SECURITY OF MOBILE AD-HOC NETWORK FROM WORM HOLE ATTACK USING MACHINE LEARNING

Abstract

A mobile ad hoc network (MANET) is a network in which the nodes are mobile and connect to one another wirelessly. In a mobile ad hoc network, each node functions as a router, searching for the best route to deliver data between two points. Because of this, the network is able to operate more effectively. For situations where it would be impractical to construct a framework, such as during armed conflict, this network is crucial. The mobile ad hoc network (MANET) is a network that forms dynamically and consists of an infinite number of nodes. In the absence of a centralized network, these nodes are unrestricted in their mobility while still maintaining their ability to communicate with one another. The finding of a wormhole by two or more malicious nodes through a tunnel is the defining feature of a Wormhole Attack. When this happens, the wormhole tunnel begins accumulating data packets in preparation for transport to a new location. The proposed research recommended MANET routing that is both effective and safe. In this research important characteristics have been used at that time to construct a dataset that was labeled with the assistance of a one-of-a-kind node address. In this vein, apply two widely used Machine Learning classifiers that group data of test samples into two classifications normal and malicious, respectively to determine which classifications best fit the data. The Genetic Algorithm is being utilized for feature selection, while the Support Vector Machine and Decision Tree classifiers are being utilized for classification and comparison of these classifiers for accuracy by Confusion Matrix. The presentation of the system included an evaluation based on several

Authors

Sania Shahid
Department of Computer Science
UAF
haniyarana4@gmail.com

Dr. Salman Afsar Awan
Department of Computer Science
UAF
salmanafsar@hotmail.com
ctdm@uaf.edu.pk

Abdul Ghaffar
Department of Computer Science
UAF
hafiz108266@gmail.com

Rehan Ali Qazi
Department of Computer Science
UAF
rehanqazi83@gmail.com

Muhammad Faraz
Software Engineer, DevHouse
UK
sonafaraz@gmail.com

Muhammad Aneeb Anwer
Department of Computer Science
UAF

different measurable parameters, as well as a comparison with more modern methods.

Keywords : MANET, Wormhole Attack, SVM, Genetic Algorithm, Decision Tree, Confusion Matrix, Accuracy

I. INTRODUCTION

1. **A Mobile Ad hoc Network (MANET)** is a collection of mobile nodes that can communicate with one another through a wireless network and act independently of one another. Each mobile node in ad hoc networks acts as a router, routing data packets from their source to their final destination as shown in Fig 1. Adaptable and scalable, remote ad hoc networks are on the rise. Each mobile node functions independently and is responsible for its own management; the network as a whole is decentralized. In order to meet their own needs, the mobile nodes are free to roam wherever is necessary. It expedites the process by which nodes can enter or leave the network depending on their needs(Su and Liu, 2011). There is no limit imposed on the amount of communication that can take place between nodes. It is possible for there to be a loss of data if the association is "formed" but the nodes are located beyond the radio range of the network.

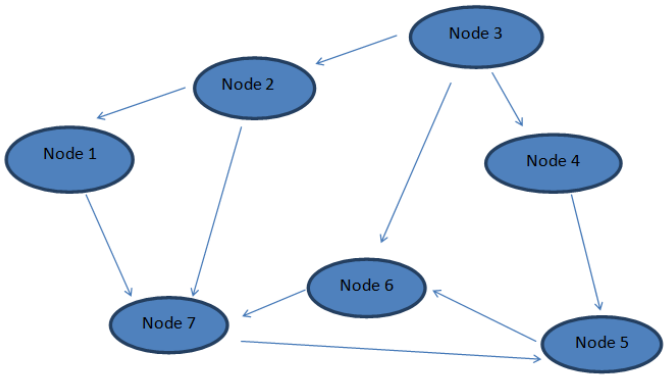

Figure 1

MANET is frequently utilised in a wide variety of disciplines, including scientific, military, search and rescue activities, and others. Improved communication between networks is another factor contributing to the rise in frequency of cyber-attacks(Chitkara and Ahmad, 2014).The MANET is an autonomously constructed network that operates without a predetermined architecture. Every node in this network performs the dual roles of router and host at the same time (Chitra and Ranganayaki, 2020). Ad-hoc wireless mobile networks are vulnerable to a wide variety of security risks due to a number of factors, including shared channel lighting, an uncertainoperating environment, constrained resource mobility, quickly growing device topology, and limited resource availability(Sookhak *et al.*, 2018).Scalability, topological changes, the absence of a hub node, scarce resources, and low bandwidth are only some of the issues that plague MANET. Due to their unpredictable motion, mobile nodes can enter or exit the network at any time. An adversarial node is now in the picture, draining resources from the network. This means that MANET is more likely to have an intruder enter their systems (Kumar *et al.*, 2017).

