Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, S. 279-286, Eylül 2020
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue, pp. 279-286, September 2020
Copyright © 2020 EJOSAT
Research Article

A Novel Hybrid IoT Based IDS Using Binary Grey Wolf Optimizer (BGWO) and Naive Bayes (NB)

Ismail Mohamed Nur[1*], Erkan Ülker[2]

[1] Konya Technical University, Faculty of Engineering, Department of Computer Engineering, Konya, Turkey (ORCID: 0000-0001-8171-3026)
[2] Konya Technical University, Faculty of Engineering, Department of Computer Engineering, Konya, Turkey (ORCID: 0000-0003-4393-9870)

(1st International Conference on Computer, Electrical and Electronic Sciences ICCEES 2020 – 8-10 October 2020)

(**DOI:** 10.31590/ejosat.804113)

ATIF/REFERENCE: Nur, I. M. & Ulker, E. (2020). A Novel Hybrid IoT Based IDS Using Binary Grey Wolf Optimizer (BGWO) and Naive Bayes (NB). *European Journal of Science and Technology*, (Special Issue), 279-286.

Abstract

One of the main objectives of intelligent environments is to enhance the quality of human life standard in terms of efficiency and comfort. The Internet of Things (IoT) model has newly evolved into the technology for establishing smart environments. IoT refers to physical things or devices which are able to exchange information with other devices. It is used in various fields such as smart home, smart city, industrial control, automobile industry, agriculture, intelligent transportation, home automation and appliances, healthcare, and many other fields. Moreover, it assures innovative business paradigms and advanced user experience. Privacy and security are counted as the key problems in any real-world intelligent environment for the IoT paradigm. Therefore, to implement the security of the IoT systems is becoming the first priority and big area of interest in the successful distribution of IoT networks. The open holes of security in IoT related systems create security risks that impact the smart applications. Mirai botnet is an example of one of the novel attacks that launched recently. The network of IoT is protected with authentication and encryption, but it can't be mitigated against malicious and harmful attacks. Thus, IoT based Intrusion Detection System (IDS) is required to detect the attacks. In this paper, a novel hybrid IoT based IDS using Binary Grey wolf optimizer (BGWO) and Naive Bayes (NB) is presented to defend and secure intrusions on the IoT network. BGWO is used as feature selection and NB as a classification method. The results are compared with other optimization algorithms. The BoT-IoT data set is used as an experimental data set.

Keywords: Internet of Things (IoT), Intelligent environments, Intrusion Detection System, Mirai botnet, Security

İkili Gri Kurt Optimizasyonu (BGWO) ve Naive Bayes (NB) Kullanılarak yeni bir hibrit IoT tabanlı IDS

Öz

Akıllı ortamların temel amaçlarından biri, verimlilik ve konfor açısından insan yaşam standardının kalitesini yükseltmektir. Nesnelerin İnterneti (IoT) modeli, akıllı ortamlar oluşturmak için yeni teknolojiye dönüşmüştür. IoT, diğer cihazlarla bilgi alışverişi yapabilen fiziksel eşyalar veya cihazları ifade etmektedir. Akıllı ev, akıllı şehir, endüstriyel kontrolu, otomobil endüstrisi, tarım, akıllı ulaşım, ev otomasyonu ve aletleri, sağlık gibi çeşitli alanlarda ve daha birçok alanda kullanılmaktadır. Dahası, yenilikçi iş paradigmalarını ve gelişmiş kullanıcı deneyimini garanti etmektedir. Gizlilik ve güvenlik, IoT paradigmasına dayalı herhangi bir gerçek dünya akıllı ortamında temel sorunlar olarak kabul edilmektedir. Bu nedenle, IoT sistemlerinin güvenliğini uygulamak, IoT ağlarının başarılı dağıtımında birinci öncelik ve büyük ilgi alanı haline gelmektedir. IoT ile ilgili sistemlerdeki açık güvenlik delikleri, akıllı uygulamaları etkileyen güvenlik riskleri oluşturur. Mirai botnet son zamanlarda başlatılan yeni saldırılardan bir örnektir. IoT ağı, kimlik doğrulama ve şifreleme ile korunmaktadır. ancak kötü niyetli ve zararlı saldırılara karşı hafifletemez. Bu nedenle saldırıları tespit etmek için IoT tabanlı Saldırı Tespit Sistemi (IDS) gerekmektedir. Bu makalede, IoT ağındaki saldırıları savunmak ve güvenlemek için ikili Gri Kurt Optimizasyonu (BGWO) ve Naive Bayes (NB) kullanılarak yeni bir hibrit IoT tabanlı IDS

