مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
Journal of the College of Basic Education Vol.29 (NO. 120) 2023, pp. 1-15

Proposed Naïve Bayes- Genetic algorithm to detect black hole attacks in MANETs.

Raghad Mohammed Hadi [(1)]
Al-Mustansiriya University,
College of Medicine,
Physiology Department,
Iraq, Baghdad
raghadqajar@gmail.com

Lamia Hassan Rahef [(2)]
Al-Mustansiriya University,
College of Medicine,
Physiology Department,
Iraq, Baghdad
lamiahassen32@gmail.com

Osamah waleed abdulqahr [(3)]
Ministry of Education,
Directorate of Nineveh Education/
Halab intermediate school
Iraq, Mosul
osamaalkubaissy@gmail.com

Abstract:

The threats and attacks on mobile ad hoc networks (MANETs) are significant, making it difficult for traditional security systems to provide complete protection. Therefore, an efficient hybrid clustering approach must be designed to construct an intrusion detection system (IDS) that is suitable for this network. IDSs are crucial in MANETs due to the presence of black hole threats, which are the most significant vulnerabilities in this network.Our suggestion is to use a hybrid classifier to detect black hole attacks in MANETs. This can be achieved by using the Naïve Bayes algorithm for clustering to select the cluster head, and modify the Genetic Algorithm to identify the node responsible for a black hole attack on the optimal path. Finally, the confidence server instructs the destination node. If permitted, it alerts the collection head; otherwise, it identifies the node as a malicious one in the black hole attack within each cluster. The results of our proposed technique show that it has improved package damage rate, quantity, package distribution ratio, whole network interruption, and standardized directing capacity parameters compared to current black hole detection approaches.

The simulation was done in KDD cup 99 to carry out black hole attack and trace file obtained is used as dataset for training and testing purpose using visual basic.

Keywords: MANETs, ANNs, Black hole Attack, Knowledge Discovery in Databases (KDD), clustering, genetic algorithm.

Introduction:

Mobile Ad-hoc Networks, also known as MANETs, are wireless networks that can function independently without the need for any infrastructure support. One of the key advantages of MANETs is their ability to adapt and reconfigure themselves on-the-fly in response to changes in the network topology. This makes them particularly appealing for military applications, where their random nature can be useful in tactical environments.

This article discusses various aspects of MANETs, including their applications, characteristics, limitations, different types, and security concerns. Overall, MANETs offer a lot of potential for military and other applications where traditional wired or wireless networks may not be feasible or practical. However, they also come with some unique challenges and risks that need to be carefully considered and addressed [1]. The movement of nodes is random, which is why an ad-hoc network works between the participating nodes, causing random changes in the network. Wireless users can form the network dynamically and do not need any infrastructural setups [2]. Through the current attention and growth in the progress of internet and announcement skills ended the previous period, there are several measures in place to safeguard the network against potential threats, such as the implementation of a firewall, and intrusion detection system (IDS) but like this defenses not prepare assurance whole network safety, so numerous organizations require to constructed for this drive such as deep learning and machine learning which are two subsections of artificial intelligence that have gathered a great deal of care to change the nodules in the network to clever and brainy. The entrenched intellect in the nodules allow them to gross brainy decision separately like persons [3, 4]. Data mining is a crucial aspect of KDD, which involves extracting essential information from vast databases or data marts and transforming it into various formats such as patterns, summary reports, and views. [5, 6, and 7]. To progress a supple and actual IDS to classify and detect unexpected and random bouts by deep neural network. The incessant alteration in MANET conduct and quick development of bouts brands it essential to assess numerous datasets which are produced ended the centuries done by stationary and active methods. This category of education enables to classify the greatest procedure which container efficiently effort in noticing upcoming attacks [8]. The black hole attack is unsafe dynamic attacks in ad hoc networks. The black hole node

