Covert Channel detection in Wireless Sensor Network

Dr. N. Penchalaiah, Department of Computer Science and Engineering, Annamacharya Institute of Technology and Sciences (Autonomous), Rajampet, Andhra Pradesh, India-516126.

N. Lakshmi Durga, G. Sruthi, N. Hari Prathap, B. Jaswanth Reddy, Department of Computer Science and Engineering, Annamacharya Institute of Technology and Sciences (Autonomous), Rajampet, Andhra Pradesh, India-516126.

ABSTRACT:

Since computer networks and modern communications have advanced, it is now simpler, quicker, undetectable, and more secure to establish covert connections than it was in the past. A system security protocol can be violated to allow the release of encrypting messages over a channel. Among the most challenging aspects is still identifying such dangerous, invisible, and camouflaged risks. Traditional Security procedures are not able to identify this hazard since it uses ways that are not intended to be used for communication. An introduction to covert operations was given in this review. definitions, varieties, and developments in channels, with a focus on machine learning testing methods computer learning techniques. It offers a thorough analysis of the most common hidden channels, along with an analysis of the ML techniques employed to counter them and an analysis of their successes as well as restrictions. Moreover, this work provides experiment that compares analysis of many widely utilised ML techniques in this field. This led to evaluation and reporting of these classifiers' performance. The report's findings include that absolutely nothing is safe, our info is still in danger, and more work on finding secret passageways is required. This project's main objective is to determine whether or not a covert channel in the network is normal. To do this, we have employed the classification techniques Random Forest, Decision Tree, Naive Bayes, ANN, and Support Vector Machines.

KEYWORDS: Machine learning. **,** Support Vector Machines, ANN, Random Forest, Decision tree and Naive Bayes.

INTRODUCTION:

A way of establishing communication between two parties in order to leak information discreetly is known as a covert channel. The organization's established security policies are broken by this communication. The development of clandestine channels across computer networks was later made possible by grilling, which expanded this idea to computer network platforms. There are now various situations that are complex enough to be of hidden channels discovered thanks to the enhanced development of computer network techniques, creating many difficulties for those trying to establish clandestine communication. A variety of malevolent acts have been made easier through network-covert channels. A covert channel differs from more established secret message transfer techniques in that it hides both the content and the route of the transmission. Network-covert channels are used to protect the transmission of private messages, in particular, have two things in mind. Security of communication links and material is one of these features. The security of these aspects is significantly enhanced by network hidden channels. Techniques by using covert channels are increasing everyday as a result of the influence of modern communication technology. These key elements for creating covert channel approaches are outlined in. Among these elements are recent advancements in internal control protocol technology, switching techniques, and network and communication technologies. This section offers a succinct overview of attacks on covert channel demonstrate the threat that quickly materialise into significant issues that require attention.

An explanation of the numerous covert channel types is given in the section that follows, with a focus on the two main categories of covert methods. The widespread application of covert channel strategies in cutting-edge technologies, such as the Internet of Things (IoT), the IPv6 protocol, and VoLTE technological advances, is then covered in Section III. It explains how covert channel assaults can employ these technologies and techniques to their advantage and provides a flexible framework for creating different covert channels of distribution that pose a variety of security challenges. The heart of our work

is Section IV, which provides an in-depth the covert channel's review identification utilising machine learning (ML) techniques.

In the subject of information systems, as well as in the field of computer science in general, ML classification models have shown their aptitude and effectiveness. To present the most up-to-date knowledge in this field, this section thoroughly examines the successes and limitations of these strategies with a special emphasis on recent research. After that, in Section V, eight classification models are the subject of an experimental comparison study to show how well they perform in terms of precision and error. The creation of a covert channel based on packet length that uses network packet length to transmit hidden messages resulted in the creation of a dataset.

LITERATURE SURVEY

D. Frolova, A. Epishkina, and K. Kogos,‘‘ Regulating traffic to safeguard clandestine channels,’’

Cloud system security and privacy are sophisticatedly threatened by covert network routes. Existing defences all share the same constraint of having a performance cost. Their actual application in high-speed networks is severely hampered by this. We create a rough design for NetWarden, a cutting-edge defence whose main objective is to protect TCP performance while minimising covert channels. NetWarden is able to modify protections that were previously only applied as proof-of-concept and apply changes at line speed thanks to the usage of programmable data planes.

