Memetic algorithm for short messaging service spam filter using text normalization and semantic approach

Arnold Adimabua Ojugo[1], Andrew Okonji Eboka[2]
[1]Department of Mathematics/Computer Science, Federal University of Petroleum Resources Effurun, Nigeria
[2]Department of Computer Science Education, Federal College of Education (Technical) Asaba, Nigeria

Article Info

Article history:

Received Jul 12, 2019
Revised Nov 13, 2019
Accepted Jan 12, 2020

Keywords:

Bayes theorem
Memetic algorithm
Semantic processing
Spam filters
Text normalization
Text processing

ABSTRACT

Today's popularity of the short messages services (SMS) has created a propitious environment for spamming to thrive. Spams are unsolicited advertising, adult-themed or inappropriate content, premium fraud, smishing and malware. They are a constant reminder of the need for an effective spam filter. However, SMS limitations of 160-charcaters and 140-bytes size as well as its being rippled with slangs, emoticons and abbreviations further inhibits effective training of models to aid accurate classification. The study proposes Genetic Algorithm Trained Bayesian Network solution that seeks to normalize noisy feats, expand text via use of lexicographic and semantic dictionaries that uses word sense disambiguation technique to train the underlying learning heuristics. And in turn, effectively help to classify SMS in spam and legitimate classes. Hybrid model comprises of text preprocessing, feature selection as well as training and classification section. Study uses a hybrid Genetic Algorithm trained Bayesian model for which the GA is used for feature selection; while, the Bayesian algorithm is used as classifier.

Corresponding Author:

Arnold Adimabua Ojugo,
Department of Mathematics/Computer Science,
Federal University of Petroleum Resources Effurun,
P.M.B 1221, Effurun, Warri, Delta State, Nigeria.
Email: arnoldojugo@gmail.com

1. INTRODUCTION

The advent of short messaging services by Neil Papworth since 1992, has seen great penetration and a tremendous growth rate of the service. Advent of mobile phones with enhance features has contributed to the large scale adoption of SMS by users. The portability, mobility, ubiquity of services and its low cost continues to promote text messages to become the most used means of electronic communication in the world today [1-2]. Short Message Service (SMS) is text service component of phones or mobile communication systems with standardized protocols that allow the exchange of short text messages between fixed line or mobile phone devices. An estimated 23-billion SMS is sent daily worldwide in 2014; While, a total of 8.3 trillion SMS was sent worldwide in the same year with net market revenue of over $128Billion in 2011. In 2016, the revenue was forecasted to be over $153Billion; And, evidence has shown that 3.39billion SMS was sent and received in Nigeria alone in the year 2013 [1]. The increased popularity and consequent proliferation of SMS platforms, has also seen a corresponding rise in unsolicited SMS called spams. The ITU 2005 campaign witnessed a rise in the unsolicited commercial adverts as sent to mobile phones via SMS. Recent drift from email to SMS spams is attributed to the availability of effective email filters, user awareness and industry collaboration [3-6].

Spams are unsolicited electronic messages that include, and not limited to, emails, SMS, Voice over IP (VoIP) and instant messaging from chats. Spams are unsolicited or unwanted messages from a sender, sent indiscriminately with no prior relationship to a user mostly for commercial reasons [7-8]. SMS Spams ranges from adult-themed and inappropriate contents, unsolicited adverts, smishing and mobile malware etc. SMS spams have since become enormous challenge – causing great loss of revenue to Internet Service Providers, Mobile Network Operators and users in general. On overall, spams grew by 300% from just 2011 to 2012 from millions of SMS received worldwide; And 33.3% attributed to spam-related messages [2, 8]. In Nigeria alone, an estimated 334,857,685 SMS spams were received daily in 2015. Implying that lots of mobile phone users are handicapped in the control of the number of spams they receive [9, 10]. Besides being distractive and annoying, users need a certain degree of privacy with their phones and free from Spam and viruses invasions [11-14]. Mobile network operators are geared towards reducing the number of spams over their network as such flooding makes the SMS channel more invasive and less secure [15-17].

The tremendous rise in the usage of SMS is attributed to [16, 1-2]: a) Trust in SMS channel: SMS is a private communication between two parties only has created some level of trust and acceptance all over the world such that financial institution has adopted its use in payment authorization. b) High open rate: Average time it takes to respond to SMS is faster than email and voice call – making it a preferred choice. Statistics have shown SMS has an average open rate of 99% and opens within 15-minutes; While, an email has an open rate of 20-25% and open with 24-hours. c) Low cost of transaction: Average cost per SMS is almost negligible, and free for some networks – affording mobile phone users the opportunity to send as many without recourse to cost. Marketers and many other institution has embrace bulk SMS a medium for advertising and interact with customers. d) Ease and Convenience of texting enables its use in nearly every environment without disrupting people around phone users; Unlike in voice call, SMS can be in absolute silence without inconveniencing people around. Aided by the portable size of most mobile devices, communication can be done almost everywhere and any position.