performances through replying to entirely trail demand packages, imagining to need the finest trail to the destination nodule, and formerly abolishing all conventional packages. In this category of outbreak, there are regularly two suitcases where the data package was gotten expending a malicious nodule; which a malicious nodule usages the routing procedure like the AODV protocol, to direct route response controller message (RREP) directly to the foundation nodule receiving of the route appeal controller nodule (RREQ). This RREQ excess reasons redundant above that clues to summary net presentation like the distribution of packages and dormancy. The achievement of the RREQ transmission was hurt from a concealed nodule problematic. Consequently it droplets the data straight. Consequently, the basis nodule developed unable to direct its informations to the terminus nodule where it interrupts the effect of the net and its connectivity [22, 9]. Jim Anderson initially conceptualized the IDS in 1980. Subsequently, several IDS products were developed and refined to meet the demands of network security. The significant advancements in technology over the years have led to a substantial expansion of the internet's reach, resulting in an increased volume of requests processed by network nodes [10]. So an enormous quantity of significant informations is life made and communal crossways dissimilar net nodules. The safety of informations and net nodules has develop a stimulating job owing to the group of a big amount of novel bouts also finished the change of an ancient bout or an original bout. Nearly all nodule inside a net is weak to safety intimidations. For example, the informations nodule might be actual significant for a society. Slightly cooperation to the nodule's material might reason an enormous influence on that society in rapports of its marketplace standing and monetary fatalities. Current IDSs have exposed disorganization in noticing numerous bouts counting zero day bouts and plummeting the false alarm rates (FAR). This consequences in a request for an effectual, precise, and price operative NIDS to deliver robust safety to the net [11, 12]. The most current classification approaches is Naïve Bays (NB) classifier which is grounded on relating Bayes proposition to categorize the novel example with robust expectations among the qualities. The assumption of individuality implies that the probability of one component does not affect the probability of another component. The NB classifier can be expressed as Equation (1), where Pro(Cl) represents the probability of a class and Pro(c1,c2,..,Cn|a) represents

the probability of features within a class. The assumption of feature independence is described in Equation (2).

$$a(F) = \arg max_{a \in A}\, pro(a) pro(c_1, c_2, \ldots., c_n\,|a) \ldots.. (1)$$

$$pro(F|a) = pro(c_1, c_2, \ldots. c_n|a) = \pi_{i=1}^{n} pro(c_i|a) \ldots.. (2)$$

While Genetic Algorithm is an Evolutionary algorithms which used a construct adaptive methods by using regular of instructions that employment evolutionary chiefs. They are probabilistic exploration approaches and optimization heuristics that require the capability to discovery a explanation to the exploration and optimization responsibilities using pretending the normal organic development, at separately cohort, the populace changes to areas in the exploration interplanetary that are healthier using faking the procedures of progress (selection, recombination, and mutation), the finest recognized approaches in the arena of evolutionary procedures are genetic algorithms [13, 14, 15]. Genetic Algorithms (GAs) was a procedure were hearty and arbitrarily exploration. Genetic algorithm contains many steps as follow: Discussing the steps involved in a genetic algorithm. The first step is initialization, which gives the algorithm a starting point. The second step is selection, where a parent is chosen for a route search. There are different ways to select the parent, such as fitness-based selection, rank-based selection, and competition-based selection. The third step is crossover, which involves swapping sections of chromosomes between couples to create new ones. There are different types of crossover, such as 1-point and 2-point crossover. The final step is mutation, where a bit in the chromosome is randomly selected and altered to ensure that all chromosomes contain the best genes in the new generation [16, 17, and 18].The important data processing step from any huge dataset is feature selection after collected it since respectively nodule in the MANET through the standard situation and the black hole attack situation in instruction to generate a usual outline which produced consuming informations composed from MANET through lack the black hole attack, and bout profile which generated consuming data composed from MANET with presence the black hole attack [9]. Two commonly used methods for reducing features involve information gain (IG), which evaluates the quality of a feature by measuring its entropy with respect to the class. Entropy is a measure of randomness in information theory, and higher entropy indicates more informative content in a given attribute. The entropy of each feature is calculated using Equation (3), where c represents the value of the feature, ranging from 1 to n. The amount of information

required to classify G after partitioning it into n subsets using C is expressed in Equation (4). The information gained by splitting a feature C is given by Equation (5) [19].

$$\text{Info G=H(C)} = -\sum_{c=1}^{n} pro(c)\log_2 pro(c) \ldots\ldots (3)$$

$$info_C(G) = \sum_{J=1}^{V} \frac{|G_i|}{|G|} * \mathrm{I}(G_j) \ldots . (4)$$

$$\text{Gain(C) =info G-}info_C(G) \ldots . (5)$$

In instruction to resolve the overhead difficulties, this paper projected an improved routing system in MANETs which based on NB classifier to find number of cluster head and optimal path to destination, and GA to select black hole attack from optimal path. This paper is structured as follows: Section 2 outlines the related work, while Section 3 details the proposed methodology. The results are presented in Section 4, and the paper concludes with Section 5.