In addition, with the aim of eventually neutralising the performance impact of channel mitigation, Net Warden uses a variety of performance-improving strategies to momentarily improve the speed of connections that are affected. According to our simulation, NetWarden can block several covert channels with little performance hit. The design and implementation of a complete system are ongoing projects that we are now working on.

L. Caviglione, ‘‘Network hidden channels trends and obstacles, and solutions,’’

This study examines patterns and difficulties in creating defences against the most often used network covert channels. In order to achieve this, we evaluated the pertinent literature while taking into account strategies that can be successfully used to identify threats or generic injection mechanisms that are seen in the wild. The focus has been on illuminating paths that should be taken into account while developing mitigation strategies or organising research to counter the rising tide of malware with information-hiding capabilities. The findings show that many works are very specialised, and that high-level and generic techniques may be advantageous in developing a successful strategy for reducing security concerns brought on by network hidden channels. Additionally, mechanisms to prevent the exploitation of anomalies should be taken into consideration early on in the development phases of both protocols and services.

J. Van Bulck, S. Vanderhallen, J. T. Mühlberg, and F. Piessens, ‘‘Using hidden channels for secure authentication in automobile control networks,’’

In this research, we investigate the development and implementation of vehicular data encryption algorithms as a resource-efficient, transparent approach to automotive network security. These are acceptable and beneficial uses. The first thorough analysis of covert channels within area networks is provided by us in terms of feasible wireless data and Controller Area Networks (CAN). Our research indicates that timing-based covert channels are possibilities to be employed in the development of a complementing nonce synchronizing channel that can increase the message loss resistance of current authentication approaches. On top of an open-source authentication process CAN communication library, we practically implement and test this design to demonstrate how covert time channels can improve communication robustness under common conditions while maintaining the security guarantees of the core authentication elements under attack.

S. Wu, Y. Chen, H. Tian, and C. Sun, ‘‘Detection of covert timing channel based on time series symbolization,’’ IEEE Open J. Commun. Soc., vol. 2, pp. 2372–2382, 2021.

This research proposes a new time series symbolization-based CTCs detection technique. The sampled IATs are first transformed into symbolic time series, and each discrete value is viewed as a status. The status transition probability matrix is then calculated by counting the times each state has transitioned (STPM). By computing the similarity score, it distinguishes the label (overt or covert) of the sampled IATs. According to experimental findings on detection accuracy, our method performs better than traditional ones in a perfect network environment, with an average accuracy of roughly 96%. In addition, our technique performs better even when there is network interruption.

L. Caviglione, M. Zuppelli, W. Mazurczyk, A. Schaffhauser, and M. Repetto, ‘‘Code augmentation for detecting covert channels targeting the IPv6 flow label,’’ in Proc. IEEE 7th Int. Conf. Netw. Softwarization (NetSoft), Jun. 2021, pp. 450–456

The IPv6 Flow Label is a target of covert channels, which can be found using the expanded Berkeley Packet Filter, which is demonstrated in this paper as a way to use code augmentation features. The proposed method has been examined in comparison to Internet-wide traffic traces that have been naturally obtained to demonstrate its efficacy. Results show that certainly, you can detect while the channel reducing the computational and memory footprint load (The processed traffic, for instance, only experiences a small amount of additional delay).

METHODOLOGY:

1.Classification of Decision Tree:

A part of the supervised machine learning algorithm family is the decision tree algorithm. The decision tree method can be used to resolve classification and regression problems, unlike the other supervised learning methods. By studying previously recorded information, a decision tree is developing a model for training that predicts the category or the specified attribute's value (data for training). Using decision trees, determine the class label for a record, we start at the tree's base. We compare what the root attribute's values are with the attribute of record. Based on comparison, we follow the branch corresponding to that value and proceed to the next node.

