


NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks

Amjad Mehmood¹ · Mithun Mukherjee² ·
Syed Hassan Ahmed³ · Houbing Song⁴  ·
Khalid Mahmood Malik⁵

Published online: 19 May 2018

© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract Internet of Things (IoT) makes physical objects and devices interact with each other through wireless technologies. IoT is expected to deliver a significant role in our lives in near future. However, at the current stage, IoT is vulnerable to various kinds of security threats just like other wired and wireless networks. Our work mainly focuses on protecting an IoT infrastructure from distributed denial-of-service attacks generated by the intruders. We present a new approach of using Naïve Bayes classification algorithm applied in intrusion detection systems (IDSs). IDSs are

✉ Houbing Song
h.song@ieee.org

Amjad Mehmood
dramjad.mehmood@ieee.org

Mithun Mukherjee
m.mukherjee@ieee.org

Syed Hassan Ahmed
sh.ahmed@ieee.org

Khalid Mahmood Malik
mahmood@oakland.edu

- ¹ Institute of Information Technology, Kohat University of Science and Technology, Kohat, Pakistan
- ² Guangdong Provincial Key Lab of Petrochemical Equipment Fault Diagnosis, Guangdong University of Petrochemical Technology, Maoming 525000, China
- ³ Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816, USA
- ⁴ Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA
- ⁵ Department of Computer Science and Engineering, Oakland University, 532 EC 115 Library Drive, Rochester, MI 48309-4479, USA

deployed in the form of multi-agents throughout the network to sense the misbehaving or irregular traffic and actions of nodes. In the paper, we also discuss the fundamental concepts related to our work and recent research done in similar area.

Keywords Internet of Things · IDS · Naïve Bayes classification · DDoS · Routing security · MAS

1 Introduction

Currently, Internet of Things (IoT) [1–4] is the most addressable area for researchers as it acquires adequate and further necessary development in many aspects. The term IoT is elucidated by various authors from different outlooks. It can be defined as “A smart world where people live in a smarter way among smart objects and things”. It is predicted, in the near future, that the technologies of wireless networks with sensors and invisible embedded information systems gradually become essential components of human environmental necessities [5]. The technologies involved in the employment of the IoT are radio-frequency identification (RFID), near-field communications (NFC), machine-to-machine communications (M2M), and vehicular-to-vehicular communications (V2V) [6–10]. IoT can be classified as a network of connected things like RFID tags, actuators, sensors, smart phones, and other handled and mobile wireless devices [11]. The motivation is to share, embed, and exchange the real-world data among all the involved objects in a network [12, 13].

In IoT, the data are collected via sensors and then sent through wired or wireless communication channels in networks. The communication system is desired to be able for handling enormous amount of data from a huge number of sensors without any loss and secured from external interfaces [14, 15]. Due to resource-constrained nature and unattended operational environment of the involved devices in IoT, it is an important issue for researchers to propose and implement effective and efficient security approaches in such systems. Moreover, IoT is prone to different security issues as it uses the Internet infrastructure for exchange of information among various heterogeneous ends [16, 17]. For any IoT system, the essential security objectives are to ensure the appropriate authentication mechanism and deliver integrity and confidentiality about the data. A threat of any of these areas could create unavoidable issues to the system. The availability of services of objects in such systems is always desirable, which may be troubled using denial-of-service (DoS) attack by the malicious intruders. DoS attacks can be generated on various layers of sensor networks starting from physical to applications layers [16]. Moreover, such attacks in the RFID technology take to breakdown in reading RFID tags temporarily or sometimes permanently. DoS attacks reduce an RFID tag to misbehave or give wrong data under the scan. These DoS attacks can be initiated from remote locations and in distributed manner known as distributed DoS (DDoS) attacks.

Due to complexity and heterogeneity of connected objects in the IoT networks, DDoS attack is the most common attack on the network layer of IoT infrastructure. These attacks are carried out for two main purposes: (1) to get down the system and (2) to aid a spoofing or authentication attack [18, 19]. The network layer of IoT is also

vulnerable to Trojan horses, viruses, spam and some other attacks which causes the unavailability of resources, information disclosure and network paralysis.

By using a secure intrusion detection system (IDS), prevention and detection of DDoS attack is timely possible [20,21]. The IDSs use the agents for data collection and monitoring of network data traffic and nodes' behaviors. An agent is a software entity that is capable of performing autonomous activities in its environment, in a flexible and intelligent manner regarding the achievement of its particular goal. Thus, a multi-agent system (MAS) is a system comprised of collection of autonomous agents that can collaborate with each other to learn and exchange experiences. The cooperation among various agents is generally achieved by means of communication. The Bayesian classification is a managed learning method and also a statistical method for classification. It is a probabilistic model which enables us to know uncertainty about a model in a principled way by using probabilities of the results. It can be used to answer diagnostic and predictive issues. In order to check the efficacy of the NSL-KDD dataset,¹ a Naïve Bayes classifier algorithm is used to model the normal and abnormal network activity. The Naïve Bayes classifier is a supervised learning algorithm based on applying Bayes' theorem [22,23]. It is one of the simplest models that can be used for classification and predictions.