Previous Studies:

Renu Popli et. al, in 2021 [12] they researchers suggest to use Machine learning methods offer the education competence to a organization and inspire version to the surroundings, founded to numerous rational and numerical processes. The main objective of machine learning was to distinguish the difficult shapes and create choices founded on the consequences. Praveen Bondada et. al, in 2022 [20] they researchers suggest to use a protected and dynamism effectual directing procedure was planned by collection key managing. Asymmetric key cryptography was secondhand, that includes two particular nodules which were the labeled the Calculator Key and the distribution key. As a consequence, additional nodules essential not achieve at all generous of added calculation for construction the secret keys. Kamini Maheshwar et. al. in 2013 [21], they researchers suggest to use Customary data mining methods that function on organized informations such as commercial databases. Data mining based intrusion detection need fewer skilled facts however deliver decent presentation. The discovery kind was rented from intrusion detection as either misuse detection or anomaly detection. This paper delivers the main progression in the data mining founded intrusion detection study by these methods, the structures and types in the plotted effort

The Main Part: (The Researcher' Work)

The main framework of the planned system is as exposed in figure (1), which show that there are three main components of proposed system:

To start, we need to set up the network simulator environment with basic dimensions and create a number of nodes within the MANETs. These nodes will be split into two subsets: training nodes and testing nodes. The basis and target nodes, starting from N node in the training set, will be labeled with their positions. Next, we will use a Naïve Bays (NB) classifier as a cluster algorithm to determine the optimal number of cluster heads. We will then produce a code to describe the route from basis to destination and use GA for selecting the best black hole node from the optimal path. After that, we will calculate the fitness function and identify any attacker nodes. If an attacker node is found, it will be saved in the routing table and all nodules connected through it will be discarded to achieve better results.The dataset of system is displays in table (1) used in algorithm and accuracy results. These spilt into two dataset and classify by NB classifier to find optimal cluster head (CH) and optimal path from source to destination. The proposed system's performance was fully assessed using basic resources such as quantity. end to end delay, bit error rate, packet delivery ratio, in which network will be advanced founded on assumed table (1).

Table 1:Parameter setting

Parameters	**values**
Shape of region	random
Number of nodes	49-200
Packet size	64kb
Routing protocols	Neural network
Simulation environment	Dynamic

Algorithm (1): feature selection based on information gain

Input*: black hole nodes and its features*

Output: *information gain for each node.*

Begin

Step 1*:T= total number of black node in (all nodes in MANTs)*

Step2*: for each class in (all nodes in MANTs)*

1. *Pro(black node)=number of black node/T*
2. *Pro(not black node)= number of not black / T*
3. *Find the entropy of class by using Equ.1:*

Entropy (E) is

$$H(E)= -\sum_{Y\in V} p(E)\, log_2\, p(E) \dots\dots Equ.1$$

P(E) : probability function for random variable E

4. *Select the best feature with the lowest value of entropy for black nodes.*

End.