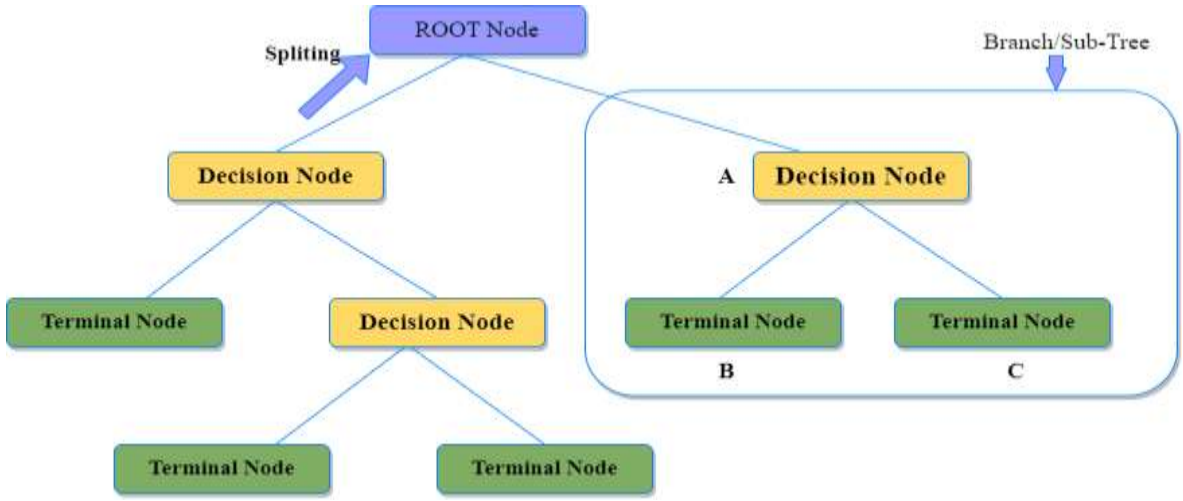


Fig.1: Classification of Decision Tree

2.Classification of Random Forest:

The supervised learning strategy uses a well machine learning algorithm Random Forest. Both regression and classification problems in machine learning may benefit from its use. It is based on the idea of

ensemble learning, a technique that includes combining a number of classifiers to address the model's efficiency by solving a difficult problem. "Random Forest is a classifier that comprises a number of decision trees on various subsets of the provided dataset and takes the average to enhance the predicted accuracy of that dataset," like name suggests. Instead of depending on just one decision tree, the random forest collects the projections from every decision tree and determines the final outcome primarily on the forecasts that received the most votes.

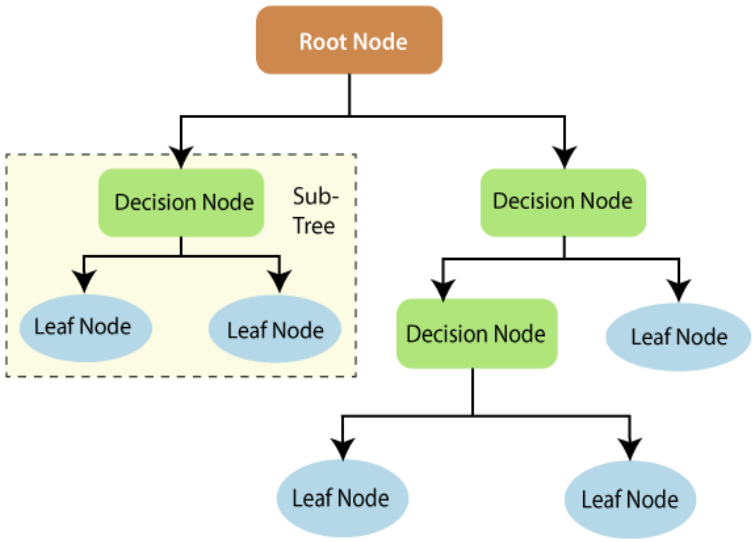


Fig:2: Classification of Random Forest

3. Networks of Neural:

Artificial neural networks (ANNs), which are a type of computing system, are designed to imitate how the biological neural assesses and processes information. It is the basis of artificial intelligence (AI) and provides solutions to problems that would be intractable or difficult by quantitative or human standards. ANNs can produce better results as more data is collected because they are self-learning is available. A neural network (ANN) is made up of many processing units, also known as artificial neurons, that are connected by nodes. Units for input and output make up these processing units. In order to create one output report, the inputs units, which collect information from the input units, the neural network attempts to learn about various types of data on an internal analysis ranking system. Backpropagation, also known as a bundle of understanding the concepts known as backward propagation of error guidelines that artificial neural networks (ANNs) employ similar to how individuals require rules and guidelines in order to achieve an effort or outcome, to improve their results.