A particularly dangerous type of security breach in MANET is the wormhole attack. It can cause problems with more than one MANET routing protocol, such as AODV, OLSR, DSDV, and so on. At least two attacker nodes discover a wormhole attack through the use of a secret channel known as a tunnel. Once that triggers, data packets

will be gathered by the wormhole tunnel and sent onward. The main components of the wormhole detection algorithm are the Genetic Algorithm (GA), the Support Vector Machine (SVM) and Decision Tree (DT). The Genetic Algorithm technique for feature selection and the SVM (Support Vector Machine) and DT (Decision Tree) algorithms are used for classification.

2. **Wormhole Attack:** is a severe attack on the MANET routing protocol that occurs when two or more malicious nodes establish a tunnel in the network to transport packets between the tunnel's endpoints. An out-of-band channel, packet encapsulation, high-power transmission, packet relay, or protocol deviations are only some of the methods that can be used to establish a tunnel. Wormhole tunnel routes are favoured by authentic nodes over multi-hop routes due to their lower latency and fewer hops. In spite of their seeming proximity to their

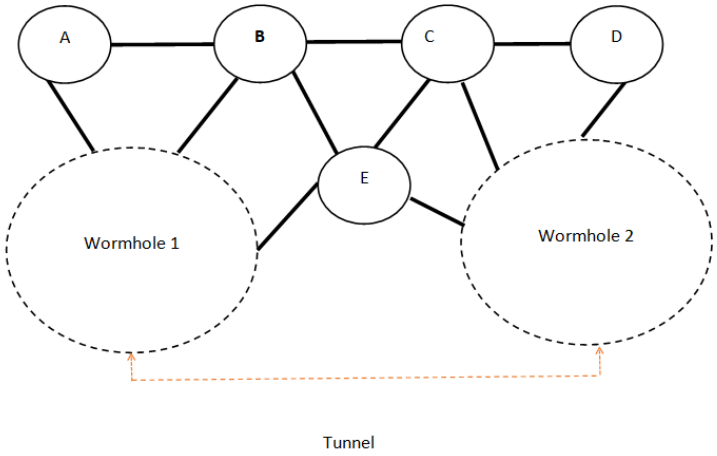

Figure 2: Wormhole Attack

targets, these malicious nodes are actually rather far away. Such an assault would inevitably produce a bogus path as shown in Fig 2..If a wormhole attack is started in the network, and the source node selects this fake route as the route with the fewest hops to the target, then the malicious nodes have the option of forwarding the packets to their intended destination or dropping them.

- **The objectives of this research are to**

(1) Learn about the existing techniques for detecting MANET wormhole attacks,
(2) Develop and Improved technique by using AI.
(3) Assess how well this new technique protects MANETs from wormhole attacks.

II. RELATED WORK

Hemanand *et al.* (2022) proposed a decentralized wireless network; Mobile Ad-hoc Networks are expanding rapidly. Because of factors like node, location, time, etc., it's susceptible to a variety of threats and attacks, including wormhole attacks, which can cause data loss, route failure, and data route diversion. Multiple methods had been proposed to

counteract the wormhole attack, but all of them had drawbacks, such as increased power consumption, sluggish packet delivery, and low throughput. Taking these issues into account, these create a Five Stage Security Analysis Model for detecting and avoiding the wormhole attack. The five-step model analyses data from the network, including the path taken by packets, the timing between hops, the number of hops, and the proximity of nodes. The suggested model does not require any middleware or specialized hardware, and it conserves resources by not having to perform wormhole detection on each and every node in the network. For the creation of the proposed model **FSSAM**, the software Network Simulator-2 is employed. Throughput, lag, energy, packet loss, end-to-end delay, and packet delivery ratio were measured to assess performance, and simulation results are validated. According to the results, the suggested model outperformed alternative methods in wormhole identification and prevention.