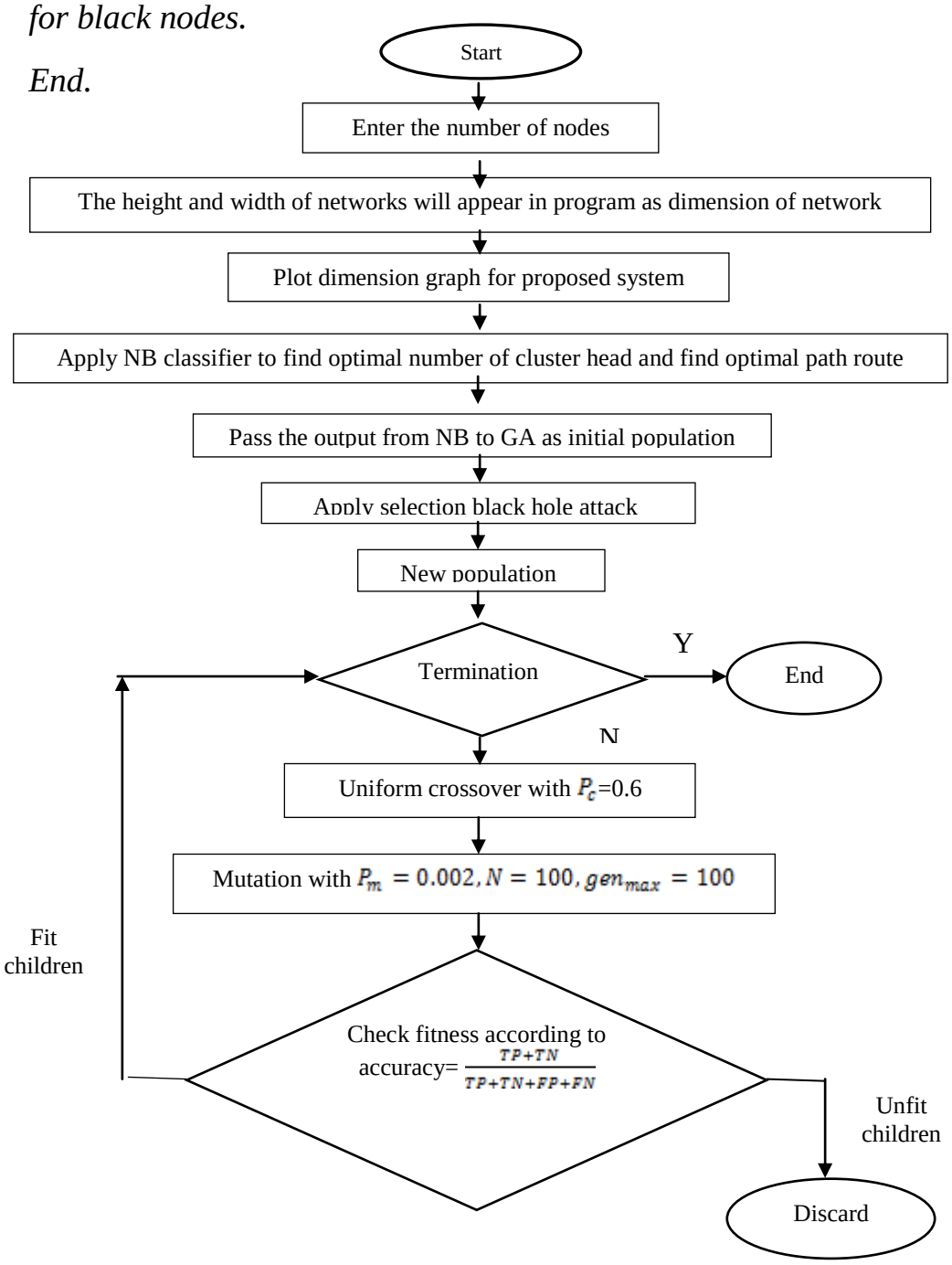

Figure 1: Flowchart of proposed system

Pre-processing the Data

This research procedure was applied to the entire NSL-KDD dataset, which was designed to address the characteristic challenges of the KDD Cup 1999 dataset that contained too many obsolete records. Although it was an old and flawless demonstration of current real networks, it is still a directory that was used to compare intrusion detection systems. The KDDCUP'99 dataset is widely castoff as single of the datasets that were freely obtainable on behalf of networks. It is founded on the 1998 Intrusion Detection Assessment Package organized by MIT Lincoln Labs to evaluate intrusion detection investigation. The KDDCUP'99 dataset consisted of approximately 4 gigabytes of training data. The large amount of training data was crucial in constructing a network for intrusion detection. Certain structures within the dataset provided features that helped distinguish attack patterns from normal behavior. The KDDCUP'99 dataset was widely used to evaluate intrusion detection systems, it hurts from approximately difficulties that could consequence on the presentation of the appraised systems. Giving to the consequences of the statistically examination on this dataset, the first significant problematic in KDDCUP'99 dataset was the enormous of terminated records. The massive volume of terminated records in training set chief to brand the learning procedures subjective to the more recurrent records. Which lead to additional damaging to the network. Therefore, arbitrary portions of the train set were castoff as test set which will create the contrast among the assessment consequences of diverse investigation effort very problematic. So to resolve these difficulties the writers planned a different dataset which was NSL-KDD. The projected dataset comprises designated archives of the KDDCUP'99 dataset lacking any terminated records, thus it was a different variety of KDDCUP'99 dataset. The projected dataset has the subsequent benefits ended the unique KDD dataset:

1. The learning procedures not dependent to the additional repeated records. So the training set in the planned dataset doesn't contain any redundant records so the
2. The estimation consequences will not dependent to the approaches that have the greatest recognition rates on the recurrent records because there weren't any terminated records in test set.
3. Any experiments can trip lacking arbitrarily choice a lesser portions from train set to usage it as test set.

