ISSN No:-2456-2165

Security threats Detection and Handling Mechanism in Wireless Sensor Networks using Machine Learning

Mohammad Farhaan, Shivanshu Singh, Shivendra Singh, Sakshi Malhotra, Dr Javed Miya
Department of Information Technology Engineering and Technology, Greater Noida, India

Abstract:- Wireless sensor networks (WSNs) have various capacity packages plus specific challenges. They commonly include masses of hundreds small sensor nodes that paintings autonomously. Conditions together with value, invisible deployment, and plenty of software domain names result in sensors with small length and restricted resources. WSNs are prone to many varieties of bodily assaults and maximum conventional community safety approaches are in operative on WSNs. because of the wireless and not unusual place quality of the verbal exchange path, suspicious broadcast, deployment in open environments, unsupervised nature and restricted resources. Security is consequently a crucial prerequisite for those networks. Though, we want to broaden the proper safety mechanism that takes into consideration the restrictions and necessities of WSN. In this document, we awareness at the Security hassle in WSN, Attacks in Wireless Sensor Networks, DOS Attack, Methods of Attack, Types of Attack ,How To Tackle with Hybrid Model Approach. This paintings allows us to discover the cause along with the competencies of the invaders. The aim, quit result, as well as effect of DO S assaults on WSNs also are presented. The article additionally deliberates famous techniques to safety detection towards DOS assaults. This might permit safety managers to greater efficiently manipulate WSNs' DOS assaults.

Keywords:- *Wireless Sensor Network (WSN), Security, Physical Attacks, WSN's structure, Security in WSN , Hybrid version Approach , Dataset Collection , SVM algorithm , KNN Algorithm , Naïve Bayes Algorithm , Random Forest Algorithm.*

I. INTRODUCTION

Innovations in wireless verbal exchange have facilitated the improvement of less-value, less-electricity wireless sensor networks (WSNs) .It has many capacity packages[1, 5] and specific challenges. As a rule, those are heterogeneous structures that incorporate many small gadgets, so-known as sensor nodes that cooperatively screen unique environments. I.e. Sensors collaborate with every different and collect their nearby statistics to obtain an international understanding of the surroundings; Sensor nodes also can paintings unconventionally. WSNs includes small sensor nodes set up in diverse geographical situations to accumulate the data approximately surroundings. The characteristic of sensor nodes is to bring together the statistics and ship amassed data to bottom level. These sensor nodes are deployed in an antagonistic and unguarded surroundings, wherein these nodes are continually in risk of safety assaults. WSN is greater vulnerable to safety breaks due its inherent nature, open surroundings and unattended antagonistic surroundings, restricted resources. Including all of the different traits, Security is the maximum essential hazard to the networks. The present safety strategies are impracticable because of the boundaries such as reminiscence, strength as well as get admission to nodes afterward deployment.

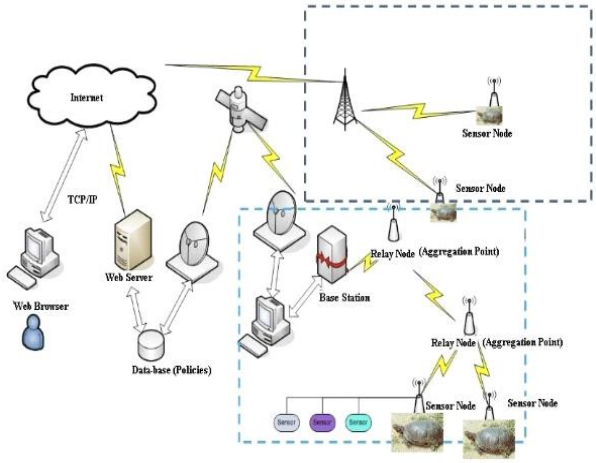


Fig. 1: WSN's architecture

II. OVERVIEW OF WSN

Here in, we gift and define of various dimensions of WSNs, together with definition, traits, packages, constraints and challenges.