1.1 Contribution

Our proposed Naïve Bayesian algorithm with multi-agent-based IDS (NB-MAIDS), against the potential threats of DDoS attacks in IoT, is based on Naïve Bayes classifier algorithm along with the implementation of multi-agents throughout the network. The agents gather information through sensors. Afterward, the gathered information is analyzed for further processing. The attacks can be prevented by reporting the malicious nodes' activities information to either the connected IoT objects or the administrator. Moreover, the IDS-based systems are more feasible for the IoT environment due to their less implementation and execution costs.

The rest of the paper is organized as follows. Section 2 presents the preliminaries and related work. Section 3 discusses our proposed scheme. The simulation results are presented in Sect. 4. Finally, conclusions are drawn in Sect. 5.

2 Preliminaries and related work

This section includes the basic concepts needed to be understood before implementing our work and a brief survey on the work related to our proposed scheme.

2.1 DDoS attacks

The DoS and DDoS attacks are indeed very thoughtful issues for security in the Internet. The primary goal of such attacks is to disrupt the services by flooding an

¹ <https://web.archive.org/web/20150205070216/http://nsl.cs.unb.ca/NSL-KDD/> accessed on 21-April, 2018.

Table 1 DDoS attacks on IoT

| Layer | Attacks |
|---------------------------|---|
| Perception layer-RFID | (a) Jamming, (b) Kill Command, and (c) De-synchronizing Attack |
| Perception layer-802.15.4 | (a) Wide-band denial and pulse denial, (b) Node-specific and message-specific denial, and (c) Bootstrapping attacks |
| Network layer-WiFi | (a) ICMP flooding attack and (b) IP spoofing |
| Network layer-ZigBee | (a) Hello flooding, (b) Homing attack and (c) Black hole attack |
| Application layer | (a) Reprogramming attack and (b) Path-based DoS |

unnecessary huge traffic over the network. DDoS is relatively simple but one of the most powerful type of attack. Protection against DDoS flooding attacks are one of the tremendous interests for security professionals. DDoS flooding attack is a massive, integrated and generally explicit in nature which attempts to exhaust victim's bandwidth or disrupt legitimate users' access to the system services [24,25]. There are two prime techniques to launch DDoS attacks in the Internet-based systems like IoT. The first technique is that attackers send some malfunctioned packets to the victim to confuse a protocol or application running on it. The other technique is the most common one, in which attackers try to do one or both of the following:

- (a) The attackers disrupt a legitimate user's services by exhausting the server resources like: memory, CPU, sockets, I/O bandwidth and disk/database bandwidth. These are typically application-level flooding attacks [25].
- (b) The attackers upset an authentic user's connectivity by exhausting the bandwidth, router processing capability, or network resources. These are typically network DDoS flooding attacks [24].

Table 1 shows the layer-wise distribution of DDoS attacks of IoT [26].

2.2 Intrusion detection system (IDS)

The IDSs continuously monitor the activities and users' actions in a network to detect intrusions and the irregular activities. It is very difficult and costly to implement a system that is not prone to attacks. A network can suffer from different types of security holes. The IDSs analyze the events and actions generated by users' operations and search out the suspicious and undesirable activities generated by malicious nodes [27]. An intrusion detection is a technology used for securing networks from the malicious attacks. The IDSs offer some usable information to the helpful preparation for protection purpose; like unique identification of the malicious intruder, time, and location of the intrusion and type of the intrusion. With the help of such information, the further or redundant intrusions can be prevented by the system. By implementing an IDS, the system is enabled to identify and prevent access of unauthorized and also legitimate users' misusing and abusing their privileges. The IDSs can be classified as statistical or Bayesian-based, pattern matching-based, rule-based, state-based, and heuristics-based [28].

Some effective IDSs can be developed such as they have the capability to sense events and send warnings to the whole network or the administrator about the possible security threats. An ideal IDS besides detection of security breach and informing others, it also automatically develops a protective response against the threats.

2.3 Multi-agent system (MAS)

The agents in MAS independently collect the data and communicate with one another in coordinated and supportive way to achieve a common goal. Each agent operates on a control algorithm and when required, it can communicate with other agents. In the context of intrusion detection, the multi-agents can drastically reduce the work load on nodes in a network by distributing responsibilities among them. Implementing MASs in a system is the most appropriate method to attain the goals in distributed systems [29].