Park *et al.* (2022) proposed a "RTT based technique" that employs calculation (route repetition, route aggregation, and Round-Trip-Time (RTT)) to achieve detection. In order to receive information in the quickest possible way and to pinpoint the location of any malicious nodes responsible for creating a wormhole tunnel, those combinations are necessary. When the source transmits an RREQ, the redundancy routing process begins and attempts all possible routes to the destination. The number of hops has been recorded from source to the destination, along with all possible routes connecting these two nodes. The information packets could be dropped and the transmission could be misled if the attacker was attempting a wormhole attack. Many researchers had developed wormhole discovery calculations based on different approaches to detect and prevent attacks on the system.

Truong *et al.* (2022) explored “A Trust-based Approach” for Identifying and Avoiding Wormhole Attacks in MANET that was written by K. Singh, G. Singh, A. Aggarwal, *et al*. A different infrastructure is proposed as a way to stop wormhole attacks. This one would be able to tell when an attack is about to happen and take steps to stop it.MANET devices, which was used to construct nodes and devices, are categorised as Mobile nodes, Cluster Heads, and Monitoring workers. All things considered, these nodes care about sharing data.

Zulfiqar *et al.* (2022)presented indicators that can be used to spot a wormhole intrusion. The benefits and drawbacks of each of these characteristics were discussed at length. The limitations of IDSs were also analysed to see where they may lie. This study provides the groundwork for developing effective IDS for detecting wormhole attacks in MANETs. These findings suggest that, when trying to differentiate between wormhole attacks, it is best to use either a method that relies on route request (RREQ) or hop count. This plan to create an RREQ-based IDS for MANETs as part of future work.

Prasad *et al.* (2023) described that a mobile ad hoc network (MANET) is a temporary network that relies on mobile devices, and it is commonly used in situations where a permanent network would be difficult. There will be no difficulty in either setting it up or managing it. Unfortunately, a network that is always evolving is more vulnerable to routing attacks. There are many different kinds of intrusion detection methods available for protecting against vulnerabilities and hacks. These studies used numerous statistical indicators and performance measures to validate their techniques. The several existing works each make different claims or provide different justifications. Despite this, there is a lack of

clarity when attempting to compare the performances of these pieces. Differences in performance are possible even when using the same dataset due to differences in sample distribution, the amount of training samples, the number of labels, and so on. The paper detailed the network's implementation, data generation, sample labelling, feature extraction, a method for intrusion detection, and an evaluation model for performance and reliability. After analysing both the performance and hardware dependability of related approaches, the evaluation model uses a **fuzzy logic system**to compute the performance dependability of each. As one statistical performance increases, another performance deteriorates due to an unequal sample size, as shown by the result. In light of this, the proposed evaluation methodology contrasted the best outcomes.

III. PROPOSED METHODOLOGY

In this paper, a genetic algorithm is used for feature selection and DT, SVM for classification to detect wormhole attacks. The system's performance is tested on statistical metrics and compared to contemporary methods.

1. **Genetic Algorithm:** is employed to optimize the paths taken. Genetic algorithms are used in AI to solve problems by combining through a set of possibilities until they find the right one. The genetic algorithm is used to select features.In order to increase the detection accuracy of the model, select the features that have the most influence and get rid of the features that are unimportant. It is possible for features to contain information about the target variable. The nodes find the best answer by exploring the space used to model all of the outcomes in the nodes' environment.

2. **Support-Vector Machine:** a type of supervised machine learning that uses a certain type of learning computation to analyse data for purposes of classification and regression. The vast majority of the time, however, they are employed to solve issues of categorization. Compared to other AI computations, SVMs run in a slightly different way.

3. **Decision Tree:** DT is comparable to supervised machine learning algorithms that make use of arraysand then other rules to make the code more readable. DT is home to two distinct species of trees. One type of node is the leaf node, while another type is decision node. A prediction of a class or objective is made by DT on the basis of the judgment rules, and a training model is generated based on the results of training. The use of decision trees has various benefits, including increased transparency, reduced complexity, and more rigorous study of decision-making options. Decision trees are utilized to find solutions to a variety of issues pertaining to WSNs, such as connectivity, data aggregation, mobile devices, and others(Shu *et al.*, 2017).