A. Definition and suppositions of WSNs

The WSN various gadget includes batches or hundreds of low-cost and occasional low-power sensors for tracking and collecting data from real-time posted [6, 7, 8]. Common features of WSNs include streaming and multicast, routing, forwarding and retention courses. The sensor supplements are: sensor unit, processing unit, storage / recall unit, power supply unit and wireless radio transceiver; those devices speak to all the different things, as proved in the following illustration. Current additions to WSN structures that contain sensor nodes (motes or location gadgets that are statistical) community manager, security manager, integrated objects, base level (get gate access) and user

ISSN No:-2456-2165

interface. In addition, there are WSN-related fashion exchange methods that include WSN sequencing as opposed to distribution [6] and corresponding WSN in contrast to heterogeneous [6]. The most vulnerable area for networks is:

- Unsafe radio links [8, 9, 10],
- Package injection and re-play [8, 9],
- Resistant insecurity [10],
- Multiple sensor nodes (overcrowding) and occasional malicious nodes
- The ruling invaders (in the laptop-class) [10, 20].

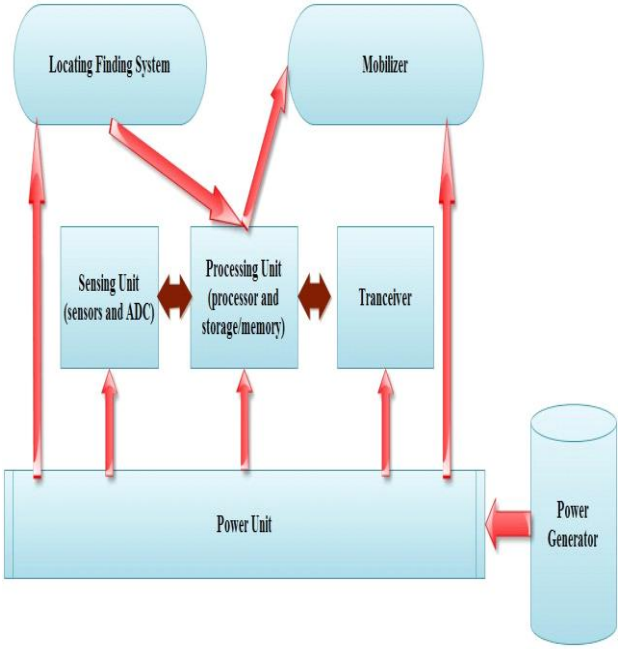


Fig. 2: WSN's routine architecture

B. WSNs traits and weak point

Utmost essential traits of WSNs are consisting of:

- Persistentor cellular sensors (mobility),
- Sensor restricted resources[4,18](radio verbal exchange, strength and processing[4]),
- Less dependability, wireless verbal exchange and exception [4],
- Unpredictable WSN's topology and sociality.[4,21] ,
- Un-important controlling, independently and structure-less[8],
- antagonistic-surroundings wildlife [8,10] and excessive concentration.

C. WSN's applications

In total, there are two phases of WSN collective applications, monitoring and tracking; therefore, a few daily applications of these networks are: military, medical, environmental management [2, 6, and 8], industry, infrastructure security [2, 8], disaster risk exposure and development, agriculture, intelligence structures, law enforcement, transportation and new facilities (as in figure3).

Fig. 3: WSN's applications

III. SECURITY INWSNS

These days, WSN entry strategies have grown; in addition it introduces many strategies to disrupt those networks. In this case, statistical accuracy and social stability are mandatory; because those networks are often used in private and sensitive environments. 3 key WSN security features, which include gadget (integrity, availability), source (verification, authorization) and statistics (integrity, privacy).

Fig. 4: Security in WSN

A. Security Challenges in WSN

WSNs are greater prone to safety assaults because it is open surroundings. Certain troubles concerned in safety are indexed down [31]:

a) Limited Hardware:
The sensor nodes are very small and within the current features there is a need to enhance the life of the nodes by reducing the bandwidth used, recall etc. Because of these limited resources, setting up security between those nodes is a very difficult task.

b) Wireless Communication :
The verbal exchange method is very expensive and is extremely vulnerable to threats such as earwax, placing vicious nodes in public, floods etc. Due to the wireless connector, we cannot select complex contracts that require more big data or messages.