Some notable characteristics of agents in MAS are like autonomy, reactivity and pro-activeness [30]. Agent-based IDS gives an idea to divide the workload through distributed IDS so that the speed of network operations can be boosted. In such IDS environment the agents can be distributed and/or mobile [31]. According to [32], MASs empower the platform for sensors with the autonomic self-management property.

2.4 Naïve Bayes (NB) classifier algorithm

Naive Bayes methods are a set of managed knowledge gathering algorithms based on using Bayes theorem with the ‘Naïve’ assumption of individuality between every pair of features. In order to check the efficacy of the NSL-KDD dataset a Naïve Bayes classifier algorithm was used to model the normal and abnormal network activity. The Naïve Bayes classifier is a supervised learning algorithm based on applying Bayes’ theorem [22]:

$$P(H|E) = \frac{P(E|H)P(H)}{P(E)}, \quad (2.1)$$

and

$$P(H|E) = P(E_1|H) \times P(E_2|H) \times \dots \times P(E_n|H) \times P(H) \quad (2.2)$$

According to this theorem, we can calculate the probability of event H conditioned on the data E by first calculating the probability of the data E conditioned by event H multiply by the probability of event A and normalized by the probability of the data E . In case of Intrusion detection, this means that we can calculate the probability of an attack is occurring based on some data by first calculating the probability that some preceding data were part of that type of attack and then multiply by the probability of that type of attack occurring, dropping the normalization of $P(E)$ [22].

2.5 Related work

A reasonable work has been done in the area of securing communication networks. In [33], authors proposed an intrusion detection system for DoS detection in IPv6 over low-power wireless personal area networks (6LoWPAN)-based IoT. They designed an architecture to detect DoS attacks in ebbits networks. Basically, they integrated the 6LoWPAN with the network manager of ebbits. Moreover, the IDS probe (IDS-P) helps the IDS to listen 6LoWPAN network traffic. In addition, a DoS protection manager is integrated and the IDS with the ebbits network manager works as the security manager.

Furthermore, Sen [34] presented the framework of Distributed IDS (DIDS) which consists of a set of autonomous agents that cooperates with other to perform a distributed intrusion detection procession. The DIDS can detect both signature-based and anomalous activities in real-time by using distributed computation and message passing scheme among the agents. Multiple sectioned Bayesian networks are used to make distributed inferences. The IDSs have the capability to identify and isolate the suspicious nodes in the system with the help of Byzantine agreement p. A multi-agent system for intrusion detection (MASID), developed by Mechtri et al. [30], is an intrusion detection system for ad hoc networks. It is based on a multi-agent switch in a distributed and cooperative architecture. There is no need of the presence of any central entity in the entire system. Due to distributed nature of the system, the fault tolerance is increased, and the system failure is impossible. With implementation of agents, the authors used more flexible and completely automated intrusion detection processes.

Moreover, in [35], authors proposed a framework of Naïve IDS (NIDS) based on Naïve Bayes algorithm. The framework generates the pattern of the network services over data set labeled by the services. By using Naïve Bayes classifier algorithm, the framework detects the attacks with build-in patterns.

The authors in [36] designed an intrusion detection system for the IoT system called as SVELTE. They proposed their work securing systems from routing attacks specifically and other various attacks in general. The designed model is also compatible with IPv6-connected IoT. The SVELTE is an IDS giving positive results with small overhead deployment and limited energy consumption. However, the proposed system gives a noticeable number of false alarms during the detection process.

The techniques of artificial immune system, proposed in [37], are implemented in an IoT environment. An immune system is constructed and applied to detect possible attacks. A library is kept for defining attacks' information and the immune system evolves as the data in library are updated. The system seems to be incomplete in some cases and also puts an extra burden on the processing nodes.

3 Naïve Bayesian algorithm with multi-agent-based IDS

The motivation of our work is to deliver a solution for detection and prevention of DDoS attacks in Network layer of IoT infrastructure. Before network operations are

disrupted, the system prompts the proper execution of countermeasures aiming to increase network availability.

The work NB-MAIDS is an agent-based intrusion detection system for securing connected objects in IoT. The agents are viewed as autonomous, reflective, proactive and cooperative entities in the system. These are responsible for data collection, analysis and development of suitable inferences based on the analyzed data. Naïve Bayes algorithm is used for the classification of events data gathered by monitoring the network operations.