4. **AODV Protocol:** Ad hoc on-Demand Distance Vector (AODV) is a reactive routing algorithm commonly used in wireless networking situations.The task of AODV is finding a route from source to destination which is performed collaboratively by all portable nodes. The actual transfer of information doesn't take place until after the path has been determined. The routing table in AODV is a technique that automatically updates itself for a particular time. This protocol can be utilised for both unicast and multicast routings simultaneously. AODV provides a unique technique to give routing information to the desired node. It makes use of route tables and sequence numbers that have been

predefined. Each packet makes use of this sequence number in order to locate the adjacent node. The utilization of timer-based states over the entirety of an AODV node is a distinctive quality that sets it apart.

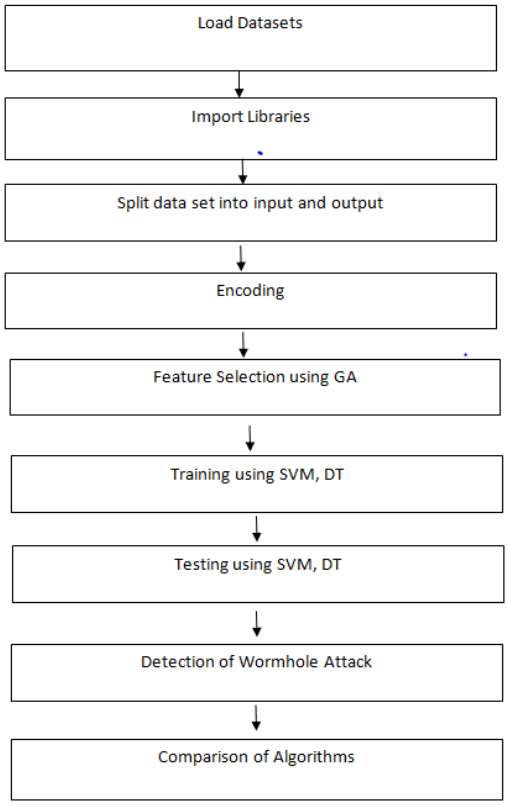

Figure 3: Proposed Methodology

An unlawful use of network resources by a node constitutes a wormhole attack, which is one of the most significant types of attacks that can have an effect on the performance of a MANET. This realization served as the impetus for the emphasis of this paper, which is the creation of a wormhole attack detection system for MANETs. The work for this paper is broken up into stages of completion as shown in Fig 3.

Preparing the dataset is the primary emphasis of the initial phase of the endeavor. In this phase, data is collected by conducting simulations utilizing the Ad-hoc on-demand distance vector (AODV) routing protocol. These simulations include both normal and malicious behavior of mobile nodes. Google Colabplatform was utilized in order to accomplish this. It is preferable to keep the dataset in the same directory as our Python code, as this makes it much simpler to read the file. Following the completion of the preprocessing and analysis of the raw data, the trace file is used to generate a total of 637862 dataset records, each of which has 20 features as shown in Table 1.

The development and testing of the suggested attack detection system is the focus of the second part of the study. The suggested system has been trained and assessed using supervised machine learning methods (Support Vector Machine and Decision Tree) in order to detect wormhole attack. We used 80% data for training and 20% for testing

purpose. The effectiveness of the system has been evaluated using statistical measures and compared.MANET security is crucial to prevent damage from assaults. Worm-hole attacks are known to degrade systems and hinder connections. AODV routing protocol finds the shortest path between two nodes when the path is needed.

5. Dataset Features:

Table 1: Dataset Features

S. No	Feature Name	Type
1	Duration	Continuous
2	Protocol	Discrete
3	Packet length	Continuous
4	Flag	Discrete
5	Message length	Continuous
6	hop count	Continuous
7	life time	Continuous
8	message type	Discrete
9	destination sequence number	Continuous
10	message sequence number	Continuous
11	Land	Discrete
12	Message transfer Mode	Discrete
13	number of neighbors	Continuous
14	highest flow	Continuous
15	average flow	Continuous
16	lowest flow	Continuous
17	average hop count	Continuous
18	number of failed connection	Continuous
19	failed connection rate	Continuous
20	Label	Discrete

IV. SIMULATED RESULTS

Based on the results of the study, it was determined that the suggested attack detection system using Decision Tree and Support Vector Machine algorithms had a detection rate of 99.97% and 98.19% respectively. Not only are the findings that were obtained for accuracy, precision, and F-score an essential indicator of the quality of dataset, but they also demonstrate that the proposed attack detection approach is successful.

