Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Integrating Risk Profiles

Mobile Adhoc Networks and Networking

Highlights

Existing Network Traffic Datasets

Overview of Existing Intrusion Prevention

Discovering Thoughts, Inventing Future

VOLUME 23 ISSUE 3 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 23 Issue 3 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

Editorial Board

Global Journal of Computer Science and Technology

Dr. Stefano Berretti

Ph.D. in Computer Engineering and Telecommunications, University of Firenze Professor Department of Information Engineering, University of Firenze, Italy

Dr. Abdurrahman Arslanyilmaz

Computer Science & Information Systems Department Youngstown State University Ph.D., Texas A&M University University of Missouri, Columbia Gazi University, Turkey

Dr. Lamri Sayad

Ph.d in Computer science, University of BEJAIA, Algeria

Dr. Tauqeer Ahmad Usmani

Ph.D in Computer Science, Oman

Dr. Hazra Imran

Ph.D in Computer Science (Information Retrieval), Athabasca University, Canada

Dr. Magdy Shayboub Ali

Ph.D in Computer Sciences, MSc in Computer Sciences and Engineering, BSc in Electronic Engineering, Suez Canal University, Egypt

Dr. Nurul Akmar Binti Emran

Ph.D in Computer Science, MSc in Computer Science, Universiti Teknikal Malaysia Melaka, Malaysia

Dr. Asim Sinan Yuksel

Ph.D in Computer Engineering, M.Sc., B.Eng., Suleyman Demirel University, Turkey

Dr. Anis Bey

Dept. of Computer Science, Badji Mokhtar-Annaba University, Annaba, Algeria

Alessandra Lumini

Associate Researcher Department of Computer Science and Engineering University of Bologna Italy

Dr. Rajesh Kumar Rolen

Ph.D in Computer Science, MCA & BCA - IGNOU, MCTS & MCP - MIcrosoft, SCJP - Sun Microsystems, Singhania University, India

Dr. Rajneesh Kumar Gujral

Ph.D in Computer Science and Engineering, M.TECH in Information Technology, B. E. in Computer Science and Engineering, CCNA Certified Network Instructor, Diploma Course in Computer Servicing and Maintenance (DCS), Maharishi Markandeshwar University Mullana, India

Dr. Aziz M. Barbar

Ph.D. IEEE Senior Member Chairperson, Department of Computer Science AUST - American University of Science & Technology Alfred Naccash Avenue Ashrafieh, Lebanon

Dr. Federico Tramarin

Ph.D., Computer Engineering and Networks Group, Institute of Electronics, Italy Department of Information Engineering of the University of Padova, Italy

Dr. Chutisant Kerdvibulvech

Dept. of Inf. & Commun. Technol., Rangsit University Pathum Thani, Thailand Chulalongkorn University Ph.D. Thailand Keio University, Tokyo, Japan

Dr. Roheet Bhatnagar

Ph.D in Computer Science, B.Tech in Computer Science, M.Tech in Remote Sensing, Sikkim Manipal University, India

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 23 Issue 3 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Mobile Adhoc Network Risk Profiles - An Overview of Existing Network Traffic Datasets to Determine Ideal Axiom Criteria

By Jedidiah Aqui & Michael Hosein

University of the West Indies St. Augustine

Abstract- A Mobile Adhoc networks also known as MANET or Wireless Adhoc Network is a network that usually has aroutable networking environment on top of a Link Layer ad hoc network. It consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. Recent studies and fieldwork have pointed in the direction of making MANETS a publicly viable option in the event of another world event/crisis such as the recent COVID-19 pandemic. As opposed to their traditional military and emergency uses, this has become a focal point due to the evident strain that was observed on mainstream Internet Service Providers as substantial adjustments had to be made to facilitate a new 'working-from-home' public. A primary aspect that must be considered before public adoption is addressing the issue of MANET risk and Security which leads into identifying and classifying risks associated with MANETS.

Index Terms: *MANET, risk profile, dataset, IDS, network, traffic.*

GJCST-E Classification: *ACM: C.2.1, C.2.3, C.4*

Strictly as per the compliance and regulations of:

Mobile Adhoc Network Risk Profiles - An Overview of Existing Network Traffic Datasets to Determine Ideal Axiom Criteria

Jedidiah Aqui [α] & Michael Hosein [σ]

Abstract- A Mobile Adhoc networks also known as MANET or Wireless Adhoc Network is a network that usually has aroutable networking environment on top of a Link Layer ad hoc network. It consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. Recent studies and fieldwork have pointed in the direction of making MANETS a publicly viable option in the event of another world event/crisis such as the recent COVID-19 pandemic. As opposed to their traditional military and emergency uses, this has become a focal point due to the evident strain that was observed on mainstream Internet Service Providers as substantial adjustments had to be made to facilitate a new 'working-from-home' public. A primary aspect that must be considered before public adoption is addressing the issue of MANET risk and Security which leads into identifying and classifying risks associated with MANETS. This paper seeks to analyze the various existing fields and meta-data within various networking datasets, protocols as well as scenarios and subsequently establish what aspects of existing network traffic can be classified into axioms (Risk Classifying arguments) to determine Risk Profiles of MANETS. The paper also seeks to determine and propose the ideal data fields within Network traffic for classifying Risk Profiles.