SMS has great benefit for both subscribers and operators in diverse ways centered on convenience, flexibility, seamless integration of messaging services and data access. Others may include [1-2]: (a) delivery of notifications, (b) guaranteed delivery, (c) reliable, low-cost for concise data, (d) ability to screen messages and return calls, (e) increases productivity, (f) more sophisticated functionality provides enhanced user benefits, (g) delivery to multiple users at same time, (h) ability to receive diverse information, (i) e-mail generation, (l) creation of user groups, (m) integration with other data and Internet-based application, and (n) increase in revenue for mobile network operators (MNO).

2. SMS, SPAMS AND FILTERS

The tremendous rise in the usage of SMS is attributed to its ease of use, ubiquity in nature, high open rates, low cost of transaction and inherent trust in the channel. The ease of use, portability, ubiquity, low open rate and low cost of SMS are major factors for its popularity and usage. This growth rate has equally attracted spamming to the channel. Spammers are well organized businesses seeking to make money through the use of email, mobile (SMS), Instant message, UseNet newsgroup, Social network and internet telephony channel without the consent of subscriber (user). Their merchandise are unsolicited advertising, inappropriate or adult-themed content, premium fraud, smishing and even distribution of malware generally called spam. SMS spams are thus, unsolicited and unwanted messages sent to mobile phone users. Spam trend is on the rise and its toll on subscribers and even MNO is getting intensive and proven to be of great concern to all [18- 20].

2.1. Spams: sources and consequents

SMS spam is generates from various sources; one of the typical spam sources is number harvesting, which is carried out by Internet sites offering “free” services. End users can also receive mobile spam from the following sources [12]:

- Organizations and individuals that pay MNO to deliver SMS to the subscribers: They are responsible for the highest number of spam received on subscriber’s mobile phones. Although, MNOs have adopted and enforced use of opt-out, or even opt-in processes for the user to stop receiving promos or ads.
- Organizations that do not pay for the SMS that are delivered to the subscribers: they are usually worse and considered as fraud because it damages MNO brands.
- Individual originated messages that disturb recipients.

Apart from the distracting and annoying effects of spam, there are other serious consequences generated. There is the issue of competition for resources between millions of illegitimate and legitimate messages being transmitted. These messages consume network resources that could have otherwise been allocated to other legitimate services by MNO [15]. Spamming activities attracts extra cost for mobile operators to adequately maintain and service their mobile communication infrastructures for effective service delivery. Also flooding of MNO infrastructure with illegitimate massages can cause legitimate users to suffer denial of service. Huge amount of spam messages also concerns the cellular carriers as the messages traverse through the network, causing congestion and hence degrade network performance [16]. Mobile communication industries are also faced with threat from virus, Trojan horse, worms and malware propagated by spam SMS [15]. Fraudulent messaging activities such as phishing identity theft and other fraud related activities which were prominent in email messaging services has migrated to SMS platform [17, 18]. Financial loss, damage to mobile user’s reputation and that of the MNO are issues to be considered [19].

2.2. Spam filters

SMS spam filters shares similar features and challenges with email spam filters. They are both saddled with the task of real-time filtering efficiency and the option to decide between client-side and or server-side filtering. The mobile space is also faced with the challenge of overcoming misclassification cost and eliminate false-positives (genuine SMS incorrectly classified as spam by filter), and issue of concept drift in order to evade filters. Thus, most existing approaches of combating SMS spam are imported from successful email-solutions [21, 22]. Not all solutions to email spam are applicable to SMS due to the fact that established email spam filters are unable to tackle SMS Spam because performance of email spam filters is seriously degraded when used to filter SMS spam. This is attributed to its limited 160-character of 140-bytes sized messages. Also, these messages are rife with slangs, symbols, emoticons and abbreviations that inhibit proper classification [23-24]. To overcome the shortfall of email filters in handling SMS spam successfully, a combined filtering technique to reduce noise in SMS and expands the message size [25, 26] – is the focus of this research. Spam filters can be divided into a number of broad categories based on the method used to filter Spam. They include [27]: list based, challenge/response system, content based, collaborative and Heuristics Based filters.

2.3. Challenge-response filters

This filter forces a message sender to prove they are human via some test. This filter blocks undesirable messages by forcing the sender to perform a task before their message is delivered. With task success, the message (and future messages) will be delivered to the recipient; While, failure to complete the challenge after a certain time period, leads to message rejection [24]. The most common challenge consists of distorted images and text. To triumph this challenge, a user must type text or arrange images correctly. With challenge/response false positives can be reduced to barest minimum. Another merit of this approach is in its low system resource requirements, since no CPU-intensive pattern matching is required. However, this approach causes more problems than it solves. For inexperienced or visual handicapped users, the challenges are completely unsolvable. Regular users are provoked by the challenges and choose not to do so since they view it as an unacceptable irritation. Also, automated email that a user would want to receive (travel confirmations, online purchase receipts, etc) are trapped by this approach and never delivered [28-30].