3.1 Architecture of the multi-agent system (MAS)

Each IDS in distributed routers consists of four types of agents, playing different but correlative roles, and cooperating with each other. These agents are either stationary or mobile agent, depending on the task which they perform. Furthermore, they adopt one of two different architectures: the proactive or deliberative. Agents of both types of architectures share some useful characteristics among them. Each agent is autonomous, intelligent, cooperative, rational, and capable of communicating with other agents. By employing the agents, we then look for a complete automation process of the detection. The agents are listed as follows:

- (a) *Collector agent* The collection agent is a reactive agent that is responsible for collection of audit or network data from source. We suggested My SQL as a data source from where collector agent collects data results of NSL-KDD Cup classified by Naïve Bayes classifier algorithm.
- (b) *System monitoring agent* The system monitoring agents are responsible for monitoring of the whole structure of MAS. It confirms whether the classified resultant data is normal or an attack. For this purpose, it looks up for previously detected data, if evidences are not enough, then it further collects more information from cooperating with IDSs with others.
- (c) *Actuator agent* The actuator agent is a deliberative agent. Its main functionality is to react to the detected intrusions, as quickly as possible, to avoid future damages. An active response may include dropping of the connectivity to the potential attacker. It is also concerned with the update of normal and attack profiles in the database.
- (d) *Communication agent* The communication agent serves as a communication channel. This mobile agent is decision-making to share information with agents in sub-domain to which it belongs as well as inform IDSs in distributed nodes with the detection of the results and, if needed, inquire them for more information.

As shown in Fig. 1, the agents of MAS are connected together to perform various operations collectively. The figure shows that collection agent is directly connected to the Naïve Bayes database. The flowchart in Fig. 2 shows that the information is first of all classified and if an abnormal traffic is detected then the system further analyzes the situation. In the flowchart, it is shown that both results of attack confirmation are forwarded to other routers for knowledge update. If the system finds an attack situation, then it takes appropriate action for avoidance of such attacks.

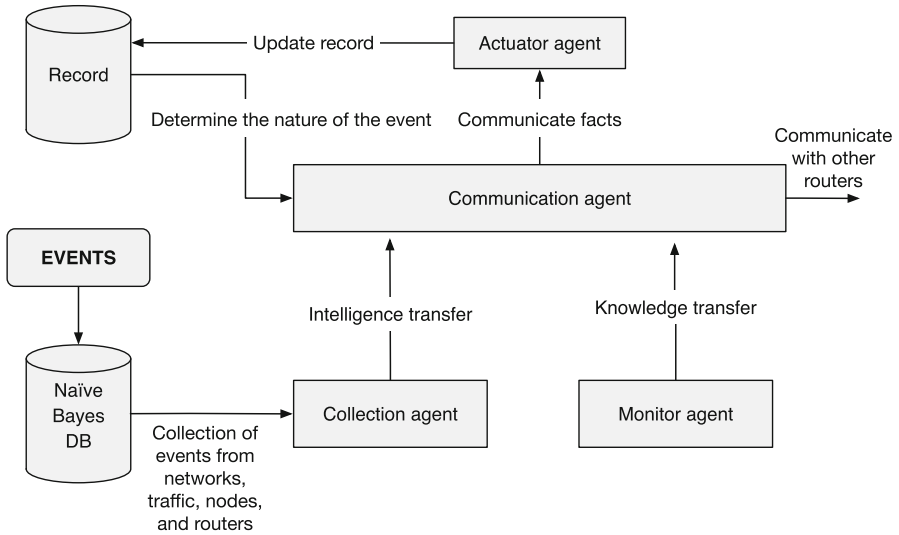


Fig. 1 Multi-agent system

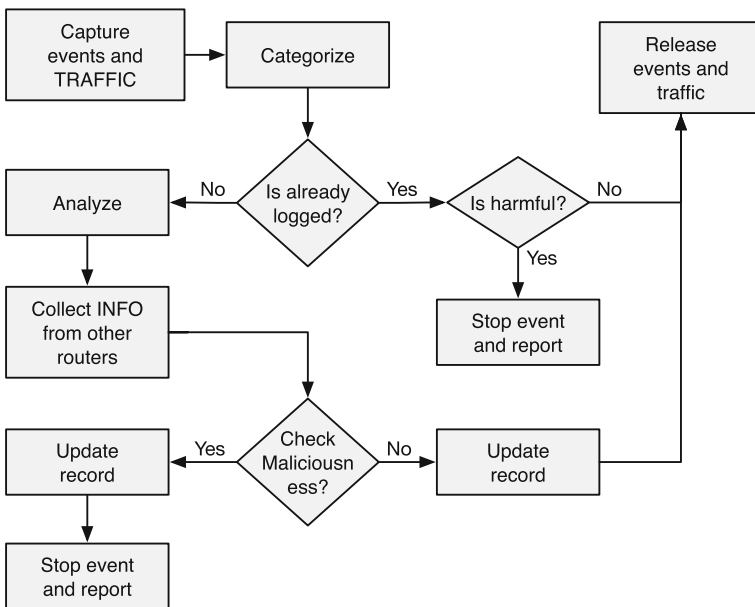


Fig. 2 Flowchart of the proposed algorithm

The three stages of the proposed model are illustrated in Figs. 3, 4 and 5. In the first phase, the system processes the data for Naïve Bayes classification. The module considers some domain knowledge, attack graphs, and process it with the help