ISSN No:-2456-2165

c) Hostile Environment:
Since sensor nodes are installed in unattended environments, hackers can get into access to nodes and extract content. Nodes do not resist resistance because of their growing value which provides a clean way for the attacker to be accepted into the nodes.

d) Aggregation Processing :
Sensors nodes typically receive data from every sensor and change the destination data. The life of sensory nodes can be duplicated by minimizing verbal exchanges between locations. But this cannot be done because sensors nodes need to speak to perform statistical analysis of sensory areas.

e) Large Scale Deployment :
Sensor networks use 100s with large quantities of sensors in packages. Increment is therefore an important factor to consider within the terminal network.

B. Security issues

This section sets out the most important discussions on WSN:

- Key innovation,
- Security, Proof of authenticity,
- Privacy, intensity of the DoS attack,
- Safe tracking, capturing of locations

IV. ATTACKS IN WSN

A. DOS Attack

DoS (Denial of Service) attack targets at blocking, for legitimate users, unapproved access to a system resource or the holding of system operations and functions. The unexpected result of this attack is congestion and starvation problem an attempt to make a computer resource inaccessible to its intended users. Predictably the focus are high profile web servers where the invader is aiming to affect the hosted web pages to be unavailable on the Internet.

B. Types of DOS Attack

a) Jamming Attack:
It is caused by stopping the radio frequency of attackers nodes with opposite positions. Attacks are carried out by means of radio transmissions. It is mainly due to the fact that the Rejection of attackers providers and all nodes do not speak due to jamming attacks and especially from the jammer.

b) Collision Attack:
In this attack, each time a legitimate connection passes the records, the attacker hears the transfer and transmits a private signal to create obstacles. Even a single byte argument can reveal errors and damage the whole message. The impact of a collision is higher than a collision with the ability to penetrate electricity and space. It aims to end the channel of exchange of words and socialization Institutions.

c) Sinkhole Attack:
In this attack, the attacker's main objective is to capture the action. This collaborative node can focus on the delays of the floodplains and tries to introduce a simplified course of regenerating nodes in a shorter way.

d) Sybil Attack:
The attacker has caught more than one and has gaps and is found in more than one location. It focuses on error-tolerant structures such as retention, social topology, duplicate route, recording recordings, voting, discovery of misconduct and actual resource allocation, etc.

e) Wormhole Attack:
These beatings need to happen in the worst and worst places. They set up a wormhole link between the wrong places. Thereafter, packets found in one public area are transferred to the public domain.

f) Hello flood Attack:
It is a beacon that is often sent in the form of brand new methods to the opposite nerve nodes that announce a brand new course. It makes use of HELLO messages as a tool to do this job. Here, the invasive transmitter transmits HELLO messages to sensory structures that may be in a large freed region and the nodes are encouraged that the attacker is a neighbor and begin to transmit records. The message was skipped from the attacker and the attacker displayed the message before streaming the record to In this assault, the invader will commonly have right sign power [33].

Layer	Attacks	Security Approach Defenses
Physical layer	Jamming Tampering	*Lower duty cycle, Priority messages, Spread-spectrum techniques *Tamper proofing, Hiding
Data Link layer	Collision Exhaustion Unfairness	*Error-correcting code *Rate limitation *Small frames
Network layer	Sink hole Sybil Worm hole Hello floods	*Monitoring, Redundancy, Authentication *Probing, Authentication * Authentication, Packet leashes by using geographic and temporal information *Verify the bidirectional link, Authentication
Transport layer	Flooding Desynchronization	* Client puzzles *Authentication
Application layer	Attacks on reliability	Unique pair wise keys and cryptographic approach.

Fig. 5: Attacks in each layer

C. HOW TO DETECT?

- The version used should be easy and rapid sufficient to locate the safety danger in WSN.
- Lack of information garage and strength sensor networks are the barriers to the implementation of conventional pc protection strategies in a WSN.
- HYBRID MODEL Approach: growing Classifiers in Machine Learning set of rules for detection of Threats.