Index Terms: MANET, risk profile, dataset, IDS, network, traffic.

I. Introduction

Research on the usage of wireless protocols and networks such as Bluetooth, NFC and MANETS in a public capacity has recently undergone a resurgence due to Global events such as the COVID-19 pandemic. And whilst protocols such as NFC and bluetooth has been explored in varying settings such as mentioned in, [1], [2] and further research was done in light of the Global Pandemic as per [3] and [4]. There was an evident need for greater public usage and adoption of these protocols to test the reliability and uses of them in light of the traditional reliance on mainstream Internet Service providers. To this end, advances in multiplexing connectivity for the Bluetooth protocol were made as per the work conducted in [5], [6] and [7] to allow for more simultaneous connectivity amongst mobile nodes in a network. However, the challenge of having a reliable wide-area infrastructure less network remained a challenge. Consequently, the prospects of utilizing MANETS in a public setting was explored.

As mentioned in the Abstract a MANET is a network that usually has a routable networking environment on top of a link layer ad hoc network. It consists of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. However, prior to delving into any discourse on public adoption, it is imperative to underscore a critical focal point: the risks and security considerations inherent to Mobile Ad-Hoc Networks (MANETs).

Based on [8] and [9] both qualitative and quantitative research has alluded to the fact that there is an evident disparity in probability-based Risk determination not only within MANETS but generally in Networking on a whole. An evident trend in Risk and Security analysis within MANETS has also shown that most Intrusion and Anomaly detection and prevention systems undertake a reactive approach to network security events which can be attributed to the dominance of 'impact-based' studies and techniques developed to address MANET and Network security.

This paper serves as an extended and in-depth analysis, aiming to substantiate the concept of Risk Profile generation introduced in [10]. Through meticulous examination, the study identifies specific domains within Network Traffic that can be readily categorized into axioms, laying the foundational groundwork for constructing an initial Risk Profile for Mobile Ad-Hoc Networks (MANETs). The research also assesses the optimal fields suitable for establishing axioms crucial to the generation of a risk profile. This analysis is integral to complementing both the passive and active phases proposed in [10] for a comprehensive solution and/or framework.

II. Literature Review

The following dataset was used in [11], [12] and [13], the work of these papers focused on developing a reference model to address the constraint of limiting user data usage in a generalized manner due to a

Author α σ: Department of Computing and Information Technology University of the West Indies St. Augustine, Trinidad and Tobago.
e-mail: aqui2_jed@yahoo.com

subsection of 'feature-rich', 'bandwidth-heavy' over the top (OTT) applications. This paper focused on personalizing service degradation policies by providing guidelines for users' OTT consumption behavior classification based on Incremental Learning (IL).

In essence, the research focused on creating a tailored framework designed to pinpoint users influencing network service quality through Over-The-Top (OTT) applications. This approach steered clear of a generalized strategy that would restrict data to all users, instead honing in on specific individuals. Notably, the dataset employed, denoted as Uninauca 141 applications, encompassed a diverse array of fields, a subset of which is exemplified in Figures 1 and 2 respectively.

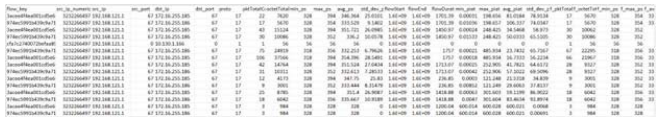

Fig. 1: Features and Fields Captured in the Uninauca Dataset

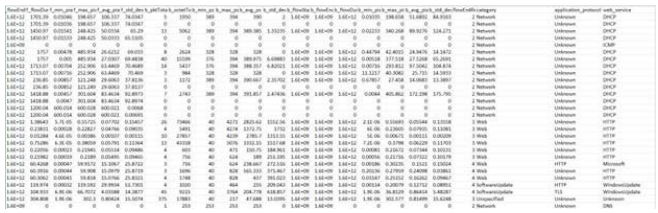

Fig. 2: Features and Fields captured in the Uninauca dataset continued

One of the immediate observations was that this network traffic focused heavily on layer 7 (application layer) information as the usage of applications by nodes connected were being monitored hence in the 'category' column for all Network packet captures there was a reading of 'unkown' for the application layer.

This dataset contains 50 features in which each instance holds the information of an IP flow generated by a network device i.e., source and destination IP addresses, ports, flow durations, interarrival times, packet sizes and layer 7 protocol (application) used on that flow as the class. For this dataset Axiom1 (Device Type) may not be easily achievable as the data suggests that of all protocols used ARP was not captured/utilized as it is a layer 3 protocol and thus, identifying MAC addresses for resolution would not be possible via this means. The only method would be to deduce the device type by patterns observed in network traffic, or type of requests made and what protocols were used.