Fig. 3 Stage 1—data preprocessing in NB-MAIDS

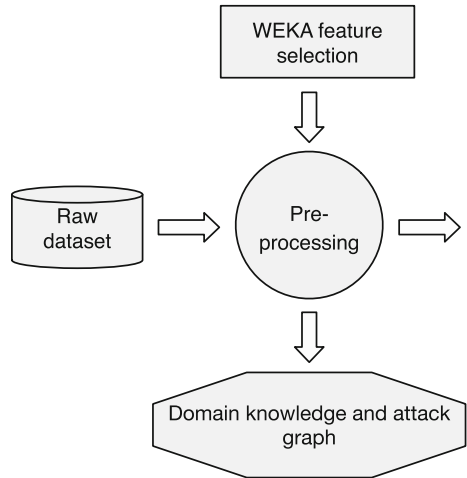


Fig. 4 Stage 2—Naïve Bayes network model and training

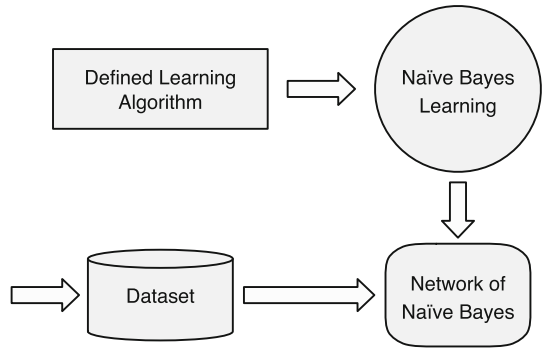
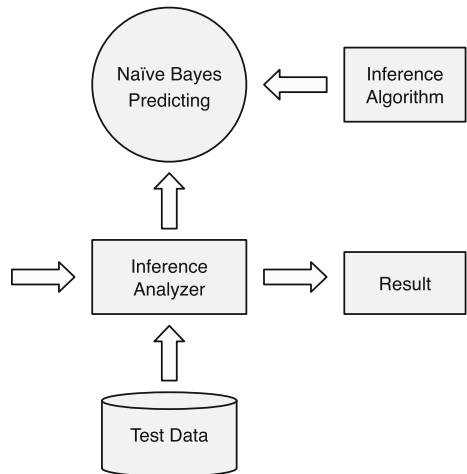


Fig. 5 Stage 3—test data classification



Algorithm 1: Preprocessing and Classification

```

1 Input: NT, Prep, Attributes, Classify, NB, Info, Routers, Task;
2 begin
3   Prep NT: Removal of unnecessary attributes;
4   Classify NT via NB ;
5   if NT = Normal then
6     | Processed to perform task;
7   else
8     | Collect more info from other Routers;
9   end
10 end

```

Algorithm 2: Store Results

```

1 Input: Attack, ABN, DB, N, Alert;
2 begin
3   if Attack = Confirmed then
4     | Update ABN Behavior DB;
5   else
6     | Update N Behavior DB;
7   end
8   do
9     | Broadcast to Inform other Routers;
10    while Attack = Confirmed || Attack ≠ Confirmed;
11    if Attack = Confirmed then
12      | Broadcast Alert;
13    end
14 end

```

of WEKA,²-based selection mechanism. In this stage of preprocessing, the dataset is normalized and unnecessary attributes and instances are removed as per defined principles.

In stage 2, the processed data are collected by the system. The network of Naïve Bayes learning agent analyzes the dataset provided with the help of a predefined algorithm. This stage inputs the phase of test data classification.

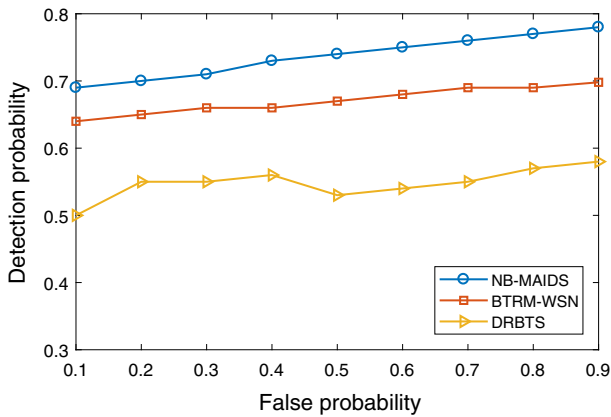
Figure 5 shows the last phase, stage 3, of the whole process. An inference analyzer is used to execute the test data with the help of the Naïve Bayes prediction mechanism to produce the ultimate conclusions in the form of results.