2.4. List-based filters

- Blacklist: This earliest spam-filtering method seeks to block unwanted messages from an already created list of senders. Blacklists are records of email addresses, Internet Protocol (IP) addresses and phone numbers that have been previously used to send spam. When incoming message arrives, spam filter checks if IP, email address or phone number is on a blacklist. If so, the message is considered spam and rejected. Blacklists ensure known spammers cannot reach users' inboxes. Their only demerit is that they can also misidentify legitimate senders as spammers [24, 29]].
- Whitelist: To block spams, whitelist rather than specify senders to block messages from, it specifies which senders to allow messages from. These addresses are stored in trusted-users list. Most spam filters uses a whitelist alongside other techniques to cut down on the number of genuine SMS that accidentally get flagged as spam. A filter that uses just whitelist implies that anyone not approved is automatically blocked. Some anti-spams use a whitelist variation called automatic whitelist. Here, an unknown sender address is checked against a database; if they have no history of spamming – their message is delivered to the recipient's inbox and added to the whitelist [24, 29].
- Greylist: This filter works with the assumption that most spammers sends batch of messages once. When message from unknown address is received, it blocks and revert a failure delivery to the sending server. If the message is resent, which most legitimate servers do, filter receives it and adds the address/phone number to the list. Although overhead of the filter is low, its demerit is the unjust delay delivery experienced by genuine messages to its recipient [24, 29].

2.5. Content-based filters

Content-based filtering methods are based on the evaluation of individual words or phrases found in the mail/message to determine if message is spam or not. This method analyzes message header, subject and body to discover any distinctive characteristic [30]. They are further classified into word-based and heuristic filters. Word-based filters use a set of rules to detect genuine from spam SMS. Also known as rule-filters, they use rules about actual word(s) or phrase(s) in a message to classify messages into genuine and spam classes. Rule features include word type, frequency of occurrence, structure of text (e.g. font size, colour etc), presence of many periods between letters (e.g. F.R.E.E), existence of image, etc. Rules are filter-dependent and can vary from simple to very complex. A demerit of rule-based filters is that: (a) they are knowledge intensive, (b) time consuming process in reviewing spam messages to determine the rules, and (c) needs regular update of rules as spammers changes their tactics [31-34].

Conversely, heuristic-based filter examines message content through various algorithms and resources, and assigns points to words or phrases. Words commonly found in spams such as “FREE” or "SEX," receive higher scores. Terms commonly found in normal messages receive lower scores. The filter then adds up total scores. If the message receives a certain score or higher (determined by anti-spam application's administrator), the filter identifies it as spam and blocks it. Messages with score(s) lower than the target number are delivered to the use [35]. Bayesian filter, KNN classifier, AdaBoost classifier, Gary Robinson technique, Support Vector Machine, Neural Network are examples [36]. Using a heuristic filter allows many spam filtering methods to be used, resulting in better performance than any single method by itself.

3. SOFT-COMPUTING FRAMEWORK

3.1. Bayesian networks

Are based on the Bayesian theorem of conditional probability. They have been successfully applied to many domains such as medicine, machine learning, speech recognition, signal processing, natural language processing and cellular networks. They are an attractive machine learning technique that represents domain knowledge and data in an elegant mathematical structure with simplified visual representation. Bayesian net shows graphic probability relationships between a set of variables under the domain of uncertainty. They are usually structured as a directed acyclic graph and conditional probability tables (CPTs). CPT tables represent probability of a random variable where, given the occurrence of its parent nodes. We can apply same conceptual strategy to spam filters [37].

Bayesian net classifiers are built based on the training data. Its building process includes structure learning, parameter learning, and building probability distribution tables for each node in the network. There are two major learning processes namely: (a) structured learning or casual discovery in which network learns the structure and parameters with the provided input data. The causal discovery aims to learn the structure and learn the parameters. It achieves this using either of K2, Hill climbing and Tabu-Search; and (b) probability distribution learning is achieved with algorithms like Bayes Net estimator, BMA estimator and multinomial estimator. Once structure learning is complete, parameter learning completes the CPT tables for each feature in the Bayesian Network. The network design in fig 1 is for detecting texts in SMS and helping the model and algorithm to classify these SMS into either of genuine/legitimate and spam SMS. Bayesian network design needs to consider the attributes, search algorithm and estimation algorithms. Thus, we use the hill-climber search algorithm with five parents used as the search algorithm for this network with simple estimator as an estimate on algorithm with threshold value “0.5” [38].

3.2. Genetic algorithm (GA)

Inspired by Darwinian evolution of survival of fittest, it consists of a chosen population with potential solutions to a specific task. Each potential solution is an individual for which optimal is found using four operators namely: initialize, select, crossover and mutation [39]. Individuals with genes close to optimal, is said to be fit. Fitness function determines how close an individual is to optimal solution. [40-42]. The basic operators for GA include:

- Initialize – Individual data are encoded into forms suitable for selection. Each encodings type used has its merit. Binary encodings are computationally more expensive. Decimal encoding has greater diversity in chromosome and greater variance of pools generated; float-point encoding or its combination is more efficient than binary. Thus, it encodes as fixed length vectors for one or more pools of different types. The fitness function evaluates how close a solution is to its optimal – after which they are chosen for reproduction. If solution is found, function is good and selected for crossover. The fitness function is the only part with knowledge of task. If more solutions are found, the higher its fitness value.