Axiom2 (malicious node/repeat offender) is more achievable as one of the methods to identify a malicious node is to observe the identified anomalous nodes based on cached IPs or observe patterns for suspicious node behaviour, this can be derived from understanding (Source IP, Destination IP, Protocols being used).

The research conducted in [14] and [15], an in depth analysis was conducted on existing bodies of datasets to determine the accuracy of their usage in contemporary Intrusion Detection and Intrusion Prevention systems. What was found was that the 11 datasets used since the year 1998 was grossly outdated and unreliable which therefore lead to inaccurate deployment, analysis and evaluation of IDS's and IPS's. Additionally, it was found that some of the datasets such as 'DARPA98', 'KDD99', 'ISC2012', 'ADFA13' suffered from lack of traffic diversity and volumes, there were disparities in terms of the types of attacks the datasets covered.

Thus, the authors produced reliable datasets which contained benign and seven common attack network flows that meet real world criteria. All with the aim to evaluate performance of a comprehensive set of network traffic features and ML algorithms to give an indication of the optimum set of features for detecting certain attack categories.

The datasets (CICIDS2017dataset) provided covered network traffic for 5 days of the week (Monday through Friday) and identified different types of Network attacks such as: 'DDos', 'PortScan', 'Infilteration', 'WebAttacks', 'Brute Force SSH'. This was a guided approach based on the attack listing provided by McAffee.

Apart from the well-known network traffic meta-data, there were several other noted meta-data fields, most notably the datasets were categorized by Network Behavioural patterns observed in traffic and subsequently labeled based on the perceived type of attack the network experienced. This label was also observed to form the basis of the "Label" field within each of the Network traffic Datasets as shown in the below figures 3, 4, 5 and 6 respectively:

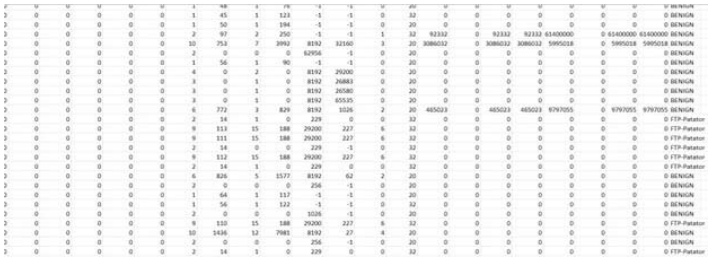

Fig. 3: Brute Force Attack

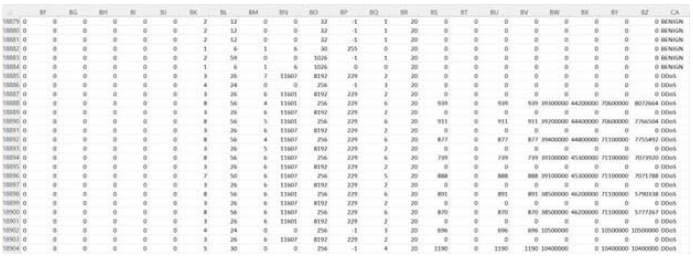

Fig. 4: Distributed Denial of Service Attack

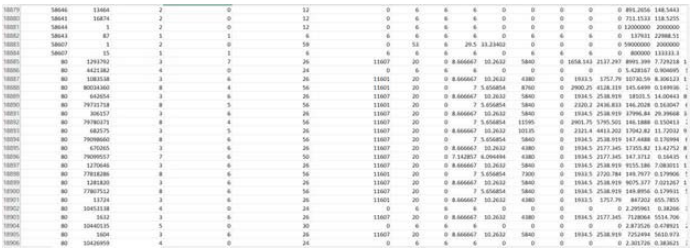

Fig. 5: Distributed Denial of Service Attack cont'd

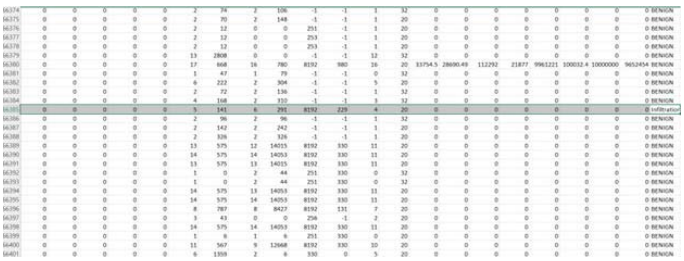

Fig. 6: Showing an Infiltration Attack

One of the most integral points to note on this paper was the method of labelling and classification utilized to further fine tune the dataset for more accurate and relevant Intrusion Detection and Prevention analysis. The most critical meta data field can be recognized by the 'Label' field as it distinguished between a benign Network activity and a specific attack. Similarly, a strain of this methodology is desired for the determination of Risk Profile for a MANET based on the identified axioms.