The procedure is further explained with the help of following algorithms. Algorithm 1 discusses the preprocessing and classification of data and Algorithm 2 updates the dataset with information about new suspicious attack information, both true or false results.

² <https://sourceforge.net/projects/weka/> Accessed on April 21, 2018.

Table 2 Simulation parameters

| Parameters | Values |
|---------------------------|----------------------------|
| Simulator environment | NS 2.35 under Ubuntu 14.04 |
| Number of nodes | 400 |
| Number of malicious nodes | Random |
| Nodes placement | Random |
| Transmission range | 250 m |
| Number of connections | 35 |
| Packet size | 512 bytes |
| Application traffic | CBR |

**Fig. 6** Relationship between false and detection probability of threats

4 Simulation results

For simulations and result evaluations, we perform the work simulated in NS 2.35 under Ubuntu operating system. Plots are taken at the average of each ten different runs. The source and destination nodes are selected randomly after injecting malicious behavior to some of them to determine the threat effectiveness and other values. The simulation parameters are summarized in Table 2.

Detection probability specifies that whether a model can detect the intrusions properly. In Fig. 6, Bio-inspired Reputation and Trust Model WSN (BRTM-WSN) [38] performs better compared to Distributed Reputation-based Beacon Trust System (DRBTS) [39] model. It is observed that the BRTM-WSN model have an improved handling mechanism for intrusions generated by malicious users. Our model gives better results than the other two due to the existence of distributed Naïve Bayes based agents in the networks.

The end-to-end packet-forwarding ratio is shown in Fig. 7. Results are made using Ad hoc On-Demand Distance Vector (AODV) routing protocol with and without our model. Some malicious nodes are injected to the system randomly. The percentage in gradually increased from 10 to 50 to collect various results.

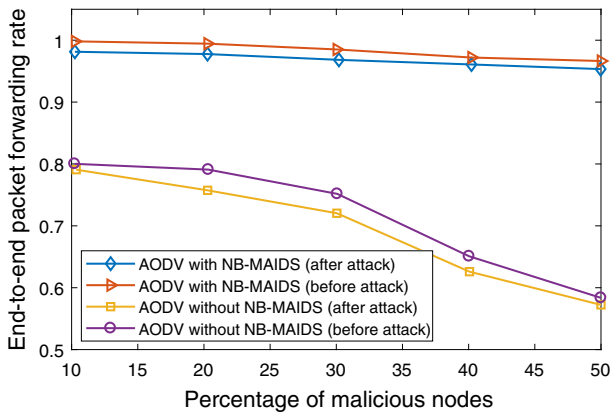


Fig. 7 End-to-end packet-forwarding rate with variable number of malicious nodes

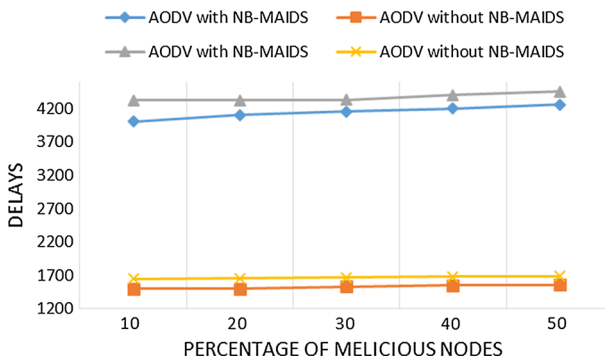


Fig. 8 Effect on performance in terms of delays

The end-to-end delay is shown in Fig. 8. As the system relies on IDS in MAS therefore it puts an extra delaying time as compared to a non-secured system. Results are taken by comparing our work with and without using AODV protocol.

Figure 9 shows the activity recorded at ten different time intervals. Each time the amount of packet dropped with and without a DDoS is recorded. The records indicate that the amount is decreasing with passage of time as the system learns and acquires knowledge in its dataset through agents in the IDS.

Figure 10 illustrates the detection ratios with respect to number of attacks. Our system detects anomalies more precisely as compared to a generic IDS for DDoS attack in the WSNs.

Finally, Fig. 11 shows the performance of detection rate with throughput of different methods. It is shown that the detection rate of our proposed system is significantly higher than BRTM-WSN [38], DRBTS [39], and optimal objective entropy (OOE)-based [40] methods.