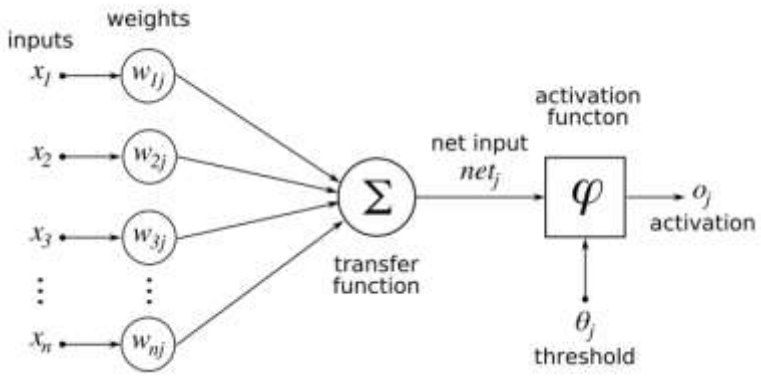
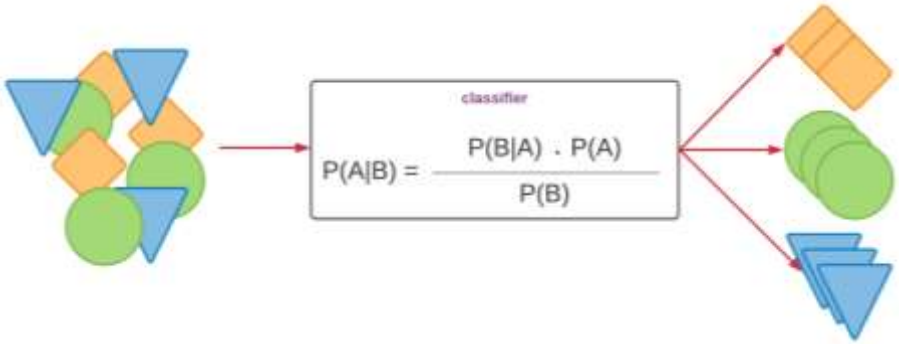


Fig: 3: Neural Network's

4. Naive Bayes Classifier:

Naive Bayes classifiers are a subset of categorization algorithms based on the Bayes Theorem. It is a set of algorithms, not an unique algorithm, that is all guided by a common core principle: that each combination of qualities becoming categorised is distinct of the others.Let us think about a dataset to get things started.

Fig:4: Naive Bayes Classifier



Results of Implementation:

Utilizing our enhanced dataset, eight classifications models were designed and validated, which is shown in preceding section. These models include stack (use several classifiers), neural network, nave bayes, logistic regression, random forest, SVM, decision tree, and KNN. To achieve accurate and reliable results, strategies for stochastic testing were used per test 20 times. With the use of two distinct sets of testing data, each classifier was developed and evaluated. Each model's classification performance, recall, and precision were determined using equations 1, 2, and 3, respectively. For each classification model, a confusion matrix (error matrix) was also created, which illustrates the FP and FN classification mistakes as a measure of categorization performance.

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

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

$$\text{Precision} = \frac{TP}{(TP + FP)} \quad (3)$$

TABLE 1. Performance of Classifiers:70% training: 30% testing.

Classifier	Indicators of performance		
	Training Volume:80% Testing Volume:20%		
	Recall	Precision	Accuracy
Decision Tree (DT)	99.8%	99.8%	99.8%
Random Forest (RF)	99.6%	99.6%	99.6%
Neural Network (NN)	84.4%	84.6%	84.4%
Naïve Baye's (NB)	97.8%	97.8%	97.8%

SVM	96.6%	96.8%	96.6%

TABLE 2. Performance of Classifiers:80% training: 20% testing.