[*] Corresponding Author: Konya Technical University, Faculty of Engineering, Department of Computer Engineering, Konya, Turkey, ORCID: 0000-0001-8171-3026, ismailmohamednur@gmail.com

sunulmuştur. BGWO, özellik seçimi olarak ve NB de sınıflandırma yöntemi olarak kullanılmıştır. Sonuçlar diğer optimizasyon algoritmalarıyla karşılaştırılmıştır. IoT-botnet veri kümesi, deneysel bir veri kümesi olarak kullanılmıştır.

Anahtar Kelimeler: Nesnelerin İnterneti (IoT), Akıllı ortamlar, Saldırı Tespit Sistemi, Mirai botnet, Güvenlik

1. Introduction

With the rapid of technology enhancement, the concept of Internet of Things (IoT) is becoming well known. It is an emerging model in the world of computer and traditional network extension that allows information exchanging between all kinds of various smart sensing objects through the internet (Atzori, L. et al., 2010). So, The IoT can be accessed by everyone, all the time and on any device from anywhere (Benabdessalem, R. et al., 2014). It is estimated that a trillion new IP devices will be connected to the internet by 2022. IoT will be used in a wide range of applications and will be covered almost all the areas of human daily life base including smart home, household appliances, smart plant, intelligent transportation and public facilities, medical facilities, battlefield monitoring and unmanned aerial vehicles, interconnected vehicles, wearable equipment, and environmental monitoring as well as many other applications that require internet (Olasupo, T. O., 2019; Roy, S. K. et al., 2019; Yang, Y. et al., 2019). Moreover, The IoT security has progressively taken the widespread concern. When a malicious intruder launches an attack to the IoT, it will face significant damages. It has drawbacks of limited resources (e.g. low memory, computing power, and etc). So, the confidentiality, integrity and availability of the IoT information sharing is in danger (Meneghello, F. et al., 2019). The IoT is one of the fastest developing internets based flied, before the end of 2020 fifty billion connected appliances expected (Evans, D., 2011). Yuan, X., Li, C., & Li, X. (2017) argued that 17 million Denial of Service (DoS) intrusions would occur by 2020. Greenberg, A. (2016). showed an open hole on the Jeep vehicle automotive system which allowed remote control via the internet. In 2016, security investigators have found out a vulnerability that enables smart thermostats connected to the internet to be subjected to remote ransomware attacks in which an intruder gains exclusive control of the thermostat until the charges requested is paid (Raywood, D., 2016). Mirai was one of novel ransomware attack launched in 2016. It’s an uncommon kind of botnet that triggers large scale of DDoS strikes by exploiting IoT devices (Kolias, C. et al., 2017). IoT network is protected with encryptions, authentications and topology construction of secure network. But these mechanisms are not enough to defend it once the intruder launches malicious attacks via data analysis (Öztürk and Özkaya, 2020). Therefore, other models of security mechanisms, such as Intrusion Detection System (IDS) should be considered to protect the IoT networks (Wang, C. X., et al., 2014).

Intrusion Detection System (IDS) is an effective and efficient method used to monitor and analyze malicious traffic in a certain network. It can behave as a second layer of defense which can defend the network against invaders when cryptography is broken (Anand, A., et al., 2012; Arrington, B. et al., 2016). Intrusion is a malicious or harmful activity that harms sensor nodes. IDS can explore and analyze machines and user behaves, detect signatures of well-known intrusions, and identify harmful network activity. The main goal of IDS is to observe for various intrusions in the networks and the nodes, and to alert users after attack detection performed. The IDS functions as an alarm or a network watcher. It prevents damage to the systems by generating an alert before intruders start to attack. Such programs could help human security analysts who are already dealing with large data sets and inundate of security alerts daily to better prioritize their security tasks (NUR, I. M., & ÜLKER, E., 2018).

In this article, we study hybrid of Naïve Bayes and Binary Grey Wolf Optimizer (BGWO-NB). BGWO used as feature selection and NB as classification method. BoT-IoT is one of the most up-to-date data set for intrusion detection. The rest of the article is written as follows: literature review of recently developed intrusion detection for IoT security using machine learning, Naïve Bayes, grey wolf optimizer, binary grey wolf and BGWO-NB presented in section 2, Experimental results and data set are discussed in section 3, and the conclusion presented in section 4.

