



AN EFFECTUAL INTRUSION DETECTION SYSTEM IN WIRELESS NETWORK

Dr. K.Sivasakthi Associate Professor, Department Of Computer Science,
Christhu Raj College-Trichy 12. (Affiliated by Bharathidasan University)

ARTICLE INFO	ABSTRACT
Received : 09.03.2025 Revised : 27.05.2025 Accepted : 19.08.2025 Published : 26.09.2025 Corresponding author: Dr. K.Sivasakthi shaku.ngrkl@gmail.com Keywords: Network Security, Intrusion Detection, UGR Dataset, Wireless Network.	The fast expansion of wireless network and mobile computing applications has modified the aspect of network security. The new refusal of attacks on significant network has shown us, no open PC network is invulnerable from intrusions. The wireless network is especially unprotected because of its elements of open medium, powerful changing topology, agreeable algorithms and absence of centralized observing. The conventional approach to safeguarding networks with firewalls and encryption programming is at this point not adequate and compelling. The IDS mechanism is the control unit of the intrusion detection framework. Its primary object is to deal with the framework, i.e., direct all tasks of the intrusion detection system. Its job relies upon the intrusion detection type utilized. Wireless has opened a very interesting world for us. Its innovation is progressing and changing consistently and its prominence is expanding. The greatest worry with wireless is security. The conventional wired IDS is an extraordinary system, yet sadly it does little for the wireless world. In this paper the effectual intrusion detection system implemented on wireless network.

INTRODUCTION

The networking administration has at long last grown up. The chances of changing internet processing are boundless. It is significant that the security policy of a system are planned in order protect unapproved access to system and information. In any case, totally protecting breaks of security show up, at now, unreasonable. We can, in any case, attempt to identify these intrusion attacks so that move might be made to fix the harm later. This field of analysis is called Intrusion Detection. Wireless has opened an intriguing world for us. Its technology is progressing and changing consistently and its fame is expanding. The greatest worry with wireless, be that as it may, has been security. Together with enhanced encryption techniques another answer for assist with combating this issue is the Wireless Intrusion Detection System (WIDS). In the security and wireless world this has quick turned into a significant one in securing network.

Intrusion Detection System

An Intrusion Detection System (IDS) is a techniques used to distinguish unrecognized access of a system or network. A wireless IDS plays out this effectively only for the wireless network.

These system watch traffic on your network searching for and logging access and making aware to replay.

Need For Wireless Intrusion Detection System

The conventional wired IDS system does very little for the wireless world. The issue with wireless is that it also attacks that might be performed on a wired network, the actual medium must be safeguarded. To do this there are many estimates which can be taken, but there are much more mechanism intended to break them. Because of the idea of wireless, it challenge to controlling the areas of access. Frequently the scope of a wireless network arrives at outside the actual limits of an organization. With such an issue with wireless security, creating and executing WIDS system is surely a positive development. In the event that you have wireless and are worried about attacks and attackers, a WIDS might be smart.

Countless potential attacks can be recognized by a WIDS. The succeeding will list significant attacks and actions that can be recognized with the assistance of a WIDS. Rebel devices ,for example, a user connecting an unapproved wireless switch, inappropriate setups, network issues, sticking, man-in-the-center attacks, war drivers, checking with programs like Nets tumbler or Kismet, RF obstruction, Macintosh satirizing, DoS attacks, make an effort of brute power to get pass, areas of strength for 802.1x, or utilization of traffic infusion devices. Different WIDS mechanisms and programming have various abilities in what can be detected.

There are at present just a modest bunch of merchants who offer a wireless IDS arrangement - yet the items are powerful and have a broad list of capabilities. Famous wireless IDS arrangements incorporate Air-defense, Rogue Watch and Air-defense Guard, and net Security system Real fix Server sensor and remote scanner devices. A local wireless IDS can be created with the utilization of the operating system.

Literature Survey

PriyankaJadhav et all[4] has studied that, Both open-source and commercial wireless IDS solutions are available, and each has its own benefits. Wireless intrusion detection systems are a crucial component of wireless local area networks' security. The advantages of a wireless IDS can be significant because it can help with policy enforcement and can identify probes, DoSs, and various 802.11 attacks. Veeram Reddy Jyothsna et all[7] developed generic meta heuristic

scale for both known and unknown attacks with high detection rate and low false rate by adopting efficient feature optimization techniques.

Gabriel Macia Fernandez et all[5]evaluated a new dataset with real traffic with and up to date attacks. The main advantage of this dataset over others is that the background is very representative of the internet traffic as it captured from sensors in ISP network where many different profiles of clients are located. Reduced input features are crucial for creating effective and efficient IDS, according to Mukherjee et al.'s [3] research. Utilising correlation-based feature selection (CFS), information gain (IG), and gain ratio (GR), they looked into the effectiveness of three common feature selection techniques. They applied the Naive Bayes classifier to the reduced intrusion dataset and devised the Feature Vitality Based Reduction Method (FVBRM) to find significant reduced input features.