Evaluation metrics

The evaluation of classifiers has always been done through the use of a confusion matrix. This environment comprises evidence around the real and foretold arrangements made through the classifiers. This data is used to determine how well the classifiers are performing.

Table below displays an example of confusion matrix for dual modules. Where (TPo) was the value specifies for the quantity of confident tasters that are properly classified by proposed system. FPo denotes to the quantity of positive tasters that was erroneously confidential, likewise FNe denotes to the quantity of adverse tasters that are categorized as Positive tasters as a replacement for Adverse taster. Whereas, TNe was the quantity of Negative tasters which are properly categorized by the classifier. Founded on the below Table, the presentation of each one of the preceding classifiers can be assessed consuming some of actual general arithmetical events which are:

- Accuracy: was an amount that cast-off to control the fraction of tasters that were categorized properly. Since the confusion matrix, accurateness was intended as subsequent:

$$Accuracy = \frac{TPo + TNe}{TPo + FPo + FNe + TNe} \ldots\ldots (6)$$

- Precision: was a relation of amount of related tasters that were recovered to the total amount of tasters that are recovered. It was calculated as following :

$$\text{precision} = \frac{\text{TPo}}{\text{TPo} + \text{FPo}} \ldots (7)$$

- Recall; it was a relation of the amount of related tasters that were recovered to the whole amount of related tasters.

$$\text{Recall} = \frac{\text{TPo}}{\text{TPo}+\text{FNe}} \ldots (8)$$

- F-measure: it was a choral nasty of recall and precision, and intended as subsequent:

$$\text{f} - \text{measure} = \frac{2 * \text{precision} * \text{recall}}{\text{precision} * \text{recall}} \ldots\ldots (9)$$

Table 2: Confusion matrix

	Positive class	Negative class
Positive class	TPo	FNe
Negative class	FPo	TNe

The estimation of the planned organization presentation was assumed in relations of; accuracy of noticing bouts against normal actions (accuracy binary), accuracy of distinguishing four types of attacks, accuracy to distinguish black hole attack in MANETs network, Discovery rate (DR), error rate(ER) and confusion matrix were occupied in deliberation. Where TPo (true positive), TNe (true negative), FPo (false positive) and FNe (false negative). Table3 and figure3 shows the results in the system suggested, Table4 shows comprasion of proposed system with related work.

Table 3: The proposed system results using NB classifier and GA

datasets	Accuracy	Precision	Recall	DR-normal	DR-black hole	FPR-normal	FPR-black hole
KDD test	96.98%	0.955	85.15%	90.95%	80.87%	39.89%	20.71%
KDD test 21	76.99%	0.978	80.01%	97.08%	85.56%	40.86%	19.62%