2. Material and Method

2.1. Related Work

Thanigaivelan et al., proposed a distributed internal anomaly detection system for the IoT. The system’s main characteristics are ranking, observing, isolation and notifying. Nodes observe, analyze and note to their neighbours at a hop, and if a neighbor does not provide the required output and rating then neighboring node to be classified as an anomaly. Raza, S. et al., (2013), presented a real-time IDS in the Internet of Things named SVELTE. It is an IDS valid for IoT that is implemented in Contiki OS. This mechanism only mitigates content spoofing intrusions within the network, selective and gulp transfer intrusions. Summerville, D. et al., (2015) developed an ultra-lightweight deep packet anomaly mitigation technique that is possible to implement on small IoT appliances. The method utilizes n-gram bit patterns to form payloads and enables the n-gram size to vary by dimension. An attribute-based dimensionality-abated Artificial Neural Network (ANN) classifier to solve high dimensional cases in IDS has been investigated by (Manzoor, I. et al., 2017). Firstly, their approach suggests ranking of the received attribute correlation and information gain. Then, it merges them to calculate the information degree of the feature and selects to retain the attributes that have greater effect on data classification. Finally, their system employs an ANN classifier for the data classification. Their approach not only removes irrelevant and redundant data using pre-processing, but also enhances resource utilization and abates time complexity. However, for ID with a huge amount of data, the time complication of conventional neural network algorithms is too high to be fitting for IoT.

Aburomman, A. A., & Reaz, M. B. I., presented a weighted one against rest SVM (WOAR-SVM) classifier method and comparing various SVM-based classifier paradigms. Their approach uses a set of weights to compensate a single binary classifier, and every binary classifier has its own unique set of classification parameters. Lastly, two classifiers are implemented to classify and estimate a multiple class classifier. Their experimental results indicated that the new method has outstanding performance in overall accuracy of the multi class data. Zhang, M. et al., suggested a new technique based on probabilistic neural network (PNN) for intrusion detection. The technique only needs a feedforward process and does not need backpropagation. The training time is well shortened when compared with Naive Bayes and the back propagation (BP) neural network. An event processing-based IDS to resolve the problem of real time of IDS in IoT proposed by Jun, C., & Chi, C., (2014). They designed the IDS structure on the basis of Event Processing Model (EPM). The method is rule-based IDS in which rules are kept in rule pattern repository and takes SQL and EPL of Epser as a reference. The result obtained from this method showed more consumption of CPU resources, less memory consumption and took less processing time than conventional IDS.

Alsadhan, A., & Khan, N. presented an optimized IDS based on soft computing approach. The main goal of this security mechanism is to improve the performance of the system and identify each event in a robust way. They implemented soft computing approaches such as LDA, PCA, LBP, Greedy Search, PSO, MLP and SVM. Their results showed that the number of features reduced and the detection rates improved. Singh, D. et al., suggested a new IDS by combining three phases: feature selection, trust calculation, and classification decision. Their approach comprehensively analyses the security of the nodes. So, it increases the network's intrusion detection accuracy. However, its comprehensiveness makes the computing resources high. Cervantes, C. et al., presented a novel IDS to mitigate sinkhole attacks for IoT named as INTI. The new IDS is implemented in Cooja simulator. Their technique defines four modules. The first module is Cluster con- figure ration module which is responsible for classifying a node like members, leaders and associated according to their network functions. The second one is intruder detection module which mitigates the sinkhole attacking node. The third is observing of routing module in which observer node monitors the number of transmissions is occurred. The fourth one is the isolation of intruder module which isolates the harmful node from the cluster and it also raised an alarm to notify its neighbouring nodes. The simulation result showed that detection rate of 92%. The technique mitigates sink hole intrusions, so this work can be improved by detection other types of intrusions.