- Selection – best fit individuals close to optimal are chosen to mate. The larger the number of selected, the better the chances of yielding fitter individuals. This continues until one is chosen, from the last two/three remaining solutions, to become selected parents to new offspring. Selection ensures the fittest individuals are chosen for mating but also allows for less fit individuals from the pool and the fittest to be selected. A selection that only mates the fittest is elitist and often leads to converging at local optima.
- Crossover ensures best fit individual genes are exchanged to yield a new, fitter pool. There are two crossover types (depends on encoding type used): (a) simple crossover for binary encoded pool. It allows single- or multi-point cross with all genes from a parent, and (b) arithmetic crossover allows new pool to be created by adding an individual's percentage to another.
- Mutation alters chromosomes by changing its genes or its sequence, to ensure new pool converges to global minima (instead of local optima). Algorithm stops if optimal is found, or after number of runs if new pools are created (though computationally expensive), or when no better solution is found. Genes may change based on probability of mutation rate. Mutation improves the much-needed diversity in reproduction.

Cultural GA is a variants of GA with a belief space define as thus: (a) Normative (has specific value ranges to which an individual is bound), (b) Domain (has data about task domain), (c) Temporal (has data about events' space is available), and (d) Spatial (has topographical data). In addition, an influence function mediates between belief space and the pool – to ensure and alter individuals in the pool to conform to belief space. CGA is chosen to yield a pool that does not violate its belief space and helps reduce number of possible individuals GA generates till an optimum is found [43, 44].

3.3. Motivation / statement of problem

a. Spams have continued to soar with the advent of SMS. The alarming growth rate of spams with SMS popularity have now created a propitious environ for spammers to exploit subscribers; Thus, causing both financial loss and emotional instability as consequences to users, corporate organs and mobile network operator(s).

b. Academic researches and companies are today, faced with the challenge of dealing with SMS spam. A major issue has been that existing approaches to resolving SMS spam are imported from successful email anti-spam solutions (Wang et al., 2010). Thus, are quite unable to effectively and efficiently tackle SMS spam successfully – as their performance is seriously hampered and degraded by the parametric feats used to filter spams.

c. The formulation and design of an effective SMS filter has continued to suffered setback(s) due to the inherent reason that SMS filters by design are not as simple as email filters due to its limited size of 160-characters of 140bytes sized data. These amongst other constraints, continue to create rippled impediment in size of feature to be selected for training and consequently contributing to poor learning and classification of learning algorithm.

d. Furthermore, SMS are rippled with slangs, abbreviations, symbols and emoticons that inhibit proper classification of words or texts [45].

To overcome these amongst many other shortfalls inherent in the adoption of email filters as adapted to handling SMS spam successfully, a hybrid filtering technique that reduces noise in form of slangs, emoticons, abbreviations in SMS as well as expand message size must be employed to enhance adequate classification. Thus, our research goal(s) is to propose a hybrid deep learning neural network model for text normalization and semantic expansion in SMS spam filtering.

The proposed model properties and goals will include:

- Perform repetitive tasks without emotional defects
- Embody the knowledge of human experts with the help of special software tools, manipulate data to solve problems and make decisions in that domain.
- Processes are better formalized and defined on machines.
- Knowledgebase update is automatic
- Processes are better formalized and defined on machines.

4. MEMETIC BAYESIAN NETWORK EXPERIMENTAL FRAMEWORK

SMS spam filters can have capacity and granted capability to transcribe emoticons, abbreviations and slangs into standard terms as well as expand message size to enhance better feature extraction for classification algorithms and approaches. The study will also serve to reduce orthographic error found in SMS, chat groups and another social network communication medium that impedes machine learning algorithm. This is because from the various approaches adopted to SMS spam filters – the content-based models with text pre-processing has shown to perform better. Machine translation (MT) performs better when applied to normalized text messages [46]. It can combined multiple approaches in noisy data, text normalization to create a better output. But, extracting only relevant feats and/or parameter to train the classifier has been reported to contribute to the efficiency of SMS spam filters [47-50]. Thus, we propose text preprocessing SMS spam filter model with the capability of normalizing, expanding text messages and extracting suitable features as dataset input parameters for training the adopted classification algorithm and model. Study uses KDD-CUP ’99 dataset.

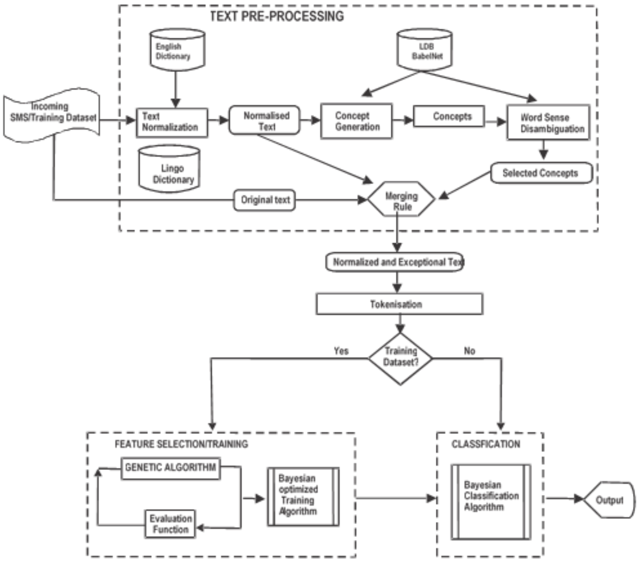

Figure 1. Proposed genetic algorithm trained bayesian network

The model is represented in Figure 1 explained as thus:

a. Raw text represents the original text from the sender for normalization and expansion.
b. Text normalization employs two dictionaries: (a) first, an English dictionary to check if text are English so as to then normalize text to its root form, and (b) second, is a slang dictionary to translate slangs into English text. The basic operation of this stage is to replace slangs and abbreviation with standard English words from these dictionaries. The Freeling English dictionary and No slang dictionary are proposed.
c. Concepts generation are semantically analyzed already normalized text to deduce their concept. The concepts are provided by Language Data Base BabelNet repository.
d. Word sense disambiguation (WSD): Here, from a variety of concept generated, this stage is used to find the concept that is more relevant according to the context of the original message, among all generated concepts related to a certain word. It equally relies on concepts are provided by Language Data Base (LDB) BabelNet repository
e. Tokenisation unit: Tokenization is the process of breaking down a text corpus into individual elements that serve as input for various natural language processing algorithms. Normalised texts are broken into individual words and stop words and punctuation characters are equally removed in this unit.
f. Merging Rule: It employs parameters that define the combination of result of pre-processing (original text, normalization and disambiguation stage). Merging rule answers the question from each stage as follows: (a) should it keep the original token(s)?, (b) should text normalization be performed?, (c) should it perform concepts generation?, and (d) should it perform the word sense disambiguation?
g. Normalized and Expanded text is a combination of text obtained from various output of preferred stages of the pre-processing model.

4.1. Feature selection, training and rationale for choice of model

Need to minimize the number of features as input parameters for classification – since, an increase in the number of features used will add to the computational complexity of the system. Thus, the CGA algorithm is used in selection of features obtained from the text pre-processing section. The input is the dataset (tokens obtained via tokenization of normalized and expanded text from text pre-processing section). The model is made up of the following sections:

- GA Unit – yields a rule-based, genetic representation of normalized and expanded test defined. The algorithm then initializes model with a random population that is created and subjected to repetitive application of recombination, mutation, inversion and selection operators to improve the generated population from the original dataset.
- Evaluation Unit contains a fitness function that measures the quality of represented solution. It computes optimality of a solution by comparing the chromosomes against all other chromosome using some predefined function.
- Training Unit: Trains the filter based on Bayes Probability Theorem. It uses known SMS corpus of spam and genuine messages/texts. A collection of tokens appearing in each corpus and their total occurrences (scores) are maintained in the database – so that based on their occurrences, each set of spam and genuine data is assigned a criterion or probability score for its capacity of determining a text or message to either be a spam or genuine text.

4.2. Classification section

Based on the frequency probability of occurrence of each word (tokens) as spam or legitimate, each incoming unseen normalized message data is processed and classified as either legitimate or spam by the Bayesian classifier. In the event of misclassification, users can rectify this classification by reading the message and re-adding the message to inbox. This will automatically correct and update the database for future classification. Thus, making Bayesian filters quite adaptive.

4.3. Output section

Result of the classification of the filter into Spam or Ham, is the expected output of this unit.

4.3. Experimental model operations

Ojugo [42] described a genetic algorithm trained neural network employed in early diabetes detection. GANN is initialized with (n-r!) individual if-then, fuzzy rules (i.e. 6-4!). Individual fitness is computed as 30-individuals are selected via the tournament method to determine new pool and selection for mating. Crossover and mutation are applied to help net learn the dynamic, non-linear underlying feats of interest via multipoint crossover to yield new parents. The new parents contribute to yield new individuals. Mutation is reapplied and individuals are allotted new random values that still conform to the belief space. The mutation applied depends on how far CGA is progressed on the net and how fit the fittest individual in the pool (i.e. fitness of the fittest individual divided by 2). New individuals replace old with low fitness so as to create a new pool. Process continues until individual with fitness of 0 (i.e. solution) is found. Rule-based encoded spam as shown in Table 1. Generation of population from parents as shown in Table 2.

Table 1. Rule-based encoded score

Code	Rule Input Parameters	Genuine	Spam
P01	Message Size	0.50	0.50
P02	Message Character	0.50	0.50
P03	Message From	0.50	0.50
P04	Message To	0.50	0.50
P05	Subject	0.30	0.70
P06	Body of Message	0.25	0.75

Table 2. 1st and 2nd generation of population from parents

S/N	Selection	Chromosomes (Binary 0 or 1)			Fitness
		Parent 1st Gen	Crossover	Parent 2nd Gen	Function
1	50	110010	1 and 6	1100**01**	49
2	50	110010	2 and 5	1100**10**	50
3	50	110010	3 and 6	1100**01**	49
4	50	110010	4 and 5	1100**10**	50
5	30	011110	5 and 6	0111**01**	29
6	25	011001	6 and 5	0110**10**	26

Initialization/selection via ANN ensures that first 3-beliefs are met; mutation ensures fourth belief is met. Its influence function influences how many mutations take place, and the knowledge of solution (how close its solution is) has direct impact on how algorithm is processed. Algorithm stops when best individual has fitness of 0.3. Model stops if stop criterion is met. GANN utilizes number of epochs to determine stop criterion.