V. MODEL APPROACH

A. Methodology

To triumph over these kind of shortcomings, device gaining knowledge of technique is preferred. In proposed system, we've got taken one dataset which has 28 functions together with supply deal with, vacation spot deal with, packet identification etc. classifying the values primarily based totally on functions together with supply and vacation spot deal with the use of device gaining knowledge of strategies which incorporates SVM, KNN and Naive Bayes to locate the DistributedDoS assault and calculating the version accuracies of the same. In order to calculate worst case possible, we've got used the subsequent traits: signed kernel for SVC, 5n_neighbors for KNN and default for Naive Bayes.

B. Hybrid Model Approach

In this project, designed a hybrid version set of rules which encompass hybrid set of rules which encompass a mixture of numerous device gaining knowledge of strategies to teach a version which may be used to locate and classify the sorts of DOS assault with extra accuracy than that if every character device gaining knowledge of strategies used withinside the hybrid version. Figure Hybrid version Approach The hybrid version will offer extra stage of accuracy prediction of the DOS Attack .Also, is extra powerful than the alternative fashions individually.

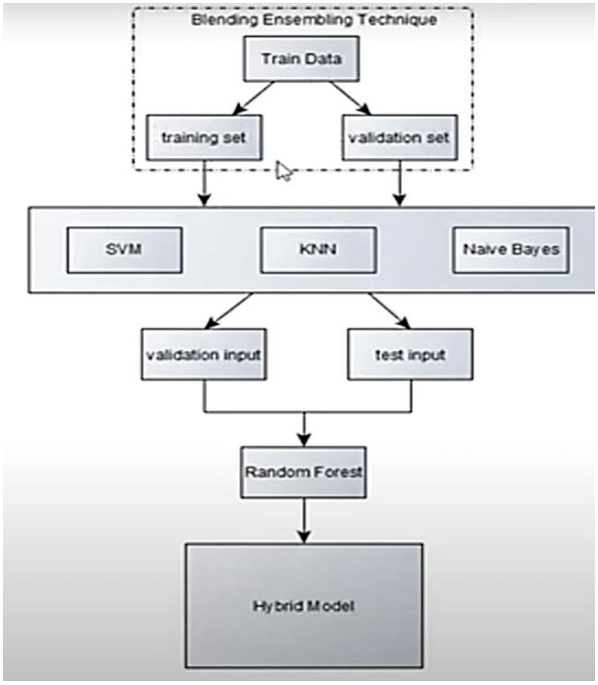


Fig. 6: Hybrid model Approach

C. ALGORITHM PROPOSED

- First the corresponding Dataset is break up into Train Data (80%) and Test Data (20%).
- After that Train Data once more break up into Training set (80% of Train Data) and Validation set (20% of Train Data).
- Later dividing them, we ship the validation set as an enter to the 3 one of a kind set of rules(SVM, KNN, Naive Bayes) to yield predictions from the corresponding algorithms .
- Individual version offer prediction units namely, validation prediction units and take a look at prediction units.
- Hence, every validation prediction set shape the three fashions are concatenated into validation enter.
- Likewise, every take a look at prediction set from the 3 fashions are concatenated into take a look at enter.
- Finally, the newly acquired Data i.e. validation enter, can be skilled with Random wooded area method to create the Hybrid Model.
- This version is used to make very last prediction at the take a look at enter to get the very last prediction output which in flip as compared with the real take a look at information and the accuracy is been calculated.

a) DATASET COLLECTION

A new dataset changed into accrued on this paintings due to the fact there may be no current information units that incorporate a contemporary-day DDoS assault including (SIDDOS, HTTP Flood), and furthermore, different to be had information units may also encompass a super transaction of replica and surplus records, and which can bring about an last unrealistic outcome. Our accrued dataset consists of 4 sorts of DDoS assault as listed: (HTTP Flood, SIDDOS, UDP Flood, and Smurf) without similar and replica entries [34].