UGR DATASET

The assessment of algorithms and strategies to execute intrusion discovery system strongly depend on the presence of the dataset. Somewhat recently, a great deal of attempt have been finished towards building these datasets. However, there is still space to get to the next level. In this paper, we present a new dataset that is worked with actual traffic and recent attacks. The fundamental benefit of this dataset over past ones is its convenience for assessing IDSs that think about long haul development and traffic periodicity. Models that think about contrasts in daytime/night or work days/ends of the week can likewise be prepared and assessed with it. We examine every one of the necessities for a cutting edge IDS assessment dataset and investigate how the one introduced here meets the various requirements.

Types of Attacks in UGR dataset

Types of Attack	Class	Label
DOS11	Signature	dos
DOS53s	Signature	dos
Dos53a	Signature	dos
Scan11	Signature	Scan11
Scan44	Signature	Scan44
Botnet	Signature	nerisbotnet
Ipinblacklist	Signature	blacklist
UDP scan	Anomaly	Anomaly-udbscan
SSH scan	Anomaly	Anomaly-ssbscan
SPAM	Anomaly	Anomaly-spam

ECWNA (Efficient Classification Wireless Network Algorithm)

ECWNA is specially designed for wireless network. This algorithm detects the intrusion in the wireless network. ECWNA classify the attacked record in a efficient way. It detects signature based attacks and also anomaly based attacks in the network.

The formula for ECWNA:

$MAX[(\sum[P(Fi/C1)], \sum[P(Fi/C2)], \dots, \sum[P(Fi/CN)])]$ Where

$Fi \leftarrow$ Features in the record

$C1, C2, \dots, CN \leftarrow$ No of Classes in the dataset (Types of At-

tack, Normal)

$P(Fi/Ci) \leftarrow$ Probability of each feature belongs to the class

ALGORITHM

STEP 1: Read the training dataset S

STEP2: $R1, R2, \dots, Rn$ are the records to be classified.

STEP3: $F1, F2, F3, \dots, Fn$ are the features $\in R$.

STEP4: Calculate $P(Fi/C1), P(Fi/C2), \dots, P(Fi/Cn)$

Find the probability of each feature with each class.

STEP5: Calculate $\sum[P(Fi/Ci)]$ for each class.

STEP6: Stop until all Fi perfectly classified.

STEP7: Get the highest like-hood.

Detection Accuracy Rate for DOS Attack

DOS	SCAN	BOTNET	IPINBLACK LIST	SPAM
4850	2	0	1	0
2	25	2	0	0
1	1	3	0	1
1	1	0	1	0
0	0	0	0	0

Table 1

A Denial-of-Service(DOS) attack is an attack meant to collapse a machine making it inapproachable to its own end users. DOS attacks accomplish this by submerging the target with traffic. The above table1 is the samples of confusion matrix of DOS attack. Total number of DOS attack in the dataset is 5000. Out of 5000 records 4850 records are classified as DOS class.

Detection Accuracy Rate for SCAN Attack

DOS	SCAN	BOTNET	IPINBLACKLIST	SPAM
1	1	0	0	0
1	3100	1	2	0
0	1	1	4	0
1	0	2	0	0
0	1	0	1	1

Table 2

Scanning is used to identify the systems joined to an association network. It provides data about the systems and services on a intended system. Some may relate to this type of check up as an active scan because it can definitely screw up services on those host that are affected.

The above table2 is the samples of confusion matrix of scan attack. The total number of SCAN attack in the dataset is 3500. Out of 3500 records 3100 records are detected as SCAN class.

Detection Accuracy Rate for Botnet Attack

DOS	SCAN	BOTNET	IPINBLACKLIST	SPAM
1	0	1	0	0
2	1	0	1	0
1	0	3500	0	0
1	0	0	0	0
0	1	0	1	0

Table3

The attackers can take over control of the devices activities to remotely control them using botnet command and control. The above table3 is the samples of confusion matrix of botnet attack. The total number of botnet attack in the dataset is 3700. Out of 3700 records 3500 records are detected as BOTNET class.

Detection Accuracy Rate for IPINBLACK LIST Attack

DOS	SCAN	BOTNET	IPINBLACKLIST	SPAM
1	0	0	1	0
1	0	1	0	0
0	0	3	1	0
0	1	0	1450	0
1	0	0	1	0

Table4

IP blacklisting is a technique for preventing malicious (or) unauthorized IP addresses from connecting to your networks. List of IP addresses (or) IP address ranges that you want to block are called blacklists. The above table4 is the samples of confusion matrix of ipinblack list.

The total number of ipinblack list attack in the dataset is 2000. Out of 2000 records 1450 records are detected as IPBLACK LIST class.

Detection Accuracy Rate for SPAM Attack

DOS	SCAN	BOTNET	IPINBLACKLIST	SPAM
1	0	2	0	1
1	0	0	1	0
0	0	1	0	1
5	1	0	1	0
0	1	1	0	1200

Table5

Spamming is the practice of sending numerous unsolicited messages to numerous recipients for any unlawful purpose using messaging network. The above table5 is the samples of confusion matrix of spam attack. The total number of spam attack in the dataset is 1800. Out of 1800 records 1200 records are detected as SPAM attack.