5. FINDINGS AND DISCUSSION

With Naïve Bayes and GA (as standalone model) to benchmark the intelligent system and ascertain how well our hybrid GABN algorithm performed, we obtain the results in Figure 2 and Figure 3 respectively as seen below. the hybrid gabn (memetic) algorithm outperforms standalone naïve bayes and GA model. However, for the mean processing time required to converge – it is found that GABN performed least. This can be attributed to the fact that: (a) the hybrid model needs to first use GA as pre-processor to train Bayesian network, (b) for such hybrids, there are always structural dependencies with the underlying heuristics employed/merged and conflicts in data encoding that is required. These must be resolved in order for the model to perform appropriately.

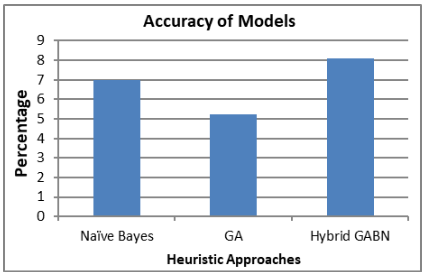

Figure 2. Model/heuristic accuracy in percentage

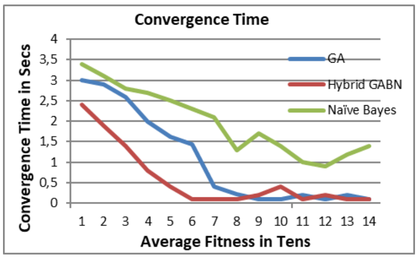

Figure 3. Model/Heuristic convergence time in seconds

5.1. Model Evaluation

In this study, accuracy, recall, error rate (ER) and specificity are used to evaluate the performance of the detection models. The formulas of the above criteria are calculated as follows:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

$$Error\ Rate = \frac{FP+FN}{FP+TP+TN+FN} \quad (3)$$

$$SPEC = \frac{TN}{TN+FP} \quad (4)$$

A true positive (TP) is a case (rule) that correctly distinguishes spam from ham. A true negative (TN) shows normal text data classified correctly as normal. A false negative (FN) is a case in which a text is classified as normal data, and a false positive (FP) is a case in which a normal text is classified as a spam. The accuracy rate is the overall correct detection accuracy of the dataset. ER refers to the robustness of the classifier, Recall is degree of correctly detected attack types of all cases classified as attacks; while, specificity is the percentage of correctly classified data. In the above, higher accuracy and recall and lower ER indicate good performance.

To further measure effectiveness and accuracy, we measure their rate of misclassification and corresponding improvement percentages in both training and test data sets as summarized in Tables 3 and 4 respectively. Equations for misclassification rate and its improvement percentage of unsupervised (B) model against supervised (A) model respectively, is calculated as follows:

Tables 3 and 4 respectively shows misclassification error rate with Naïve Bayes, GA and GABN at 23.2%, 4.7% and 1.02% (i.e. error rate in false-positive and true-negative) respectively; Consequently, they all promise an improvement rate as of 3.6%, 4.02% and 0.12% respectively.

$$Misclassification\ Rate = \frac{No.of\ Incorrectly\ Classified\ Rules}{No.of\ Sample\ set} \quad (5)$$

Table 3. Misclassification Rate of Each model

Model	Classification Errors	
	Training Data	Testing Data
Naïve Bayes	52.5%	23.2%
Genetic Algorithm	48.4%	4.7%
GABN	19.6%	1.02%

Also, its improvement percentage is computed as thus:

$$Improvement\ Percentage = \frac{MR(A)-MR(B)}{MR(A)}\ x\ 100 \qquad (6)$$

Table 4. Improvement Percentage

Model	Improvement %	
	Training Data	Testing Data
Naïve Bayes	2.11%	3.6%
Genetic Algorithm	2.32%	4.02%
GABN	0.09%	0.12%

3. CONCLUSION

From the consequences of spam to users, several concerted efforts to detect spam intrusion in various communication media has paid off especially in combating email spam. Spam Filters work by first receiving part (or all) of the message and then analyzing it in some way to decide whether it is ham (i.e. legitimate message) or spam. The performance of a spam filter can be measured by the number of false-positives (incorrectly marked as spam) and false-negatives (unidentified spam) that it generates. An ideal spam filter will correctly classify all SMS with almost zero error rates of false positive/negative – through tradeoffs between the number of false positives and false negatives.

REFERENCES

[1] Ojugo, A. A and Eboka, A. O., "Comparative evaluation for high intelligent performance adaptive model for spam phishing detection," *Digital Technologies*, vol. 3, no. 1, pp. 9-15, 2018.

[2] Ojugo, A.A., Eboka, A.O., "Signature-based malware detection using approximate Boyer Moore string matching algorithm," *Int. J. of Mathematical Sciences and Computing*, vol. 3, no. 5, pp. 49-62, 2019.