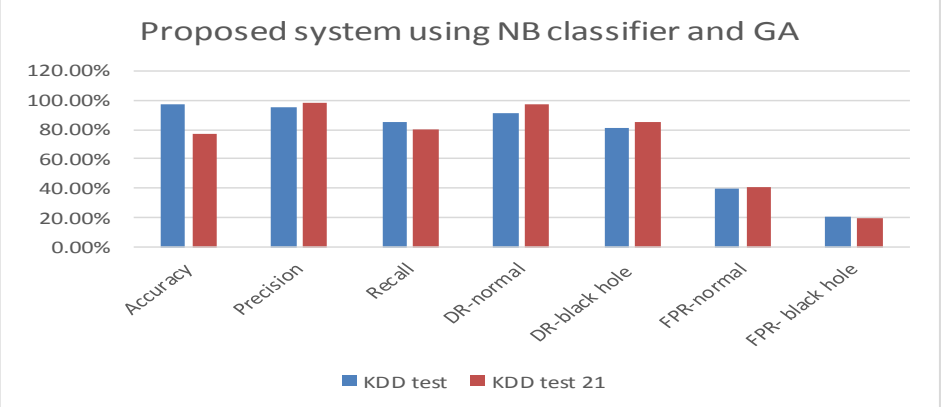

Figure 2: Results of proposed system using NB and GA

Table 4: comparison with the related works

REF.	Methods	Accuracy	advantages	disadvantages
[10]	Using machine learning (ML) and deep learning (DL)-based IDS systems	94%	deployed as potential solutions to detect intrusions across the network in an efficient manner	Depended on improving ML and DL-based NIDS to detect IDs.
[12]	ML algorithms	92%	applied to protected the mobile ad-hoc networks	Ineffective whenever there is a alteration in security pressures.
[14]	using group key management. Asymmetric key cryptography	94%	which involves two specialized nodes, labeled the Calculator Key (CK)and the Distribution Key (DK).	Extensive experimentsare performed by considering the existing and the proposed protocols.
[16]	using email	90%	identify the template mails	It has utilised relatively fewer inputs and needed tested on big

	templates for sending spam		from the whole corpora of training set emails to make the filtering process faster	data to get an optimum training set.
Proposed method	Using Naïve Baye and Genetic algorithm	97%	detect black hole attacks in MANETs.	Wants KDD cup 99 dataset to carry out black hole attack and trace file obtained for training and testing purpose using visual basic

Conclusion:

In Mobile Ad-hoc Networks (MANETs), quickly detecting malicious attacks is crucial to ensure the network's security. In this study, we developed a method that can successfully deliver packages to their destinations even in the presence of attack nodes. As the network size increases, our method reduces package damage and improves safety. Our experimental results show that our method effectively detects attack nodes, as it receives multiple responses from the standing package. The proposed method also achieves a high package delivery ratio and low delay by connecting only reliable nodes after detecting attack nodes in the network. However, our method can only detect known attacks and not all attacks. Our research shows that this method is an effective way to detect black hole attacks in MANETs. In upcoming work, we strategy to extend this method to wireless sensor networks for environmental monitoring and intelligence gathering while increasing its accuracy through more stringent criteria.

References

1. Zunnurain Hussainf M., Zulkifl Hasan M., and Ullah Z., “Mobile Ad-Hoc Networking (MANET)”, Hussain et al. (2020), UW Journal of Computer Science, Vol. 03, 09-18.

2. C. Yuen, R. Seah, S. Soon, and T. Jia, "Mobile Ad Hoc Networking," Dsta.gov.sg. 2019.
3. P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Networks," Infoscience. 2019.
4. K. Neha, M. Yogi Reddy, "A Study On Applications Of Data Mining", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 02, FEBRUARY 2020.
5. Aarti Sharma, Rahul Sharma, Vivek Kr. Sharma, Vishal Shrivastava, ―Application of Data mining-A Survey Paper‖ in International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2023-2025 2014, ISSN: 0975-9646.
6. Bharati M. Ramageri,"Data Mining Techniques and Applications‖", in Indian Journal of Computer Science and Engineering, Vol. 1 No. 4 301-305, Dec 2014.
7. Hadi M. R. , Abullah H. S., Salih Abedi M. W., "Proposed neural intrusion detection system to detect denial of service attacks in MANETs", Periodicals of Engineering and Natural Sciences Original Research Vol. 10, No. 3, May 2022, pp.70-7.
8. Hadi M. R., Hamza A. N., Abdullah H. S. , "Propose effective routing method for mobile sink in wireless sensor network", Periodicals of Engineering and Natural Sciences, 2020.
9. Yassein M. B., Khamayseh Y., AbuJazoh M., "Feature Selection for Black Hole Attacks", Journal of Universal Computer Science, vol. 22, no. 4 (2016), 521-536 submitted: 1/10/15, accepted: 30/3/16, appeared: 1/4/16 © J.UCS.
10.Ahmad Z., Khan A. SH., Shiang CH. W., Abdullah J., Ahmad F., "Network intrusion detection system: A systematic study of machine learning and deep learning approaches", Trans Emerging Tel Tech. 2021;32:e4150, wileyonlinelibrary.com/journal/ett.
11.Kotecha K. , Verma R. , Rao P. V. , Prasad P. , Mishra V. K. , Badal T. , Jain D. , Garg D., and Sharma Sh., "Enhanced Network Intrusion Detection System", Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https:// creativecommons.org/licenses/by/ 4.0/).
12.Popli R., Sethi M., Kansal I. , Garg A. and Goyal N., "Machine Learning Based Security Solutions in MANETs: State of the art approaches", Journal