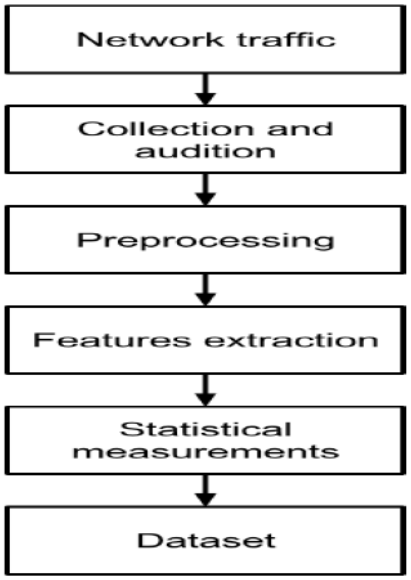


Fig. 7: Dataset Collection

ISSN No:-2456-2165

b) Blending
Blending Ensemble Technique-In this method,
- Respective Data is break up into Train Data (80%) and Test Data (20%).
- Then the Train Data once more break up into Training set (80% of Train Data) and Validation set (20% of Train Data).

c) SUPPORT VECTOR MACHINE ALGORITHM
- Supervised learning algorithm.
- Used for classification.
- Goal is to create decision boundary that can segregate n-dimensional space into classes.

- **Objective:**
  To achieve a hyperplane in an N-dimensional space (N — the number of features) that specifically classifies the data points.

- **Important Tuning Parameters for Support Vector Classifier:**
  Class weight - Weights related with classes in the form of class label: Weight. If not specified, all classes are hypothetical to have weight one.

  Degree - Degree is a constraint used once kernel is set to poly. It's usually the degree of polynomial practice to get the hyperplane to fragment the data.

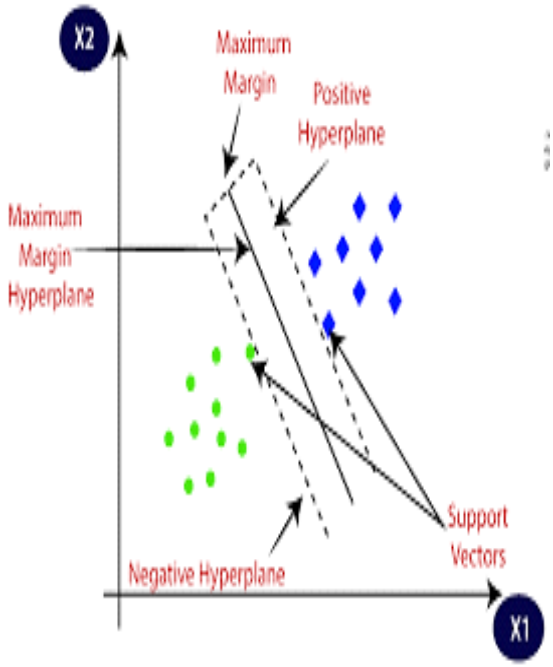


Fig. 8: SVM algorithm

- Gamma - kernel coefficient for ruff, ploy and sigmoid to handle non-linear classification
- Kernel - This choose the kind of hyperplane used to divide the data.
- Toll- tolerance for stopping criterion.

d) KNN(k-nearest-neighbor)
- K-Nearest Neighbor is a supervised machine Learning algorithm.
- It is a nonparametric method.

Phases to be performed during the K-NN algorithm are As given below:
- Split the data in training data and test data.
- Select a value K.
- Define which distance function is to be used.
- Select a sample from the test data that requires to be categorized and calculate the distance to its N training trials.
- Arrange the distances acquired and take the k-nearest data samples.
- All other test class to the class based on the majority vote of its k neighbors'.

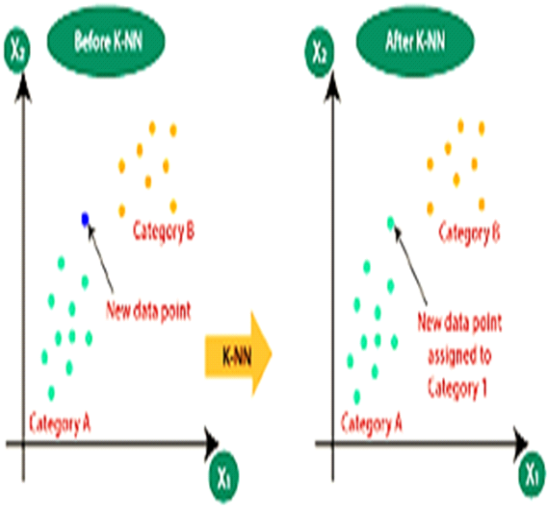


Fig. 9: KNN Algorithm

e) Naive Bayes
This algorithm is a supervised learning algorithm, based on Bayes theorem and used for answering classification challenges. It is primarily used in text classification that containsa high-dimensional training dataset. Modest and supreme successful Classification algorithms. It is a probabilistic classifier, which result inpredictions on the basis of the probability of an object.