Another Dataset that was examined from the work conducted by [16] was captured from a Network Intrusion Detection System and captured fields such as 'Source Address Bytes', 'Destination Address bytes', 'Ip Address', 'Port Number', 'Fragmentation Bit', 'Mac ID', 'Protocol Type', 'DNS', 'TLS – transport security layer', just to name a few, However one of the most critical Meta Data fields captured in this dataset was observed to be the 'Mac ID' field. As it pertains to the current direction of the proposed solution for establishing Risk Profiles, One of the most basic Axiom defined for classifying the risk level of the MANET identifies device types. The MAC Id can be observed as an iterative step towards determining device type once it has been sourced and the device determined. This therefore, leads to a much more accurate determination of devices as opposed to observing network node behaviours which are more reliant on experience and humanistic determinations. The below figures 7 and 8 show examples of Network Meta Data fields that were captured:

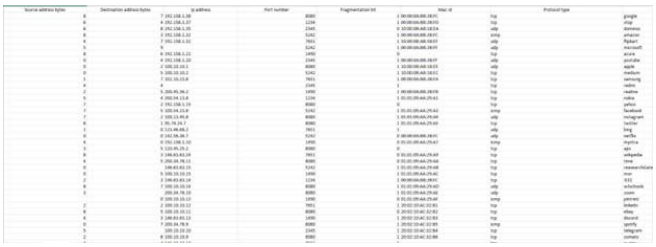

Fig. 7: Showing Packet Data Captured from an Intrusion Detection System

Another dataset (UNSWNB15) that was analyzed was derived from several papers [17], [18], [19] and [20]. These papers are namely "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)", "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset", "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks", "Big data analytics for intrusion detection system: statistical decision- making using finite dirichlet mixture models."

DNS	TLS - transport security layer (0 or 1)	SSH – secure shell (0 or 1)	Service
google	0	0	http
vtop	0	1	private
dominos	1	1	private
amazon	0	0	https
flipkart	0	0	eco_i
microsoft	1	0	http
azure	1	1	domain_u
youtube	1	0	https
apple	1	0	smtp
medium	0	1	domain_u
samsung	0	0	https
redmi	0	0	private
realme	0	1	http
nokia	1	1	http
yahoo	1	1	domain_u
facebook	0	1	private
instagram	1	1	https
twitter	0	0	eco_i
bing	0	0	https
netflix	0	0	domain_u
myntra	0	1	http
ajio	1	0	http
wikipedia	0	0	domain_u
time	0	1	http
reasearchGate	0	0	https
msn	1	0	http
IEEE	1	0	eco_i
w3schools	0	1	smtp
zoom	0	1	https
pintrest	0	0	http
linkedn	0	1	http
ebay	0	1	eco_i
discord	0	0	http
spotify	0	0	https
telegram	0	0	domain_u
zomato	0	0	http

Fig. 8: Showing Packet Data Captured from an Intrusion Detection System Cont'd

The Datasets utilized in these papers can be viewed as a combination of a 100Gb network traffic (PCAP files) and the generated datasets created by the IXIA PerfectStorm tool in the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS). The work done primarily focused on improving the resilience of intrusion detection within Networks specifically for the protocols: "Domain Name System (DNS)", "Hyper Text Transfer Protocol (HTTP)" and "Message Queue Telemetry Transport (MQTT)". A main focal point for these protocols was the extensive usage of same by internet of Things (IOT) devices within a network and the likelihood of cyber threats against them and the services they utilize. The Dataset contains nine distinct type of attacks namely:

- Fuzzers
- Analysis
- Backdoors
- Denial of Service
- Exploits
- Generic
- Reconnaissance
- Shellcode
- Worms

Features of the Dataset with class labels were developed by 12 algorithms. The below diagram depicts all 49 of the generated features of the Dataset:

In Addition to improving the resilience of IDS' the research conducted was also aimed at reducing the amount of 'false positives' generated by IDS in response to zero-day vulnerabilities and other type of Network threats. In [20]: Statistical Decision-Making Using Finite Dirichlet Mixture Models" focus was placed on developing a scalable framework for building an effective and lightweight anomaly detection system. The framework consisted of three (3) modules:

- Capturing and Logging – Responsible for sniffing and collecting network data.
- Pre-processing – Responsible for analyzing and filtering data to improve performance of the decision engine.
- Decision Engine – Designed based on the Dirichlet mixture model with lower upper interquartile range as decision engine.

The framework's performance was based on the two main datasets the NSL-KDD and UNSQ-NB15 with the aim of determining which technique provided a higher detection rate and lower false alarm rate than other predominant techniques.