Yulong Fu et al., developed an automata-based IDS. It is a uniform of IDS for the greatly diverse structure IoT networks based on an automata paradigm. Their mechanism can mitigate, analyze and report the possible intrusions in IoT. They divided the detection steps into three: jam-attack, false-attack, and reply-attack automatically. Sedjelmaci, H. et al., presented a lightweight anomaly prevention method using game theory for IoT intrusion detection. Their method was hybrid of signature and anomaly intrusion detection. It achieves by creating the game model of attacker and normal user. The simulation results showed that anomaly detection method requires a low energy usage to mitigate the intrusions with high detection and low false positive rates. Hodo, E. et al., developed a novel Artificial Neural Network (ANN) based IDS. A multi-level perceptron which is a type of supervised ANN, is trained employing internet packet traces and was assessed on its ability to mitigate DoS/DDoS intrusions on IoT tools. The detection method was based on classifying patterns into normal and threat. It was able to identify successfully various types of intrusions. The experimental results indicated accuracy of 99.4% and it can successfully prevent various DDoS/DoS attacks. Susilo, B., & Sari, R. F., (2020) discussed several machine learning and deep learning techniques, as well as datasets for enhancing the IoT security performance. They developed a method for mitigating denial-of-service (DoS/DDoS) intrusions using a deep learning mechanism. They found that a deep learning technique could improve the accuracy so that the mitigation of attacks that occur on an IoT network is as effective as possible.

2.2. Naive Bayes

Naive Bayes classifier algorithm is a derived from Bayesian probability theorem, that mainly works on independence attributes, each feature has its own probability without effecting others features. Moreover, the result of naïve classifier is mostly achieving an optimum result compare to some supervised algorithms. Naïve Bayesian is a model which is used to calculate the probabilities of two events which are *I* and *M* events. The method involves maximum probability principle, another word is the classifier assumptions the feature of the class which be affiliated to superior and larges probability, the formula is defined as this. Suppose I and M are random events

$$P(I \mid M) = \frac{P(M \mid I)\, P(I)}{P(M)} \qquad (1)$$

Where $P(I)$ is an independent probability of I, $P(M)$ is an independent probability of M, $P(\mathrm{M} \mid \mathrm{I})$ is the likelihood probability of event *M* when event *I* given, $P(I)$ and $P(M)$ equivalent to prior probability, $P(I \mid M)$ equivalent to posterior probability.

2.3. Grey Wolf Optimizer

In 2014, Grey wolf optimizer algorithm (GWO) was developed by Mirjalili et al. It is bio-inspired of the hunting behaviors and social leadership of grey wolves in nature. The GWO swarm split into four groups: alpha(α), beta(β), delta(δ), and omega(ω). The fittest wolves are alpha, beta and delta and they lead other wolves to the search space. The mathematical equations of encircling, search and attacking prey modelled as follow:

1. Encircling the prey

Equations (2) and (3) are defined to shape the encircling formula of the swarms around the prey.

$$D = |C \cdot X_P(t) - X(t)| \qquad (2)$$

$$X(t+1) = X_P(t) - A \cdot D \qquad (3)$$

Where X is the wolf location, and t is the number of loops. X_P is prey location and D is computed from equation (2). A and C are coefficients computed based on equations (4) and (5) respectively.

$$A = 2a \cdot r_1 - a \qquad (4)$$

$$C = 2r_2 \qquad (5)$$

r1 and r2 are random vectors between 0 and 1 employed to reveal optimal solution (for finding hunting prey).

2. Hunting stage

The hunting performed by whole swarm by using information coming from the α, β and δ which are required to know the prey position, as stated in the below equation.

$$X(t+1) = \frac{X_1 + X_2 + X_3}{3} \qquad (6)$$

The values of X_1, X_2, and X_3 is evaluated as in equations (7), (8) and (9) respectively.

$$X_1 = X_\alpha - A_1 \cdot (D_\alpha) \qquad (7)$$

$$X_2 = X_\beta - A_2 \cdot \left(D_\beta\right) \qquad (8)$$

$$X_3 = X_\delta - A_3 \cdot (D_\delta) \qquad (9)$$

The best three solutions in the population are X_1, X_2, and X_3 at iteration t. The equation of A and C are mentioned above. D_1, D_2, and D_3 are calculated in equations (10), (11), and (12) accordingly. All other wolves adapt their locations using the locations of α, β and δ.

$$D_\alpha = |C_1 \cdot X_\alpha - X| \qquad (10)$$

$$D_\beta = \left|C_2 \cdot X_\beta - X\right| \qquad (11)$$

$$D_\delta = |C_3 \cdot X_\delta - X| \qquad (12)$$

3. Attacking prey stage

The linearly decreased parameter a is from 2 to 0 through the number of loops. The formula of a is as below.

$$a = 2 - t(2/NLoops) \qquad (13)$$

Where t is the loop number, and $NLoops$ is total number of the loops. Parameter a is utilized to control the trade-off between exploitation and exploration of the packs. Half of the wolves are assigned to exploration while the other used for half exploitation. So, GWO can transit smoothly between exploitation and exploration. A in the equation (4) is random value in the range of [-a, a]. When a decrease the A also decrease. When A is in [-1, 1], the next location of search swarm can be any location between current location and prey location (i.e. exploitation occurs when A < 1 and C < 1).