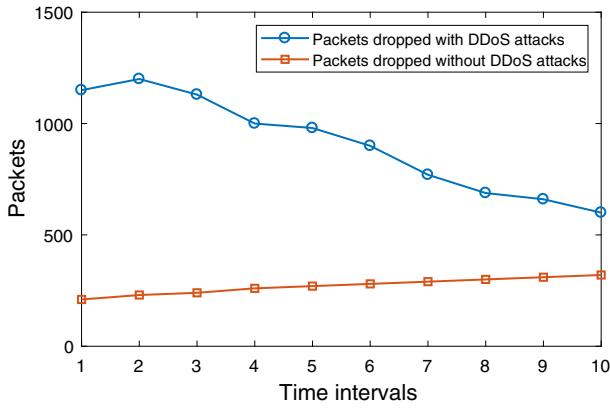


Fig. 9 Average packets dropped during no attack and DoS attack

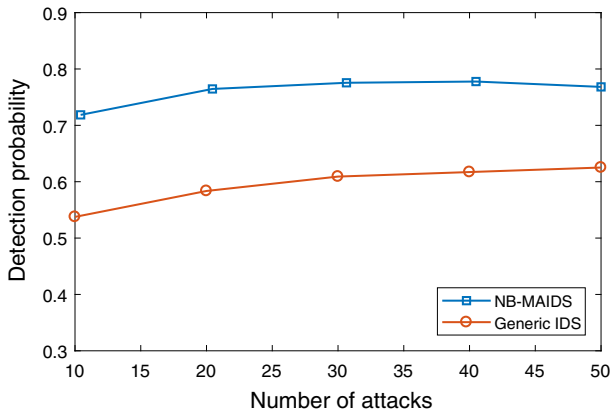


Fig. 10 Attack detection rates

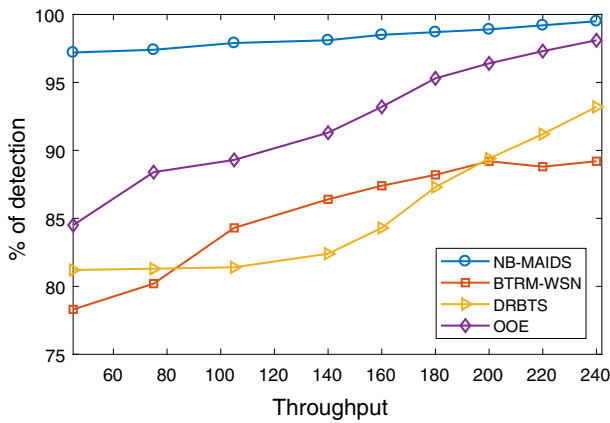


Fig. 11 Detection rates on different throughput

5 Conclusion

Since the technologies and concepts of wireless sensor networks and mobile ad hoc networks are supposed to be integrated in the next generation Internet as a core part of IoT, most of the work is influenced by practices developed for these networks. The proposed NB-MAIDS mechanism is an advanced system for the intrusion detection in a network. The Naïve Bayes classification algorithm with practice of multiple agents for the DDoS attacks detection gives better performance compared to the traditionally used IDSs. The proposed scheme aims to secure the IoT network layer from the DDoS attacks imitated by malicious objects. Due to the distributed agents on the MAS, the total load is distributed among all the participants in the network. In addition, the reporting of detection and preventions of attacks is performed very fast. This work can be further expanded by replacing the Naïve Bayes classification algorithm with a light-weight pattern matching algorithm. The types, nature, and number of agents can be further advanced.

References

1. Miraz MH, Ali M, Excell PS et al (2017) A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). arXiv preprint arXiv
2. Kumar JS, Patel DR (2014) A survey on Internet of Things: security and privacy issues. *Int J Comput Appl* 90(11):20–26
3. Farooq MU et al (2015) A review on Internet of Things (IoT). *Int J Comput Appl* 113(1):1–7
4. Said O (2013) Development of an innovative Internet of Things security system. *Int J Comput Sci Issues (IJCSI)* 10(6):155–161
5. Wang S, Wan J, Li D, Zhang C (2016) Implementing smart factory of industrie 4.0: an outlook. *Int J Distrib Sens Netw* 12(1):3159805
6. Mansor MN, Muna NU, Muhammad AS (2015) The potential of radio frequency identification (RFID) technology implementation in Malaysian Shipbuilding Industry. *J Transp Syst Eng* 2:31–36
7. Coskun V, Ozdenizci B, Ok K (2013) A survey on near field communication (NFC) technology. *Wireless Pers Commun* 71(3):2259–2294
8. Gao B et al (2015) On the overhead reduction of millimeter-wave beamforming training in wireless M2M network via multidevice multipath simultaneous training. *Int J Distrib Sens Netw* 1328–1333
9. Kuang LW, Mei-Tso L, Yu-Hsuan Y (2015) A machine learning system for routing decision-making in urban vehicular ad hoc networks. *Int J Distrib Sens Netw* 11:374391
10. Ploennigs J, Ryssel U, Kabitzsch K (2010) Performance analysis of the EnOcean wireless sensor network protocol. In: 2010 IEEE Conference on Emerging Technologies and Factory Automation (ETFA). IEEE
11. Aman W (2016) Assessing the feasibility of adaptive security models for the Internet of Things. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, pp 201–211
12. Vermesan O, Friess P, Guillemin P, Gusmeroli S, Sundmaeker H, Bassi A et al (2011) Internet of things strategic research roadmap. *Internet Things Glob Technol Soc Trends* 1:9–52
13. Mehmood A, Khanan A, Umar MM, Abdullah S, Ariffin KAZ, Song H (5694) Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks. *IEEE Access* 6:5688
14. Khan R et al (2012) Future internet: the Internet of Things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology (FIT). IEEE
15. 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):553–575
16. Borgohain T, Kumar U, Sanyal S (2015) Survey of security and privacy issues of Internet of Things. arXiv preprint [arXiv:1501.02211](https://arxiv.org/abs/1501.02211)