[3] Text Request. The Complete Overview of Business Texting. 2016. [web]: available at https://www.textrequest.com/blog/texting-statistics-answer-questions/

[4] Chaminda, T., Dayaratne, T. T., Amarasinghe, H. K. N., Jayakody, J. M. R. S., "Content-based hybrid SMS spam filtering system," *Proceedings of ITRU Research Symposium*, University of Moratuwa, pp. 31–35, 2013.

[5] Gomez Hildago, J. M., Buenaga Rodrıguez, M and Cortizo Perez, J. C., "The role of word sense disambiguation in automated text categorization," *In Proc. of the 10th NLDB*, pp. 298–309, 2005.

[6] Shahi, T. B., Yadav A., "Mobile SMS Spam Filtering for Nepali Text using Naïve Bayesian and Support Vector Machine," *Int. J. of Intelligence Science, Computer Science and Communications*, vol. 4, no.1, pp. 24-28, 2014.

[7] Murynet, S., Piqueras Jover, R., "How an SMS-Based malware infection will get throttled by the wireless link,". *In Proceedings of IEEE ICC 2012 - Communication and Information Systems Security Symposium (ICC'12 CISS)*, Ottawa, Canada, 2012.

[8] Murynet, S., Piqueras Jover, R., "Analysis of SMS Spam in Mobility Networks. *International Journal of Advanced Computer Science*, vol. 1, no. 1 pp. 1-8, 2011.

[9] Agwu. C.O., "The Consequences of Mobile Spam in Nigeria Emerging and Evolving Mobile Communication Sector of the Economy," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no.5, pp. 117-124, 2015.

[10] Mobile Ecosystem Forum, "28% Mobile Consumers Receive SMS Spam Every Day," 2017.

[11] Neelmay Desai and Meera Narvekar, "Normalization of Noisy Text Data," *Procedia Computer Science*, vol. 45, pp. 127-132, 2015.

[12] Jiang, N., Jin, Y., Skudlark, A., Zhang, Z., "Understanding SMS spam in large Cellular Network: Characteristics, Strategies and Defenses, Intelligent Systems," *IEEE*, vol. 27, no. 6, pp. 15-26, 2011.

[13] Zablotskaya, N. Fraudulent spam. Securelist, 2008.

[14] Hedieh Sajedi, Golazin Zarghami Parast, Fatemeh Akbari, "SMS Spam Filtering Using Machine Learning Techniques: A Survey," *Machine Learning Research*, vol. 1, no. 1, pp. 1-14, 2016.

[15] Wang, C., Zhang, Y., Chen, X., Liu, Z., Shi, L., Chen, G., "A Behavior-based SMS Anti-Spam System," *IBM Journal of Research and Development*, NJ, USA, vol. 54, no. 6, pp. 651-666, 2010.

[16] Tiago, A.A., Tiago, P.S., Igor, S., Jose, M and Gomez Hildago, J.M., "Text normalization and semantic indexing to enhance Instant Messaging and SMS spam filtering," *Knowledge-Based Systems*, vol. 108, no. 15, pp. 25-32, 2016.

[17] AiTi A.W., Zhang, M., Xiao, J., Su, J., "A phrase-based statistical model for SMS text normalization," *In Proceedings of the COLING/ACL on Main conference poster sessions*, pp. 33–40, 2006.

[18] Nuruzzaman, T. M., Lee, C., Abdullah, M.F.A., Choi, D., "Simple SMS spam filtering on independent mobile phone," *Journal of Security and Communication Networks*, vol. 5, no.10, pp 1209–1220, 2012.

[19] Narayan, A., Saxena, P., "The curse of 140 characters: Evaluating the efficacy of SMS spam detection on android," *In Proceedings of the 13th ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM '13)*, Berlin, Germany, pp.33–42, 2012.

[20] Androulidakis I., Vlachos V., Papanikolaou, A. FIMESS: filtering mobile external SMS spam. In Proceedings of the 6th Balkan Conference in Informatics, ACM, New York, USA, pp. 221-227, 2013.

[21] Hasib, S., Motwani, M., Saxena, A., "Anti-Spam Methodologies: A Comparative Study. *Int. J. Computer Sci. Information Technologies*, vol. 3, no. 6, pp. 5341-5345, 2012.

[22] Triggs R., "What is SMS and how does it work," 2013.

[23] Prachi, G.J., Pateriya, J.R.K., "A Survey on Email Spam Types and Spam Filtering Techniques," *International Journal of Engineering Research & Technology (IJERT)*, 2014.

[24] Delany S.J. Using Case-Based Reasoning for Spam Filtering. Published PhD Thesis submitted to the Dublin Institute of Technology in fulfillment of the requirements for the degree of Doctor of Philosophy School of Computing, Dublin Institute of Technology. [web]: available at https://pdfs.semanticscholar.org/c934/9dfe80c762249bdb030185c481653cfb2ba6.pdf

[25] Cormack, G. V., Gomez Hidalgo, J. M., Puertas Sanz, E., "Spam Filtering for Short Messages," in *Proc. of the 16th ACM CIKM*, pp. 313–320, 2007.

[26] Xu, Q., Evan, W. X., Qiang, Y., Jiachun, D., Jieping,Z., "SMS Spam Detection Using Non-Content Features," in *IEEE Intelligent Systems*, vol. 27, no. 6, pp. 44-51, 2012.