4. Search stage

Optimum search in GWO depends on the positions of the α, β and δ. The wolves diverge from each other when they search for prey and converge again to attack once they discover a better prey. Furthermore, when random value of A is less than -1 or greater than 1 (A < -1 or A > 1), search swarm diverges to prey as shown in Fig. 1. In other words, exploration occurs when (A < -1 or A > 1). Another important parameter of GWO is C in equation (5) which is between 0 and 2 assists the wolves during the exploration process at (C > 1). C impacts the distance in equation (2). So, this expresses that GWO to output more random behavior throughout the favoring exploration and local optima evasion. The GWO algorithm implementation as in below (Mirjalili, S. et al.):

- Initialize a swarm of wolves randomly based on the upper bound and lower bound
- Compute the corresponding objective value for each wolf
- Select the first best 3 wolves and store as α, β, and δ
- Update the location of the left of the swarm (ω) using equations (6) to (12)
- Update parameters a, A, and C

- If the criterion is not achieved then return to step 2
- Return the location of α as the best estimated optimum

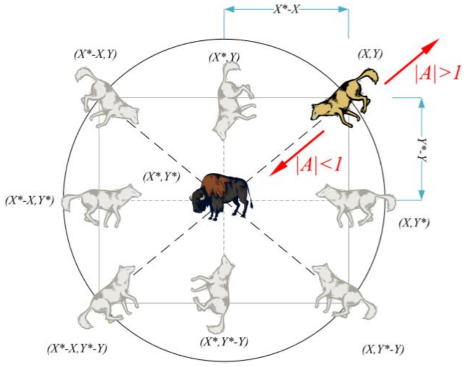

Fig. 1. Position updating technique of search packs and impacts of A on it

The binary version equations of grey wolf as follow (Emary, E. et al., 2016):

$$x_1^d = \begin{cases} 1 & if\ (x_\alpha^d + bstep_\alpha^d) \geq 1 \\ 0 & otherwise \end{cases} \qquad (14)$$

where x_α^d is the position of alpha, *d* is the dimension of search space, and $bstep_\alpha^d$ represents the binary step that can be expressed as

$$bstep_\alpha^d = \begin{cases} 1 & if\ cstep_\alpha^d \geq rand \\ 0 & otherwise \end{cases} \qquad (15)$$

where *rand* is a random vector in [0, 1], and $cstep_\alpha^d$ denotes the continuous valued step size that can be calculated as in equation (16).

$$cstep_\alpha^d = \frac{1}{1 + e^{-10(A_1^d D_\alpha^d - 0.5)}} \qquad (16)$$

where A_1^d and D_α^d are determined by applying Eq.15 and Eq.22

$$x_2^d = \begin{cases} 1 & if\ (x_\beta^d + bstep_\beta^d) \geq 1 \\ 0 & otherwise \end{cases} \qquad (17)$$

where x_β^d is the position of alpha, d is the dimension of search space, and $bstep_\beta^d$ represents the binary step that can be expressed as

$$bstep_\beta^d = \begin{cases} 1 & if\ cstep_\beta^d \geq rand \\ 0 & otherwise \end{cases} \qquad (18)$$

where *rand* is a random vector in [0, 1], and $cstep_\beta^d$ denotes the continuous valued step size that can be calculated as in equation (19).

$$cstep_\beta^d = \frac{1}{1 + e^{-10(A_1^d D_\beta^d - 0.5)}} \qquad (19)$$

where A_1^d and D_β^d are determined by applying Equations (15) and (22)

$$x_3^d = \begin{cases} 1 & if\ (x_\delta^d + bstep_\delta^d) \geq 1 \\ 0 & otherwise \end{cases} \qquad (20)$$

where x_δ^d is the position of alpha, d is the dimension of search space, and $bstep_\delta^d$ represents the binary step that can be expressed as

$$bstep_\delta^d = \begin{cases} 1 & if\ cstep_\delta^d \geq rand \\ 0 & otherwise \end{cases} \qquad (21)$$

where *rand* is a random vector in [0, 1], and $cstep_\delta^d$ denotes the continuous valued step size that can be calculated as in equation (22).