The below are snippets of the datasets utilized as well as the 'attack' classification schema:

No.	Name	Type	Description
1	srcip	nominal	Source IP address
2	sport	integer	Source port number
3	dstip	nominal	Destination IP address
4	dsport	integer	Destination port number
5	proto	nominal	Transaction protocol
6	state	nominal	Indicates to the state and its dependent protocol, e.g. ACC, CLO, CON, ECO, ECR, FIN, INT, MAS, PAR, REQ, RST, TST, TXD, URH, URN, and (-) (if not used state)
7	dur	Float	Record total duration
8	sbytes	Integer	Source to destination transaction bytes
9	dbytes	Integer	Destination to source transaction bytes
10	sttl	Integer	Source to destination time to live value
11	dttl	Integer	Destination to source time to live value
12	sloss	Integer	Source packets retransmitted or dropped
13	dloss	Integer	Destination packets retransmitted or dropped
14	service	nominal	http, ftp, smtp, ssh, dns, ftp-data ,irc and (-) if not much used service
15	Sload	Float	Source bits per second
16	Dload	Float	Destination bits per second
17	Spkts	integer	Source to destination packet count
18	Dpkts	integer	Destination to source packet count
19	swin	integer	Source TCP window advertisement value
20	dwin	integer	Destination TCP window advertisement value
21	stcpb	integer	Source TCP base sequence number
22	dtcpb	integer	Destination TCP base sequence number
23	smeansz	integer	Mean of the ?ow packet size transmitted by the src
24	dmeansz	integer	Mean of the ?ow packet size transmitted by the dst
25	trans_depth	integer	Represents the pipelined depth into the connection of http request/response transaction
26	res_bdy_len	integer	Actual uncompressed content size of the data transferred from the server's http service.
27	Sjit	Float	Source jitter (mSec)
28	Djit	Float	Destination jitter (mSec)
29	Stime	Timestamp	record start time
30	Ltime	Timestamp	record last time
31	Sintpkt	Float	Source interpacket arrival time (mSec)
32	Dintpkt	Float	Destination interpacket arrival time (mSec)

Fig. 9: Showing features of the Dataset USNW-NB15 dataset

33	32 Dintpkt	Float	Destination interpacket arrival time (mSec)
34	33 tcprtt	Float	TCP connection setup round-trip time, the sum of 'synack' and 'ackdat'.
35	34 synack	Float	TCP connection setup time, the time between the SYN and the SYN_ACK packets.
36	35 ackdat	Float	TCP connection setup time, the time between the SYN_ACK and the ACK packets.
37	36 is_sm_ips_ports	Binary	If source (1) and destination (3)IP addresses equal and port numbers (2)(4) equal then, this variable takes value 1 else 0
38	37 ct_state_ttl	Integer	No. for each state (6) according to specific range of values for source/destination time to live (10) (11).
39	38 ct_flw_http_mthd	Integer	No. of flows that has methods such as Get and Post in http service.
40	39 is_ftp_login	Binary	If the ftp session is accessed by user and password then 1 else 0.
41	40 ct_ftp_cmd	integer	No of flows that has a command in ftp session.
42	41 ct_srv_src	integer	No. of connections that contain the same service (14) and source address (1) in 100 connections according to the last time (26).
43	42 ct_srv_dst	integer	No. of connections that contain the same service (14) and destination address (3) in 100 connections according to the last time (26).
44	43 ct_dst_ltm	integer	No. of connections of the same destination address (3) in 100 connections according to the last time (26).
45	44 ct_src_ltm	integer	No. of connections of the same source address (1) in 100 connections according to the last time (26).
46	45 ct_src_dport_ltm	integer	No of connections of the same source address (1) and the destination port (4) in 100 connections according to the last time (26).
47	46 ct_dst_sport_ltm	integer	No of connections of the same destination address (3) and the source port (2) in 100 connections according to the last time (26).
48	47 ct_dst_src_ltm	integer	No of connections of the same source (1) and the destination (3) address in in 100 connections according to the last time (26).
49	48 attack_cat	nominal	The name of each attack category. In this data set , nine categories e.g. Fuzzers, Analysis, Backdoors, DoS Exploits, Generic, Reconnaissance, Shellcode and Worms
50	49 Label	binary	0 for normal and 1 for attack records