Classifier	Indicators of performance		
	Training Volume:80% Testing Volume:20%		
	Recall	Precision	Accuracy
Decision Tree (DT)	99.9%	99.9%	99.9%
Random Forest (RF)	99.8%	99.8%	99.8%
Neural Network (NN)	84.6%	84.6%	84.6%
Naïve Baye's (NB)	97.8%	97.8%	97.8%
SVM	96.8%	96.8%	96.8%

The experimental results show that some classifiers perform exceptionally well, while others function around averagely. However, some single classification methods were able to match the multi-classifier model's accuracy rate while using 80% as the training size. This is entirely expected that the multi-classifier technique performed much better in each situation between 70% and 80% of the trained random sample, respectively. They consist of the classifications NB and NN. A single classifier is used in this instance chosen since a system for several classifications require more system resources and processing time than simple classification methods. Tables 1 and 2 display the findings of all trials based on two possible scenarios.70 % of the dataset was used for training in the first situation, and 80 % in the second.

Precision, recall, and accuracy were the calculated performance indicators. We divided these classifications into four groups based on the results, according to the performance metrics described above: excellent, decent, passable, and subpar. The second category, that comprises SVM and NN, came in second and did well, obtaining extremely strong accuracy rates exceeding 97.5%. NB, DT, and RF also did well. They both attained accuracy levels of 84.6% and 96.8%. Amount of precision for each classification compared to the two separate trained testing data is shown in the figure. As is discernible, a decent efficiency rate was achieved by all classification techniques, but the decision tree classification algorithm stood out since it had the highest accuracy rate throughout both training and test cases.

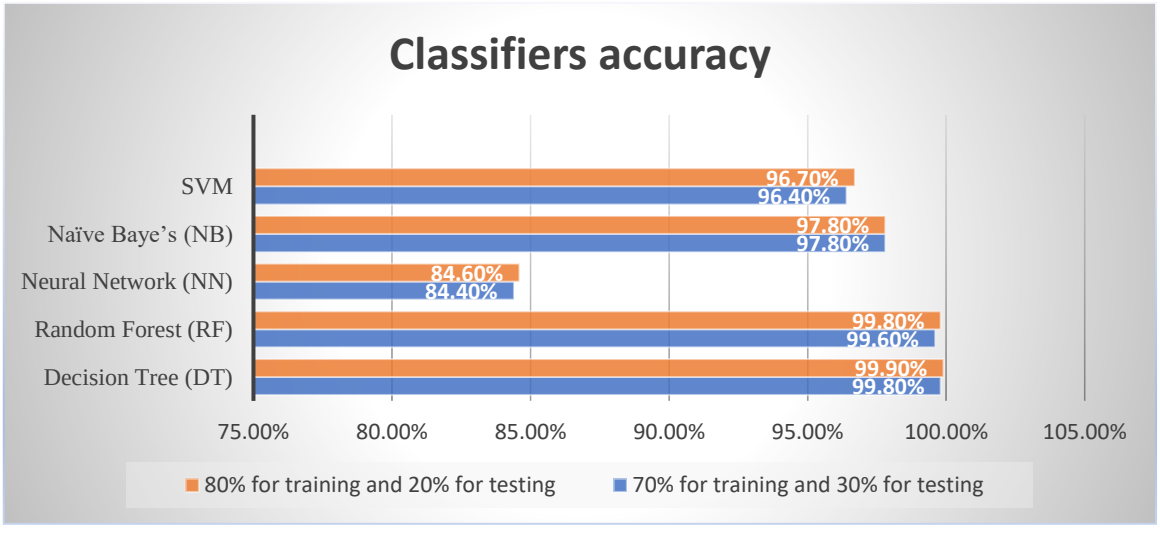


FIGURE: Classifiers accuracy.

For comparison, the accuracy rates for every classification across through two different types of training and testing are shown in Figure. The Decision Tree classification algorithm acquired a large accuracy rate

and outscored the other four classifications by doing well in each of the specific training set's two different scenarios.