$$cstep_{\delta}^{d} = \frac{1}{1 + e^{-10(A_1^d D_\delta^d - 0.5)}} \qquad (22)$$

where A_1^d and D_δ^d are determined by applying equations (15) and (22)

In this paper we will use the second model of binary grey wolf optimizer. BGWO2 updates the locations of the swarm by converting the location into a binary vector, as shown in equation (23).

$$X_{\mathrm{d}}^{t+1} = \begin{cases} 1 & if\ S\left(\frac{X_1+X_2+X_3}{3}\right) \geq rand \\ 0 & otherwise \end{cases} \quad (23)$$

where *rand* is a random number in [0, 1], X_{d}^{t+1} is updated binary location in the dimension of search space d at iteration t, and S is the sigmoid function, and it can be computed as

$$S(x) = \frac{1}{1 + e^{-10(x - 0.5)}} \qquad (24)$$

$$Fitness = alpha * P + beta\ \frac{N - L}{N} \qquad (25)$$

where P is the classification accuracy, L is the length of selected attribute subset, N is the total number of attributes in the data. *alpha* is the weight of classification accuracy and *beta* is the quality of attribute selection. *alpha* ∈ [0, 1] and *beta* =1 − *alpha*.

2.4. Binary Grey Wolf for Feature Selection

Feature selection is a process and an efficient way of selecting a subset of relevant attributes for use in model construction. It's a useful method that literally improves the quality and performance of the dataset for better classifying the data using classification algorithms. It mutes out the attributes which are not relevant in addition to the existing attributes. Feature selection has three methods; filter, wrapper and embedded methods. In this article, we will use wrapper algorithm as attribute selection.

Wrapper methods consider the choice of a set of attributes as a search problem, where different combinations of attributes are prepared, assessed and compared to others. A classification algorithm used to evaluate a combination of attributes and assign a score using the algorithm accuracy. The main specification of wrapper method is the employment of the classifier as guide of feature selection function. Wrapper-based feature selection can be classified using the following three mains; classification method, evaluation criteria and search method. BGWO will be employed as search method which can search the attribute space maximizing the attribute evaluation criteria in equation 25 and NB will be employed as classifier method. Fig.2 illustrates that the solutions represented in binary format 0 or 1. The unselected feature denotes 0, while the selected feature represents 0. For instance, given a solution *D* = {0,0,1,0,1,1,1,0, 0} this shows that the third, fifth, sixth and seventh attributes are selected.

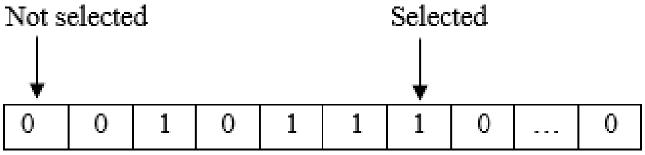

Fig. 2. Feature selection flag vector

Fig. 3 explains the flowchart of BGWO-NB for attribute selection. The initial populations are randomized and evolved in the process of fitness evaluation iteratively. In this paper, the classification accuracy obtained by the Naïve bayes classifier is employed as the fitness function. In the evaluation, if the solutions have the same fitness values, then the solution with the smaller number of attributes will be selected. At the end of the loop, the alpha wolf is selected as the global best solution (optimal feature subset).

3. Results and Discussion

In 2018, Koroniotis, N., et. al. designed a new dataset for detecting IoT networks. The data is called BoT-IoT dataset. It contains 46 features including the class. The class has one normal and four intrusions (DoS, DDoS, OS and Service Scan, keylogging and data exfiltration). The data contains 1048576 instants for training and 733706 instants for testing. In the experiment, the algorithms are executed on a computer with a 2.50 GHZ, 8 GB of RAM, Intel(R) Core i5 processor and Matlab2018 program. BoT-IoT dataset were used as intrusion detection dataset. We compared the result of BGWO-NB with Naïve Bayes (NB), Binary Particle Swarm Optimization with NB (BSO-NB), Binary Fruit fly Optimization Algorithm with NB(BFFOA) and Binary Gravitational Search Algorithm with NB (GSA-NB). The population size of optimization algorithms and maximum iteration were 100 and 150 respectively. Equation (25) is fitness function of the hybrid method. The algorithms executed 10 times each and overall results shown in Table 1.