Table 2: Simulation Profile

PARAMETER	VALUE
Number of Nodes	20
Protocol	AODV
Channel Type	Wireless Channel
Coverage Area	1000m * 1000m

1. **Comparison:** The SVM and DT algorithms were put to the test for comparison purposes, as was mentioned at the beginning of this paper. Scikit-learn were used to explore with DT and SVM-like algorithms in Python. The average performance metrics for DT algorithms withvarious numbers of selected features are shown in below table 3& Fig 4.

Table 3: Comparison of Classifiers performance

Metrics	SVM	Decision_Tree
Accuracy	0.981979	0.999945
Precision	0.989288	0.999934
Recall	0.938084	0.999835
F1_Score	0.963006	0.999884

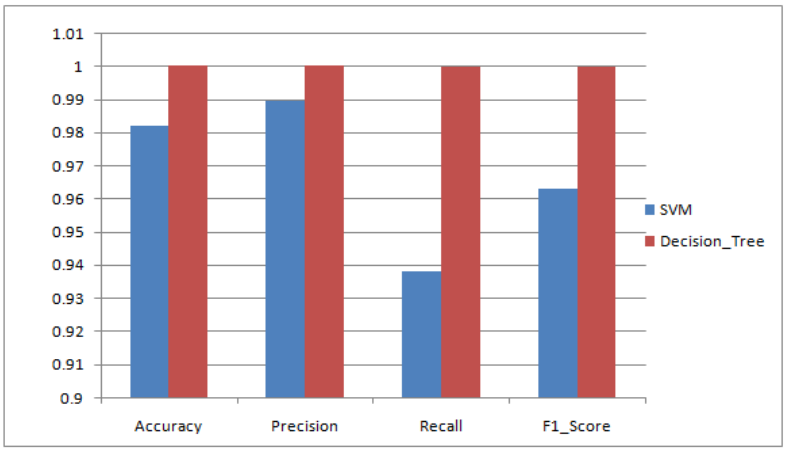

Figure 4: Performance Graph

- The accuracy of proposed Models has been shown in Fig 5

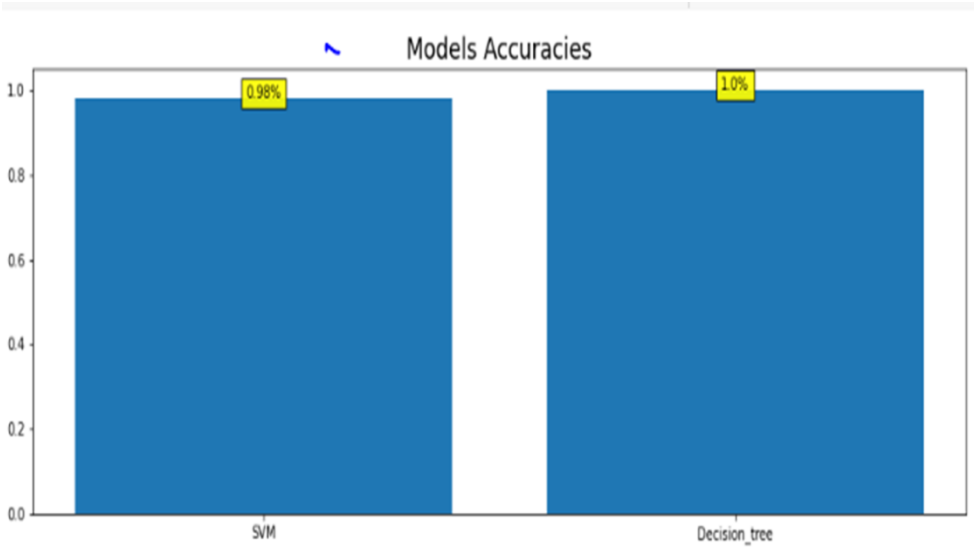

Figure 5: Accuracy Graph

V. CONCLUSION

The wormhole attack detection model that uses a machine learning method has been built for use in MANET while operating under AODV routing protocol for the purpose of this paper. As classes of a dataset, wormhole attacks, in addition to typical traffic, identified. In this research, the AODV routing protocol was successfully applied using the python language on Google Colab. Under a variety of circumstances, were run both with and without the presence of an attack. Following the completion of the dataset preparation, network features are extracted from the trace file. Both the Decision Tree classifier and the support vector machine classifier underwent training and testing. Important network properties that are employed for training and testing are successfully identified. The solution that is proposed provides an average detection rate that is 0.99% for Decision Tree classifiers and 0.98% for SVM classifiers respectively. This means that these classifiers also recorded comprehensive detection performance measures for individual classes. The DT and SVM classifiers are utilised for the purpose of comparison in order to evaluate the work that was proposed. According to the findings, the Decision Tree classifier is successful in achieving the best outcome. On the other hand, the performance metrics of SVM and DT were essentially comparable; nonetheless, the former performs superiorly to the latter. It is discovered that the data collection carried out during simulationshas contributed significantly to the enhancement of the detection model. As a result, the approach that is proposed is an effective method to detect the wormhole attack that is occurring in MANET.