CONCLUSION:

This article gives a quick review of assaults on covert channels and makes clear exactly widespread they are in modern technologies like Internet of Things (IoT), VoLTE as well as the IPv6 protocol. It highlights extremely vulnerable to covert channel attacks certain technologies and techniques are, additionally, they provide a rich atmosphere for the creation of several covert channel assault tactics, which provide a variety of challenges. With a focus on their benefits and drawbacks, this review study made its main contribution by examining the efficacy of machine learning algorithms for thwarting covert channel attacks. Eight different ML classification techniques were compared in the comparison study. The study found that while ML algorithms may successfully meet the current real-world security standards and play a key role in detecting covert channel assaults, they either fail to detect hidden channels altogether or their accuracy rate drops when trying to resemble normal traffic. Furthermore, there are several bugs in ML algorithms that let attackers carry out sophisticated assaults. In order to defend against such attacks, it is crucial to identify ML method flaws early on. Designing ML algorithms that perform well with several covert channels is tough; if any of these scenarios occurs, the technique will undoubtedly be computationally intensive and incur network overhead, lowering quality of service.

REFERENCES:

[1] D. Frolova, K. Kogos, and A. Epishkina, ‘‘Traffic normalization for covert channel protecting,’’ in Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (ElConRus), Jan. 2021

[2] L. Caviglione, ‘‘Trends and challenges in network covert channels countermeasures,’’ Appl. Sci., vol. 11, no. 4, p. 1641, Feb. 2021.

[3] S. Vanderhallen, J. Van Bulck, F. Piessens, and J. T. Mühlberg, ‘‘Robust authentication for automotive control networks through covert channels,’’ Comput. Netw., vol. 193, Jul. 2021, Art. no. 108079.

[4] S. Wu, Y. Chen, H. Tian, and C. Sun, ‘‘Detection of covert timing channel based on time series symbolization,’’ IEEE Open J. Commun. Soc., vol. 2, pp. 2372–2382, 2021.

[5] L. Caviglione, M. Zuppelli, W. Mazurczyk, A. Schaffhauser, and M. Repetto, ‘‘Code augmentation for detecting covert channels targeting the IPv6 flow label,’’ in Proc. IEEE 7th Int. Conf. Netw. Softwarization (NetSoft), Jun. 2021, pp. 450–456

[6] S. Wendzel, S. Zander, B. Fechner, and C. Herdin, ‘‘Pattern-based survey and categorization of network covert channel techniques,’’ ACM Comput. Surv., vol. 47, no. 3, p. 50, 2015.

[7] S. Wendzel, W. Mazurczyk, and S. Zander, ‘‘Unified description for network information hiding methods,’’ J. Universal Comput. Sci., vol. 22, no. 11, pp. 1456–1486, 2016.

[8] M. Wojciech, W. Steffen, Z. Sebastian, H. Amir, and S. Krzysztof, ‘‘Control protocols for reliable network steganography,’’ in Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures. Hoboken, NJ, USA: Wiley, 2016, p. 296.

[9] J. Han, C. Huang, F. Shi, and J. Liu, ‘‘Covert timing channel detection method based on time interval and payload length analysis,’’ Comput. Secur., vol. 97, Oct. 2020, Art. no. 101952.

[10] L. Zhang, T. Huang, W. Rasheed, X. Hu, and C. Zhao, ‘‘An enlargingthe-capacity packet sorting covert channel,’’ IEEE Access, vol. 7, pp. 145634–145640, 2019.

[11] S. Smith, ‘‘Hiding in the noise: Creation and detection analysis of modern covert channels,’’ Ph.D. dissertation, Dept. Comput. Sci., TennesseeTechnol. Univ., Cookeville, TN, USA, 2020.

[12] S. Wendzel, W. Mazurczyk, and G. Haas, ‘‘Don’t you touch my nuts:Information hiding in cyber physical systems,’’ in Proc. IEEE Secur.Privacy Workshops (SPW), May 2017, pp. 29–34.

[13] Y.-A. Tan, X. Zhang, K. Sharif, C. Liang, Q. Zhang, and Y. Li, ''Coverttiming channels for IoT over mobile networks,'' IEEE Wireless Commun.,vol. 25, no. 6, pp. 38–44, Dec. 2018.

[14] A. Mileva, A. Velinov, L. Hartmann, S. Wendzel, and W. Mazurczyk,''Comprehensive analysis of MQTT 5.0 susceptibility to network covertchannels,'' Comput. Secur., vol. 104, May 2021, Art. no. 102207.

[15] I. Vaccari, S. Narteni, M. Aiello, M. Mongelli, and E. Cambiaso,''Exploiting Internet of Things protocols for malicious data exfiltration activities,'' IEEE Access, vol. 9, pp. 104261–104280, 2021.