17. 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):2869–2883
18. Fremantle P, Scott P (2015) A security survey of middleware for the Internet of Things. *PeerJ PrePrints* 3:e1521
19. Mehmood A, Nouman M, Umar MM, Song H (2016) ESBL: an energy-efficient scheme by balancing load in group based WSNs. *KSH Trans Internet Inf Syst* 10(10):1–19
20. Jing Q et al (2014) Security of the Internet of Things: perspectives and challenges. *Wirel Netw* 20(8):2481–2501
21. 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):3378–3387
22. Palmer J (2011) Naïve Bayes classification for intrusion detection using live packet capture. In: Palmer J (ed) *Data mining in bioinformatics*. Springer, Berlin
23. Mehmood A, Umar MM, Song H (2017) ICMDs: secure inter-cluster multiple-key distribution scheme for wireless sensor networks. *Ad Hoc Netw* 55:97–106
24. Prasad KM, Reddy ARM, Rao KV (2014) DoS and DDoS attacks: defense, detection and traceback mechanisms—a survey. *Glob J Comput Sci Technol* 14(7):1–19
25. 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):2046–2069
26. Sonar K, Upadhyay H (2014) A survey: DDOS attack on internet of things. *Int J Eng Res Dev* 10(11):58–63
27. Sun B et al (2007) Intrusion detection techniques in mobile ad hoc and wireless sensor networks. *IEEE Wirel Commun* 14(5):56–63
28. Liao H-J et al (2013) Intrusion detection system: a comprehensive review. *J Netw Comput Appl* 36(1):16–24
29. Daneshfar F, Hassan B (2009) Multi-agent systems in control engineering: a survey. *J. Control Sci. Eng.* Article ID 531080, p 12. <https://doi.org/10.1155/2009/531080>
30. Mechtri L, Tolba FD, Ghanemi S (2012) MASID: multi-agent system for intrusion detection in MANET. In: 2012 Ninth International Conference on Information Technology: New Generations (ITNG). IEEE
31. Le A et al (2012) 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. *Int J Commun Syst* 25(9):1189–1212
32. Marsh D et al (2004) Autonomic wireless sensor networks. *Eng Appl Artif Intell* 17(7):741–748
33. Kasinathan P et al (2013) Denial-of-service detection in 6LoWPAN based Internet of Things. In: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE
34. Sen J (2010) An agent-based intrusion detection system for local area networks. *arXiv preprint arXiv:1011.1531*
35. Panda M, Patra MR (2007) Network intrusion detection using Naive Bayes. *Int J Comput Sci Netw Secur* 7(12):258–263
36. Raza S, Wallgren L, Voigt T (2013) SVELTE: real-time intrusion detection in the Internet of Things. *Ad Hoc Netw* 11(8):2661–2674
37. Liu C et al (2011) Research on immunity-based intrusion detection technology for the internet of things. In: 2011 Seventh International Conference on Natural Computation (ICNC), vol 1. IEEE
38. Marmol G, Perez M (2010) Providing trust in wireless sensor networks using a bioinspired technique. *Telecommun Syst* 46(2):163–180
39. Srinivasan A, Teitelbaum J, Wu J (2006) DRBTS: distributed reputation-based beacon trust system. In: *Proceedings of 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06)*, pp 277–283
40. Xiang Y, Li K, Zhou W (2011) Low-rate DDoS attacks detection and traceback by using new information metrics. *IEEE Trans Inf Forensics Secur* 6(2):426–437