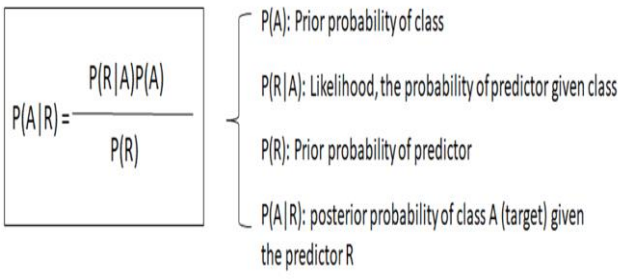


Fig. 10: Naïve Bayes Algorithm

ISSN No:-2456-2165

f) Random Forest Algorithm
Random forest Algorithm is a bagging method with trees as weak learners. Each tree is fitted on a bootstrap sample taking only a subset of variables unsystematically chosen.

Important Tuning Parameters for Random Forest:

Criterion - measure for quality of a split.

- **max_depth** - The extremedepth of the tree.
- **max_leaf_nodes** - Number of features to consider when looking for the best split.
- **min_samples_leaf** - The minimum number of samples required to be a leaf node. This may have effect of smoothing the model.
- **min_sample_split** - The minimum number of samples required to split an
- Internal node.
- **n_estimators** - The number of trees in the forest.
- **max_features** - Number of features to contemplate when observingfor the best Split.

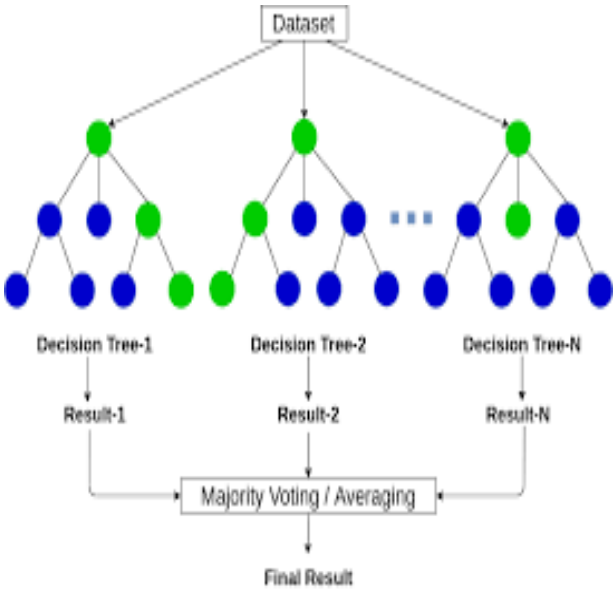
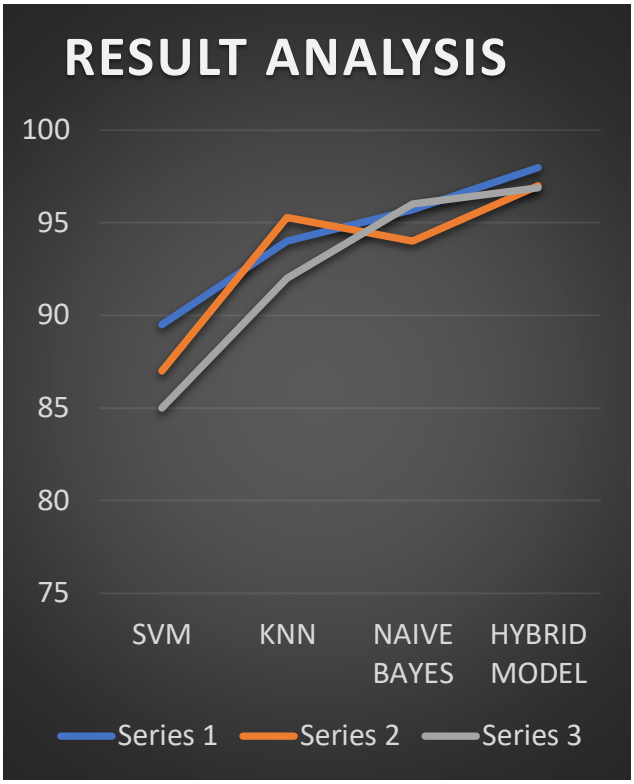