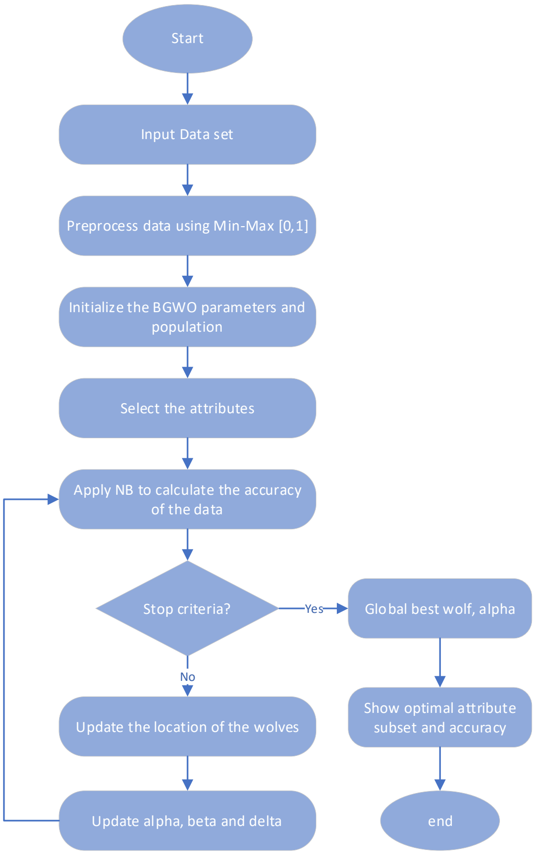
Start
Input Data set
Preprocess data using Min-Max [0,1]
Initialize the BGWO parameters and population
Select the attributes
Apply NB to calculate the accuracy of the data
Stop criteria?
Yes
Global best wolf, alpha
No
Update the location of the wolves
Show optimal attribute subset and accuracy
Update alpha, beta and delta
end

Fig. 3. BGWO-NB flowchart

Table 1. BoT-IoT Experimental Results

Methods	Accuracy (%)
NB	*90.60 %*
BPSO-NB	***98.87 %***
BFFOA-NB	*96.40 %*
BGSA-NB	*91.00 %*
BGWO-NB	***99.15 %***

We observed that the original NB algorithm is very fast compared with other hybrid methods. BGWO-NB algorithm achieved the highest accuracy 99.15 % followed by BPSO-NB, BFFOA-NB, GSA-NB and NB with accuracy of 98.87 %, 96.40 %, 91.00 % and 90.60 respectively. Furthermore, BGWO-NB approach is capable to use for intrusion detection in IoT devices.

4. Conclusions and Recommendations

With the rapid growth and widespread use of the internet, there has been a significant increment in threats to the security of information systems and an expansion in types of intrusions. So, the need to develop new methods and mechanisms arose due to the intrusions and threats. The Internet of Things faces many threats and attacks every day. In this paper, Naïve bayes and binary grey wolf optimizer have been used to improve the IoT security. The experimental results have shown that the hybrid of BGWO-NB is capable to mitigate and detect attacks over the IoT devices. It is observed that the BoT-IoT dataset is fruitful to use for the detection of denial of serves attacks.

References

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Olasupo, T. O. (2019). Wireless communication modeling for the deployment of tiny IoT devices in rocky and mountainous environments. *IEEE Sensors Letters*, *3*(7), 1-4.

Roy, S. K., Misra, S., & Raghuwanshi, N. S. (2019). SensPnP: Seamless integration of heterogeneous sensors with IoT devices. *IEEE Transactions on Consumer Electronics*, *65*(2), 205-214.

Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Information Sciences*, *479*, 567-592.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, *6*(5), 8182-8201.

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, *1*(2011), 1-11.

Greenberg, A. (2016). The Jeep hackers are back to prove car hacking can get much worse. *Wired Magazine*, *8*.

Raywood, D. (2016). Defcon: Thermostat control hacked to host ransomware.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80-84.