Fig. 10: Showing features of the Dataset USNW-NB15 dataset cont'd

59.166.0.0	1390	149.171.126.6	53	udp	CON	0.001055	132	164	31	29	0	0	dns	500473.9	621800.9	2	2	0	0	0
59.166.0.0	33661	149.171.126.9	1024	udp	CON	0.036133	528	304	31	29	0	0	-	87676.09	50480.17	4	4	0	0	0
59.166.0.6	1464	149.171.126.7	53	udp	CON	0.001119	146	178	31	29	0	0	dns	521894.5	636282.4	2	2	0	0	0
59.166.0.5	3593	149.171.126.5	53	udp	CON	0.001209	132	164	31	29	0	0	dns	436724.6	542597.2	2	2	0	0	0
59.166.0.3	49664	149.171.126.0	53	udp	CON	0.001169	146	178	31	29	0	0	dns	499572.3	609067.6	2	2	0	0	0
59.166.0.0	32119	149.171.126.9	111	udp	CON	0.078339	568	312	31	29	0	0	-	43503.23	23896.14	4	4	0	0	0
59.166.0.6	2142	149.171.126.4	53	udp	CON	0.001134	132	164	31	29	0	0	dns	465608.5	578483.3	2	2	0	0	0
10.40.182.3	0	10.40.182.3	0	arp	INT	0	46	0	0	0	0	0	-	0	0	1	0	0	0	0
59.166.0.5	40726	149.171.126.6	53	udp	CON	0.001126	146	178	31	29	0	0	dns	518650.1	632328.8	2	2	0	0	0
59.166.0.7	12660	149.171.126.4	53	udp	CON	0.001167	132	164	31	29	0	0	dns	452442.2	562125.1	2	2	0	0	0
10.40.170.2	0	10.40.170.2	0	arp	INT	0	46	0	0	0	0	0	-	0	0	1	0	0	0	0
10.40.170.2	0	10.40.170.2	0	arp	INT	0	46	0	0	0	0	0	-	0	0	1	0	0	0	0
10.40.182.3	0	10.40.182.3	0	arp	INT	0	46	0	0	0	0	0	-	0	0	1	0	0	0	0
59.166.0.1	48847	149.171.126.5	53	udp	CON	0.001093	132	164	31	29	0	0	dns	483074.1	600182.9	2	2	0	0	0
59.166.0.1	24266	149.171.126.9	41049	udp	CON	0.001851	528	304	31	29	0	0	-	1711507	985413.3	4	4	0	0	0
59.166.0.1	10393	149.171.126.6	44307	udp	CON	0.001749	528	304	31	29	0	0	-	1811321	1042882	4	4	0	0	0
59.166.0.2	62539	149.171.126.4	53	udp	CON	0.001128	132	164	31	29	0	0	dns	468085.1	581560.3	2	2	0	0	0
59.166.0.1	21270	149.171.126.9	111	udp	CON	0.005153	568	312	31	29	0	0	-	661362.3	363283.5	4	4	0	0	0
59.166.0.1	8989	149.171.126.6	111	udp	CON	0.004898	568	312	31	29	0	0	-	695794.2	382196.8	4	4	0	0	0
59.166.0.4	49346	149.171.126.5	53	udp	CON	0.001111	132	164	31	29	0	0	dns	475247.5	590459.1	2	2	0	0	0
175.45.176.3	21223	149.171.126.18	32780	udp	INT	0.000021	728	0	254	0	0	0	-	1.39E+08	0	2	0	0	0	0
175.45.176.2	21057	149.171.126.16	80	tcp	FIN	0.240128	918	25552	62	252	2	10	http	28050.42	815794.2	12	24	255	255	1.71E+09
175.45.176.0	13284	149.171.126.16	80	tcp	FIN	2.39039	1362	268	254	252	6	1	http	4233.619	749.6685	14	6	255	255	3.9E+09
59.166.0.3	4192	149.171.126.9	53	udp	CON	0.001101	132	164	31	29	0	0	dns	479564	595822	2	2	0	0	0
59.166.0.2	26872	149.171.126.8	53	udp	CON	0.001082	132	164	31	29	0	0	dns	487985.2	606284.7	2	2	0	0	0
59.166.0.8	24946	149.171.126.2	53	udp	CON	0.001122	132	164	31	29	0	0	dns	470588.2	584670.2	2	2	0	0	0
59.166.0.9	5685	149.171.126.6	53	udp	CON	0.001141	146	178	31	29	0	0	dns	511831.8	624014.1	2	2	0	0	0
59.166.0.0	22848	149.171.126.1	53	udp	CON	0.001164	146	178	31	29	0	0	dns	501718.2	611683.8	2	2	0	0	0