Fig. 11: Random Forest Algorithm

VI. CONCLUSION

Security is a critical prerequisite and complicated feature for the supply and growth of WSNs in one of a kind utility domains. Most bodily protection assaults goal WSN protection dimensions including integrity, confidentiality, authenticity, and availability. In this article, we examine diverse aspect of WSN protection, gift and classify a whole lot of WSN bodily assaults. Our technique to classifying the DOS assaults of the WSN is primarily based totally on diverse extracted functions of the bodily layer of the WSN, the traits of assaults and attackers, including the danger version of WSNs, the sort of DOS assaults, the desires and results, their techniques and Impact and sooner or later the related detection and protection strategies in opposition to those assaults on the way to manage them independently and comprehensively.



Algorithm	Series 1	Series 2	Series 3
SVM	89.5	87	85
KNN	94	95.3	92
Naïve Bayes	95.7	94	96
Hybrid Model	97.98	97	96.89

Fig. 12: Comparison between algorithms

As proven with inside the Figure collection 1 suggests the primary collection trying out of every version and calculating their respective accuracies. As we will see that the Hybrid version presents higher accuracy than that of every character version.Series2 and Series three suggests the second one and 1/3 collection trying out of every version respectively. For each collection examined above, we will see that we get higher accuracy with the Hybrid version than whilst as compared to that of different fashions.