of Physics: Conference Series 1950 (2021) 012070 IOP Publishing doi:10.1088/1742-6596/1950/1/012070.
13.Choudhary M., Prity and Choudhary V., "Performance Analysis Of Data Reduction Algorithms Using Attribute Selection In NSL-KDD Dataset ", International Journal of Engineering Science & Advanced Technology Vol. 4, Issue-2, 2014.
14.Bondada P., Samanta D., Kaur M., and No Lee H., "Data Security-Based Routing in MANETs Using Key Management Mechanism", Academic Editor: Arcangelo Castiglione, MPDI 2022.
15.Maheshwar K., Singh D., "A Review of Data Mining based Intrusion Detection Techniques", International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com Volume 2, Issue 2, February 2013.
16.Varghese, L., Supriya, M. H., & Jacob, K. P. (2015), "Finding Template Mails from Spam Corpus Using Genetic Algorithm and K-Means Algorithm", Training, 50, 50.
17..Holland, J. H., & Goldberg, D. (1989), "Genetic algorithms in search, optimization and machine learning", Massachusetts: Addison-Wesley.
18.Razi, Z., & Asghari, S. A. (2016), "Providing an Improved Feature Extraction Method for Spam Detection Based on Genetic Algorithm in an Immune System".
19.Abdullah S. , Abedi W.M.S. , Hadi R.M., "Enhanced feature selection algorithm for pneumonia detection", Periodicals of Engineering and Natural Sciences Original Research Vol. 10, No. 6, December 2022, pp.168-180.
20.Chaudhary, M., & Dhaka, V. S. (2015), "Automatic e-mails Classification Using Genetic Algorithm".
21.Ferragina, P., & Grossi, R. (1999), "Improved dynamic text indexing", Journal of Algorithms, 31(2), 291-319.
22.Prajapati. L., and Tomar A. S., 2015, "Detection of black hole attack with improved AODV protocol in MANET, 3535-3540. International journal of current research and review.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
Journal of the College of Basic Education Vol.29 (NO. 120) 2023, pp. 1-15

اقتراح نظام توجيه لشبكة MANETs باستخدام تقنيات تنقيب البيانات المختلطة

أ.م.د. رغد محمد هادي[1]
الجامعة المستنصرية /كلية الطب/فرع الفسلجة
07712384712
raghadqajar@gmail.com

م.لمياء حسن رهيف[2]
الجامعة المستنصرية /كلية الطب/فرع الفسلجة
07713879044
lamiahassen32@gmail.com

أسامة وليد عبد القهار[3]
وزارة التربية/ مديرية تربية نينوى/ متوسطة حلب للبنين
osamaalkubaissy@gmail.com

مستخلص البحث:

ان التهديدات والهجمات على شبكات الهاتف المحمول المخصصة (MANETs) كبيرة ، مما يجعل من الصعب على أنظمة الأمان التقليدية توفير الحماية الكاملة. لذلك ، يجب تصميم نظام التجميع المختلط الفعال لإنشاء نظام كشف التسلل (IDS) المناسب لهذه الشبكة. تعد معرفات IDS مهمة في أنظمة MANET نظرًا لوجود تهديدات للثقب الأسود ، والتي تعد أهم نقاط الضعف في هذه الشبكة ، ونقترح استخدام المصنف المختلط للكشف عن هجمات الثقب الأسود في MANETs. يمكن تحقيق ذلك باستخدام خوارزمية Naïve Bayes للتجميع لتحديد رأس الكتلة ، وتعديل الخوارزمية الجينية لتحديد العقدة المسؤولة عن هجوم الثقب الأسود على المسار الأمثل. أخيرًا ، يوجه خادم الثقة العقدة الوجهة. إذا كان مسموحًا به ، فإنه ينبه رئيس المجموعة ؛ خلاف ذلك ، فإنه يحدد العقدة على أنها خبيثة في هجوم الثقب الأسود داخل كل كتلة. وقد أظهرت النتائج بان التقنية المقترحة قد حسنت معدل تلف الحزمة والكمية ونسبة توزيع الحزمة وانقطاع الشبكة بالكامل ومعلمات قدرة التوجيه الموحدة مقارنة بأساليب أكتشاف الثقب الاسود الحالي.

الكلمات المفتاحية :

شبكة، هجوم الثقب الاسود ، أكتشاف المعرفة في قواعد البيانات ، التجميع او التصنيف ، الخوارزمية الجينية.