Fig. 11: Showing the Packet Data Captured in the USNW-NB15 Dataset

0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.017	0.013	0	0	0	0	0	0	0	3	7	1	1
0	132	76	0	0	9.89101	10.68273	1.42E+09	1.42E+09	7.005	7.564333	0	0	0	0	0	0	0	2	4	2	3
0	73	89	0	0	0	0	1.42E+09	1.42E+09	0.017	0.013	0	0	0	0	0	0	0	12	8	1	2
0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.043	0.014	0	0	0	0	0	0	0	6	9	1	1
0	73	89	0	0	0	0	1.42E+09	1.42E+09	0.005	0.003	0	0	0	0	0	0	0	7	9	1	1
0	142	78	0	0	29.68222	34.37034	1.42E+09	1.42E+09	21.003	24.315	0	0	0	0	0	0	0	2	4	2	3
0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.017	0.013	0	0	0	0	0	0	0	12	7	1	2
0	46	0	0	0	0	0	1.42E+09	1.42E+09	0	0	0	0	0	1	2	0	0	2	2	2	2
0	73	89	0	0	0	0	1.42E+09	1.42E+09	0.018	0.013	0	0	0	0	0	0	0	6	7	3	1
0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.018	0.013	0	0	0	0	0	0	0	6	7	2	1
0	46	0	0	0	0	0	1.42E+09	1.42E+09	0	0	0	0	0	1	2	0	0	2	2	2	2
0	46	0	0	0	0	0	1.42E+09	1.42E+09	0	0	0	0	0	1	2	0	0	2	2	2	2
0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.018	0.013	0	0	0	0	0	0	0	6	9	2	5
0	132	76	0	0	0.656903	0.328339	1.42E+09	1.42E+09	0.471	0.237667	0	0	0	0	0	0	0	8	4	2	5
0	132	76	0	0	0.640403	0.280968	1.42E+09	1.42E+09	0.458333	0.201667	0	0	0	0	0	0	0	8	4	2	5
0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.017	0.015	0	0	0	0	0	0	0	7	7	2	1
0	142	78	0	0	1.890334	1.610554	1.42E+09	1.42E+09	1.348	1.149333	0	0	0	0	0	0	0	8	4	2	5
0	142	78	0	0	1.780739	1.549507	1.42E+09	1.42E+09	1.269667	1.103667	0	0	0	0	0	0	0	8	4	2	5
0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.018	0.013	0	0	0	0	0	0	0	5	9	2	1
0	364	0	0	0	0	0	1.42E+09	1.42E+09	0.021	0	0	0	0	2	2	0	0	1	1	1	1
1.94E+09	77	1065	1	12026	1170.482	1144.383	1.42E+09	1.42E+09	21.83082	9.570304	0.051475	0.006528	0.044947	0	1	1	0	0	3	2	2	1
2.47E+09	97	45	1	0	18786.71	941.7249	1.42E+09	1.42E+09	183.5793	474.2594	0.066088	0.017959	0.048129	0	1	1	0	0	5	2	2	1
0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.017	0.012	0	0	0	0	0	0	0	0	7	4	1	1
0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.011	0.009	0	0	0	0	0	0	0	0	7	6	1	1
0	66	82	0	0	0	0	1.42E+09	1.42E+09	0.018	0.014	0	0	0	0	0	0	0	0	8	3	1	2
0	73	89	0	0	0	0	1.42E+09	1.42E+09	0.017	0.015	0	0	0	0	0	0	0	0	5	7	1	1
0	73	89	0	0	0	0	1.42E+09	1.42E+09	0.018	0.013	0	0	0	0	0	0	0	3	8	2	1

Fig. 12: Showing the Packet Data Captured in the USNW-NB15 Dataset Cont'd

AS	AT	AU	AV	AW
1	1	2		0
3	2	2		0
3	1	1		0
3	2	2		0
1	1	2		0
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1	Exploits	1
2	1	1	DoS	1
1	1	1	Exploits	1
2	1	1	Exploits	1
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1		0
2	1	1		0
1	1	2		0
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1		0
2	1	1		0
1	1	2		0
1	1	1	Exploits	1
2	1	1		0

Fig. 13: Showing the Packet Data Captured in the USNW-NB15 Dataset Cont'd

The following Dataset snippets captured the various types of attack events as well as their respective number of occurrences and associated protocols/attack sub-category for the recorded period:

Attack category	Attack subcategory	Number of events
normal		2218761
Fuzzers	FTP	558
Fuzzers	HTTP	1497
Fuzzers	RIP	3550
Fuzzers	SMB	5245
Fuzzers	Syslog	1851
Fuzzers	PPTP	1583
Fuzzers	FTP	248
Fuzzers	DCERPC	164
Fuzzers	OSPF	993
Fuzzers	TFTP	193
Fuzzers	DCERPC	455
Fuzzers	OSPF	1746
Fuzzers	BGP	6163
Reconnaissance	Telnet	6
Reconnaissance	SNMP	69
Reconnaissance	SunRPC Portmapper (TCP) UDP Service	2030
Reconnaissance	SunRPC Portmapper (TCP) TCP Service	2026
Reconnaissance	SunRPC Portmapper (UDP) UDP Service	2045
Reconnaissance	NetBIOS	5
Reconnaissance	DNS	35
Reconnaissance	HTTP	1867
Reconnaissance	SunRPC Portmapper (UDP)	2028
Reconnaissance	ICMP	1739
Reconnaissance	SCTP	367
Reconnaissance	MSSQL	5
Reconnaissance	SMTP	6

Fig. 14: Showing the Attack Events of the USNW-NB15 dataset

Axiom to ascertain which fields aligned more accurately to the axiom descriptions.

After completion of substantial qualitative research and analysis. A determination of ideal fields for Risk Profiles were established based on current network traffic data. This was done to establish an idea of the accuracy of a generated Risk profile with existing datafields in MANET traffic. Additionally, proposed meta-data and nominal data fields were introduced and would be covered in the 'Discussion' section. These proposed fields would seek to establish a more accurate Risk Profile calculation.