Wang, C. X., Haider, F., Gao, X., You, X. H., Yang, Y., Yuan, D., ... & Hepsaydir, E. (2014). Cellular architecture and key technologies for 5G wireless communication networks. *IEEE communications magazine*, *52*(2), 122-130.

Anand, A., & Patel, B. (2012). An overview on intrusion detection system and types of attacks it can detect considering different protocols. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(8), 94-98.

NUR, I. M., & ÜLKER, E. A hybrid cloud-based Intrusion Detection and Response System (IDRS) based on Grey Wolf Optimizer (GWO) and Neural Network (NN).

Thanigaivelan, N. K., Nigussie, E., Kanth, R. K., Virtanen, S., & Isoaho, J. (2016, January). Distributed internal anomaly detection system for Internet-of-Things. In *2016 13th IEEE annual consumer communications & networking conference (CCNC)* (pp. 319-320). IEEE.

Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad hoc networks*, *11*(8), 2661-2674.

Manzoor, I., & Kumar, N. (2017). A feature reduced intrusion detection system using ANN classifier. *Expert Systems with Applications*, *88*, 249-257.

Aburomman, A. A., & Reaz, M. B. I. (2017). A novel weighted support vector machines multiclass classifier based on differential evolution for intrusion detection systems. *Information Sciences*, *414*, 225-246.

Alsadhan, A., & Khan, N. (2013). A proposed optimized and efficient intrusion detection system for wireless sensor network. *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, *7*(12), 1621-1624.

Singh, D., & Bedi, S. S. (2016). Multiclass ELM based smart trustworthy IDS for MANETs. *Arabian Journal for Science and Engineering*, *41*(8), 3127-3137.

Öztürk, Ş., & Özkaya, U. (2020). Skin Lesion Segmentation with Improved Convolutional Neural Network. *Journal of digital imaging*.

Fu, Y., Yan, Z., Cao, J., Koné, O., & Cao, X. (2017). An automata based intrusion detection method for internet of things. *Mobile Information Systems*, *2017*.

Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016, May). Threat analysis of IoT networks using artificial neural network intrusion detection system. In *2016 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-6). IEEE.

Susilo, B., & Sari, R. F. (2020). Intrusion Detection in IoT Networks Using Deep Learning Algorithm. *Information*, *11*(5), 279.

Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014). Grey wolf optimizer. *Advances in engineering software*, *69*, 46-61.

Mirjalili, S. (2015). How effective is the Grey Wolf optimizer in training multi-layer perceptrons. *Applied Intelligence*, *43*(1), 150-161.

Emary, E., Zawbaa, H. M., & Hassanien, A. E. (2016). Binary grey wolf optimization approaches for feature selection. *Neurocomputing*, *172*, 371-381.

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*, *100*, 779-796.

Jun, C., & Chi, C. (2014, January). Design of complex event-processing IDS in internet of things. In *2014 sixth international conference on measuring technology and mechatronics automation* (pp. 226-229). IEEE.

Benabdessalem, R., Hamdi, M., & Kim, T. H. (2014, December). A survey on security models, techniques, and tools for the internet of things. In *2014 7th International Conference on Advanced Software Engineering and Its Applications* (pp. 44-48). IEEE.

Cervantes, C., Poplade, D., Nogueira, M., & Santos, A. (2015, May). Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (pp. 606-611). IEEE.

Zhang, M., Guo, J., Xu, B., & Gong, J. (2015, August). Detecting network intrusion using probabilistic neural network. In *2015 11th International Conference on Natural Computation (ICNC)* (pp. 1151-1158). IEEE.

Summerville, D. H., Zach, K. M., & Chen, Y. (2015, December). Ultra-lightweight deep packet anomaly detection for Internet of Things devices. In *2015 IEEE 34th international performance computing and communications conference (IPCCC)* (pp. 1-8). IEEE.

Sedjelmaci, H., Senouci, S. M., & Al-Bahri, M. (2016, May). A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. In *2016 IEEE international conference on communications (ICC)* (pp. 1-6). IEEE.

Arrington, B., Barnett, L., Rufus, R., & Esterline, A. (2016, August). Behavioral modeling intrusion detection system (BMIDS) using internet of things (IoT) behavior-based anomaly detection via immunity-inspired algorithms. In *2016 25th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-6). IEEE.

Yuan, X., Li, C., & Li, X. (2017, May). DeepDefense: identifying DDoS attack via deep learning. In *2017 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 1-8). IEEE.