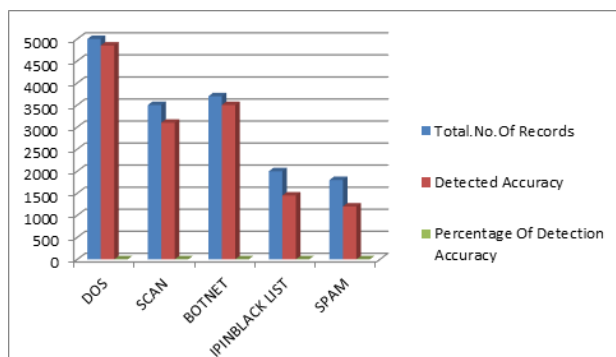
Attack Percentage in UGR Dataset

Attack Type	Total.No.Of Records	Detected Accuracy	Percentage Of Detection Accuracy
DOS	5000	4850	97%
SCAN	3500	3100	88%
BOTNET	3700	3500	94%
IPINBLACK LIST	2000	1450	72.5%
SPAM	1800	1200	66%

Table6

Total number of records taken for analysis was 20000. Out of 20000 records 14100 records are detected as attacked class. The overall detection accuracy using ECWNA is 70.5%. Out of 20000 records 5900 records are classified as normal class.

Graphical Representation of Detection Accuracy of ECWNA



Chart

The above chart described the detection accuracy of ECWNA. The chart shows that the DOS attack has higher detection accuracy. Compare to other attacks the SPAM has lower detection accuracy. Total 20000 records were selected for this work. Out of 20000 records 14100 records are detected as attacked.

Conclusion:

In this paper, the main work is using a new dataset for the evaluation of IDS algorithm and systems called UGR16. In this study address the various attacks of wireless network. The algorithm ECWNA executed in this work find both signature based and anomaly based attacks. The several attacks taking place in the

different layer of the wireless network. Totally 20,000 thousand records are taken for analysis. Out of 20,000 thousand records 14,100 records are detected as attacked. Remaining 5900 records are classified as normal. The future enhancement of the work is increase the detection accuracy of the attacks.

References

- [1] Wireless Intrusion Detection Systems Including Incident Response & Wireless Policy, by Jeff Dixon. http://www.infoscwriters.com/text_resources/pdf/Wireless_1_DS_JDixon.pdf
- [2] An Overview of the Wireless Intrusion Detection System, by Oliver Pobleto. http://www.sans.org/reading_room/whitepapers/wireless/overview-wireless-intrusion-detection-system_1599
- [3] SAURABH Mukherjee, INTRUSION DETECTION USING NAIVE BAYES CLASSIFIER WITH FEATURE REDUCTION, *PROCEDIA TECHNOLOGY-ELSEVIER*, VOLUME 4, 2012, PAGES 119-128.
- [4] PriyankaJadhav, Wireless Intrusion Detection Systems, Security, Article in International Journal of Publication, August 2010.
- [5] Gabriel Maciá-Fernández, UGR'16: A new dataset for the evaluation of cyclostationarity-based network-IDSs, Research Gate, Article in Computers & Security- November 2017.
- [6] Gong Y, Mabu S, Chen C, Wang Y, Hirasawa K. Intrusion detection system combining misuse detection and anomaly detection using genetic network programming. In: ICCAS-SICE. 2009
- [7] Veeramreddy Jyothsna, Anomaly-Based Intrusion Detection System, Web of Science, DOI: <http://dx.doi.org/10.5772/intechopen.82287>
- [8] Lee J, Moskovics S, Silacci L. A survey of intrusion detection analysis methods. CSE 221, University of California, San Diego, Spring 1999
- [9] Prayote A. Knowledge-based anomaly detection [PhD dissertation]. School of Computer Science and Engineering, The University of New South Wales; 2007
- [10] Caulkins LTCBD, Lee J, Wang M. A dynamic data mining technique for intrusion detection systems. In: Proceedings of the 43rd Annual Southeast Regional Conference (ACMSE 43). Vol. 2. 2005. pp. 148-153
- [11] Tsai C-F et al. Intrusion detection by machine learning: A review. *Expert Systems with Applications*. 2009; 36(10):11994-12000
- [12] Revathi S, Malathi DA. A detailed analysis on NSLKDD dataset using various machine learning techniques for intrusion detection. *International Journal Engineering Research and Technology (IJERT)*. Dec 2013;2(12)
- [13] Bhuyan MH, Bhattacharyya DK, Kalita JK. Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys & Tutorials*. 2014;16(1):303-336
- [14] Wagh SK, Pachghare VK, Kolhe SR. Survey on intrusion detection system using machine learning techniques. *International Journal of Computer Applications (0975-8887)*. 2013;78(16): 30-37
- [15] Gilmore C, Haydaman J. Anomaly detection and machine learning methods for network intrusion detection: An industrially focused literature review. In: *International Conference Security and Management*; CSREA Press.