REFERENCES

[1.] W. Zaidi, M. Minier and J. P. Babau; An Ontology for Attacks in Wireless Sensor Networks; INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA); Oct 2008.
[2.] K. Sharma and M. K. Ghose; Wireless Sensor Networks: An Overview on its Security Threats; IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs; CSE Department, SMIT, Sikkim, India; 2010.
[3.] K. Xing, S. Sundhar, R. Srinivasan, M. Rivera, J. Li and X. Cheng; Attacks and Countermeasures in Sensor Networks: A Survey; Computer Science Department, George Washington University; Springer, Network Security; 2005.
[4.] T. A. Zia; A Security Framework for Wireless Sensor Networks; Doctor of Philosophy Thesis; The School of Information Technologies, University of Sydney; Feb 2008.
[5.] M. Saxena; Security in Wireless Sensor Networks: A Layer-based Classification; Department of Computer Science, Purdue University.
[6.] Z. Li and G. Gong; A Survey on Security in Wireless Sensor Networks; Department of Electrical and Computer Engineering, University of Waterloo, Canada.
[7.] Dimitrievski, V. Pejovska and D. Davcev; Security Issues and Approaches in WSN; Department of computer science, Faculty of Electrical Engineering and Information Technology; Skopje, Republic of Macedonia.
[8.] J. Yick, B. Mukherjee and D. Ghosal; Wireless Sensor Network Survey; Elsevier's Computer Networks Journal 52 (2292-2330); Department of Computer Science, University of California; 2008.
[9.] padmavathi and D. Shanmugapriya; A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks; International Journal of Computer Science and Information Security (IJCSIS), vol. 4, No. 1& 2; Department of Computer Science, Avinashilingam University for Women, Coimbatore, India; 2009.
[10.] C. Karlof and D. Wagner; Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures; Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols; In First IEEE International Workshop on Sensor Network Protocols and Applications; University of California at Berkeley, Berkeley, USA; 2003.
[11.] Perrig, R. Szewczyk, V. Wen, D. culler and D. Tygar; SPINS: Security Protocols for Sensor Networks; Wireless Networking ACM CCS; 2003.
[12.] E. Shi and A. Perrig; Designing secure sensor networks; Wireless Communication Magazine; 2004.
[13.] Perrig, J. Stankovic and D. Wagner; Security in Wireless Sensor Networks; In Communications of the ACM Vol. 47, No. 6, 2004.
[14.] W. Xu, K. Ma, W. Trappe and Y. Zhang; Jamming Sensor Networks: Attack and Defense Strategies; IEEE Network; 2006.
[15.] Becher, Z. Benenson and M. Dornseif; Tampering with Motes: Real-World Attacks on Wireless Sensor Networks; RWTH Aachen University; 2006.
[16.] J. Deng, R. Han and S. Mishra; Defending against Path-based DoS Attacks in Wireless Sensor Networks; in SASN '05: Proc. 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks; 2005.
[17.] Kraub, M. Schneider and C. Eckert; Defending against False Endorsement-based DoS Attacks in Wireless Sensor Networks; in WiSec: Proc. 1st ACM Conference on Wireless Network Security; 2008.
[18.] Kraub, M. Schneider and C. Eckert; An Enhanced Scheme to Defend against False- Endorsement-Based DoS Attacks in WSNs; in IEEE International Conference on Wireless & Mobile Computing; Networking & Communication; 2008.
[19.] Y. Zhou, Y. Fang and Y. Zhang; Security Wireless Sensor Networks: A Survey; IEEE Communication Surveys; 2008.
[20.] Y. Wang, G. Attebury and B. Ramamurthy; A Survey of Security Issues in Wireless Sensor Networks; IEEE Communication Surveys; 2006.
[21.] R. H. Khokhar, M. A. Ngadi and S. Mandala; A Review of Current Routing Attacks in Mobile Ad Hoc Networks; Faculty of Computer Science and Information System, Department of Computer System & Communication, University Technology Malaysia (UTM); Malaysia.
[22.] T. Kavitha and D. Sridharan; Security Vulnerabilities in Wireless Sensor Networks: A Survey; Journal of Information Assurance and Security; 2009.
[23.] Wood and J. Stankovic; Denial of Service in Sensor Networks; IEEE Computer Mag.; 2002.
[24.] Distributed Denial of Service Attack, Detection using Naïve Bayes and K-Nearest, Neighbor for Network Forensics Amit V Kachavimath[1], Shubhangeni Vijay Nazare[2] and Sheetal S Akki[3],[1] Assistant Professor,[2][3] Student, Master of Computer Applications, KLE Technological University, Hubli,Karnataka,India. Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020)IEEE Xplore Part Number: CFP20K58-ART; ISBN: 978-1-7281-4167-1.
[25.] A DDoS Attack Detection Method Based on Hybrid, HeterogeneousMulticlassifier Ensemble Learning
[26.] Bin Jia,1 Xiaohong Huang,1 Rujun Liu,2 and Yan Ma1, Information and Network Center, Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China. Received 22 October 2016; Accepted 11 January 2017; Published 15 March 2017.
[27.] Distributed denial of service attack detection using Naive Bayes Classifier through Info Gain Feature Selection Conference Paper · August 2016.
[28.] Intrusion detection based on K-Means clustering and Naïve Bayes classification, Conference Paper · July 2011.
[29.] Frequency Based DDoS Attack Detection Approach Using Naive Bayes Classification, Conference Paper · June 2016.

[30.] SSVM : A Simple SVM Algorithm ,S.V.N. Vishwanathan, M. Narasimha Murty {vishy, mnm}@csa.iisc.ernet.in Dept. of Comp. Sci. and Automation, Indian Institute of Science, Bangalore 560 012,
[31.] Y. Zhou, Y. Fang, and Y. Zhang, Securing Wireless Sensor Networks: A Survey, IEEE Communications Survey,vol. 10, no. 3, pp. 6-28, 2008.
[32.] Padmavath, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.
[33.] Sahabul Alam `and Debashis De Department of Computer Science and Engineering, West Bengal University of Technology, Kolkata, India, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 6, No. 2, April 2014
[34.] Mouhammd Alkasassbeh IT Department, Mutah University, Karak, Jordan Detecting Distributed Denial of Service Attacks Using Data Mining Techniques, *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 20.*