[27] Uysal, A. K., Gunal, S., Ergin, S., & Sora Gunal, E., "The impact of feature extraction and selection on SMS spam filtering," *Journal Elektronika IR Elektrotechnika*, vol. 19, no. 5, pp. 67–72, 2013.

[28] Satterfield, B. 10 spam filtering methods. [web] available at http://www.techsoupcanada.ca/en/learning_center/10_sfm_explained

[29] Cook, D., "Catching Spam before it arrives: Domain Specific Dynamic Blacklists, *Australian Computer Society*, ACM, 2006.

[30] Han, B., Cook, P., Baldwin, T. Lexical Normalisation of Short Text Messages. ACM Transaction on Intelligent Systems and Technology, 2011. Article A

[31] Perlroth, N. Spam Invades last Refuge, the Cellphone. New York Times, 2012. [web]: available at http://preview.tinyurl.com/7nwvm3g

[32] Huang, D., Gan, Z., Chow, T.W.S., "Enhanced feature selection models using gradient-based and point injection techniques," *Neurocomputing*, vol. 71, pp. 3114–3123, 2008.

[33] Gheyas I.A., Smith, L.S., "Feature subset selection in large dimensionality domains," *Pattern Recognition*, vol. 43, pp. 5–13, 2010.

[34] Vafaie, H., De-Jong, K. Genetic Algorithm as a Tool for Feature Selection in Machine Learning, 1997. [web] researchgate.net/publication/2722353_Genetic_Algorithms_as_Tool_for_Feature_Selection_in_Machine_Learning

[35] Sung-Sam, H., Wanhee, L., Myung-Mook, H., "The Feature Selection Method based on Genetic Algorithm for Efficient of Text Clustering and Text Classification," *Int. Journal on Advance Soft Computing Application*, vol. 7, no. 1, pp. 23-40, 2015.

[36] Catherine, K., François, Y., Géraldine, D., "Normalizing SMS: are two metaphors better than one," in *Proceedings of 22nd International Conference on Computational Linguistics*, pp 441–448, 2008.

[37] Ojugo, A.A and Eboka, A.O., "Modeling the computational solution for market basket associative rule mining approaches using neural network," *Digital Technologies*, vol. 3, no. 1, pp. 1-8, 2018.

[38] Ojugo, A.A., Eboka, A.O., "Inventory management and prediction using market basket analysis associative rule mining: memetic algorithm approach," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 8, no.3, 2019.

[39] Ojugo, A.A., A. Eboka., E. Okonta., R. Yoro., F. Aghware., "Genetic algorithm rule-based intrusion detection system," *Journal of Emerging Trends in Computing Information System*, vol. 3, no. 8, pp. 1182-1194, 2012.

[40] Ojugo, A.A., Yoro, R.E., "Computational intelligence in stochastic solution for Toroidal N-queen," *Intelligence Computing and Applications*, vol. 2, no. 1, pp. 46-56, 2013.

[41] Ojugo, A.A., Emudianughe, J., Yoro, R.E., Okonta, E.O., Eboka, A.O., "A hybrid neural network gravitational search algorithm for rainfall runoff modeling and simulation in hydrology," *Progress in Intelligence Computing and Applications*, vol. 2, no. 1, pp. 22-33, 2013.

[42] Ojugo, A.A., D. Oyemade., Yoro, R.E., Eboka, A.O., Yerokun, M.O., Ugboh, E., "A comparative evolutionary models for solving Sudoku," *Automation, Control & Intelligent Systems*, vol. 1, no. 5, pp. 113-120, 2013.

[43] Reynolds, R., "Introduction to cultural algorithms," *Transaction on Evolutionary Programming (IEEE)*, pp.131-139, 1994.

[44] Perez, M and Marwala, T., "Stochastic optimization approaches for solving Sudoku," in *Proceeding of IEEE Congress on Evolutionary Computing*, pp 256 – 279, 2011.

[45] Gomez Hidalgo, J. M, Bringas, G. C., Sanz, E. P., Gracia, F.C., "Content-based SMS Spam filtering," in *Proceedings of 2006 ACM Symposium on Document Engineering*, pp107-114, 2006.

[46] 46 Vafaie, H., De-Jong, K. "Genetic Algorithm as a Tool for Feature Selection," *in Machine Learning*, 1997,

[47] Gheyas I.A., Smith, L.S., "Feature subset selection in large dimensionality domains," *Pattern Recognition*, vol. 43, pp. 5–13, 2010.

[48] Ojugo, A.A., A. Eboka., R. Yoro., M. Yerokun., F.N. Efozia., "Hybrid model for early diabetes diagnosis," *Mathematics and Computers in Science & Industry*, vol. 50, pp. 207-217, 2015.

[49] Phillip, K., Hieu, H.M., "Open source toolkit for statistical machine translation," *Technical report, Annual Meeting of the Association for Computational Linguistics (ACL)*, 2007.

[50] Sethi, G., Bhootna, V., "SMS Spam Filtering Application using Android," *International Journal for Computer Science and Information Technologies*, vol. 5, no. 3, pp. 1424-1426, 2014.