood A, Mukherjee M, Ahmed S.H. et al. 2018 NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. *J. Supercomput.* **74** p. 5156–5170.

[10] Zouai M, Kazar O, Haba B, Saouli H, & Benfenati H 2017 IoT approach using multi-agent system for ambient intelligence. *Intl. J of Software Engineering and its Applications* **11** p.15-32.

[11] Hasan H, Salah T, Shehada D, Zemerly J, Chan Y.Y, Al-Qutayri M, Al-Hammadi Y. 2017. Secure lightweight ECC-based protocol for multi-agent IoT systems. *Proc. of 13th IEEE Intl. Conf. on Wireless and Mobile Computing, Networking and Communications*, Rome, Italy, 9-11 October, 2017 p. 692-700.

[12] Ali I, Sabir S, Ullah Z, Internet of Things Security 2016. Authentication and access control: A review. *Int. J. of Comp. Sci. and Inf. Security* **14** 8 p. 1-11.

[13] Granjal J, Monteiro E, Silva J. 2015 Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communication Survey and Tutorial*, 2015 **99** p.1..

[14] Liao H-J et al. 2013 Intrusion detection system: a comprehensive review. *J Netw. Comput. Appl.* **36** 1 p.16–24.

[15] Buczak A. and Guven E 2015 A survey of data mining and machine learning methods for cyber security intrusion detection, *IEEE Commun. Surv. Tutorials* **99**:1-.

[16] Sahu S. and Mehtre BM. 2015. Network intrusion detection system using J48 Decision Tree. *Proc. of 2015 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI* 2015 p. 2023–2026.