The culmination of this effort demonstrates that the suggested strategy has good performance across a range of different types of attacks. However, more assaults may be launched either simultaneously or one after the other, depending on the strategy chosen. It would be beneficial to include network layer assaults like the Sybil attack and the rushed exploit in the dataset. These attacks would help improve the performance of the work that is being proposed. In the process of detection, additional machine learning techniques should also be taken into consideration. The work ought to be expanded not just to cover other levels of the MANET, but also for a variety of wireless networks such as WSN and VANET.

REFERENCES

[1] Chitkara, M. and M.W. Ahmad. 2014. Review on manet: characteristics, challenges, imperatives and routing protocols. International journal of computer science and mobile computing 3:432-437.
[2] Chitra, P. and T. Ranganayaki. 2020. A Study on Manet: Applications, Challenges and Issues. International Journal of Engineering Research & Technology (IJERT) 8:1-4.
[3] Hemanand, D., N.S. Ram and D. Jayalakshmi. 2022. FSSAM: A Five Stage Security Analysis Model for Detecting and Preventing Wormhole Attack in Mobile Ad-Hoc Networks Using Adaptive Atom Search Algorithm. Wireless Personal Communications:1-20.
[4] Kumar, S., M. Goyal, D. Goyal and R.C. Poonia. 2017. Routing protocols and security issues in MANET. In: 2017 international conference on infocom technologies and unmanned systems (trends and future directions)(ICTUS). p 818-824.
[5] Park, Y.J., H.-S. So, H. Hwang, D.S. Jeong, H.J. Lee, J. Lim, C.G. Kim and H.S. Shin. 2022. Synthesis of 1T WSe2 on an Oxygen-Containing Substrate Using a Single Precursor. ACS nano 16:11059-11065.
[6] Prasad, M., S. Tripathi and K. Dahal. 2023. An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks. Engineering Applications of Artificial Intelligence 119:105760.

[7] Shu, J., S. Liu, L. Liu, L. Zhan and G. Hu. 2017. Research on link quality estimation mechanism for wireless sensor networks based on support vector machine. Chinese Journal of Electronics 26:377-384.
[8] Sookhak, M., H. Tang, Y. He and F.R. Yu. 2018. Security and privacy of smart cities: a survey, research issues and challenges. IEEE Communications Surveys & Tutorials 21:1718-1743.
[9] Su, J. and H. Liu. 2011. Protecting flow design for DoS attack and defense at the MAC layer in mobile ad hoc network. In: International Conference on Applied Informatics and Communication. p 233-240.
[10] Truong, D.T., F.L. Trachtenberg, G.D. Pearson, A. Dionne, M.D. Elias, K. Friedman, K.H. Hayes, L. Mahony, B.W. McCrindle and M.E. Oster. 2022. The NHLBI Study on Long-terM OUtcomes after the Multisystem Inflammatory Syndrome In Children (MUSIC): Design and Objectives. American heart journal 243:43-53.
[11] Zulfiqar, B., M.A.S. Raza, M.F. Saleem, M.U. Aslam, R. Iqbal, F. Muhammad, J. Amin, M.A. Ibrahim and I.H. Khan. 2022. Biochar enhances wheat crop productivity by mitigating the effects of drought: Insights into physiological and antioxidant defense mechanisms. Plos one 17:e0267819.