AS	AT	AU	AV	AW
1	1	2		0
3	2	2		0
3	1	1		0
3	2	2		0
1	1	2		0
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1	Exploits	1
2	1	1	DoS	1
1	1	1	Exploits	1
2	1	1	Exploits	1
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1		0
2	1	1		0
1	1	2		0
1	1	1		0
1	1	1		0
1	1	1		0
1	1	1		0
2	1	1		0
1	1	2		0
1	1	1	Exploits	1
2	1	1		0

Fig. 15: Showing the Attack Events of the USNW-NB15 dataset cont'd

Exploits	SCCP	3
Exploits	SIP	1043
Exploits	TFTP	87
Generic	All	7
Generic	SIP	436
Generic	HTTP	1
Generic	SMTP	247
Generic	IXIA	7395
Generic	TFTP	116
Generic	IXIA	207243
Generic	Superflow	10
Generic	HTTP	5
Generic	TFTP	21
Reconnaissance	DNS	6
Reconnaissance	SMTP	1
Reconnaissance	HTTP	314
Reconnaissance	SNMP	12
Reconnaissance	SunRPC Portmapper (UDP) TCP Service	349
Reconnaissance	MSSQL	1
Reconnaissance	NetBIOS	1
Reconnaissance	SCTP	2
Reconnaissance	SunRPC	2
Reconnaissance	Telnet	1
Reconnaissance	ICMP	26
Reconnaissance	SunRPC Portmapper (TCP) TCP Service	349
Reconnaissance	SunRPC Portmapper (TCP) UDP Service	349
Reconnaissance	SunRPC Portmapper (UDP) UDP Service	346
Shellcode	FreeBSD	8

Fig. 16: Showing the Attack Events of the USNW-NB15 dataset cont'd

III. Methodology

The methodology undertaken was an iterative one which stemmed from the previously mentioned paper [3] which pro-posed an approach for identifying risk levels within MANETS. Several datasets with diverse attributes and situations such as data from:

- Network Intrusion Detection Systems
- Network Intrusion Prevention Systems
- Application layer network traffic
- MANET traffic
- Network (peer to peer, multihop, traditional) traffic
- generated Network traffic datasets from training and
- modeling data

These were subsequently sourced. This was done to gain a current perspective of the available meta-

data fields that are typically captured within network traffic. Based on the identified fields within the datasets, a comparative analysis was then conducted based on the general description of each.

IV. Discussion

The analysis conducted on the datasets led to the determination of the common fields captured within typical network traffic as well as the additional fields that were captured based on the type of traffic being observed. Some realizations that were observed are as follows:

- Datasets varied based on the nature of the traffic being captured.
- Different levels of granularity were observed across the numerous datasets. In terms of what were the typical network traffic fields being captured versus more nominal value fields that were identified by the packet tracers/network monitors.

The results of the assessment conducted on current network data captures revealed that some of the most common network traffic fields identified were:

- Source IP
- Destination IP
- Protocol
- Port
- Length
- Info
- number

Some of the other datafields that were observed from the network data captures were:

- MAC Id
- application protocol
- web service (i.e. http, private, ecoi, https)
- category
- label(distinguishing type of attack experienced)
- service (i.e. http, private, ecoi, https)
- DNS
- attack cat
- label (binary value 0 = normal, 1= attack records)

Based on a general description of Axioms, they form the basis for classifying risk levels within MANETS. Axiom 1 primarily pertained to the device types that are currently on a MANET, apart from observing node behaviours to gauge what type of device they may be, some helpful fields for Axiom 1 would be: *'Source IP', 'Destination IP', 'Protocol', 'MAC Id', 'application protocol', 'label', 'attack cat', 'DNS'*

Axiom 2 would have generally pertained to whether a node is a repeat offender or not and thus, the data fields that would be most useful for determining Axiom2 would be: *'Source IP', 'Destination IP', 'Protocol', 'application protocol', 'label', 'attack cat', 'DNS',* 'category' However, these fields consist of what currently exists in typical Network traffic or IDS traffic data schemas. The addition of the following fields would improve the accuracy of the determined risk level of the given MANET as it would act as additional classification criteria to determine a malicious node, similar to the machine learning classification techniques used in [21] and [22]:

- Axiom 1 - a Binary value of (0= positive, 1= negative)
- Axiom 2 - a Binary value of (0= positive, 1= negative)
- Risk Score - Ranging from 1-5 (1= being very, 2= good, 3= fair, 4= warning, 5= critical)

V. Future Work

The prospective work outlined in this paper involves implementing the Risk Profiles methodology on datasets that align with the current spectrum of Network Traffic fields being recorded. The outcome of this implementation will unveil the present Risk Profile of a designated MANET/Network. A comparative analysis will then be conducted, juxtaposing the existing dataset schema against the proposed fields outlined in the Discussion. This comparative assessment aims to illuminate the accuracy levels in dealing with the limited data fields currently available, as opposed to the introduction of Axioms for refining the precise determination of Risk Profiles.

VI. Conclusion

In conclusion, this paper's research has revealed diverse levels of granularity in the captured data fields of Network/MANET traffic. These nuances in granularity were discerned based on the origin of the network traffic, encompassing MANETs, Mobile Networks, IDS, and IPS. Although many exhibited the conventional dataset fields, noteworthy insights emerged from integrating the previously identified fields within network traffic that readily align with classifiable Axioms. Furthermore, the study established that for an accurate assessment of the current state versus a proposed configuration concerning risk level determination, the classification methods must be applied to the existing datasets. This application involves testing against new datasets that incorporate the Axioms, thereby refining the determination of risk levels specific to MANETs.

References Références Referencias

1. M. Hosein and L. Bigram. "An educational bluetooth quizzing application in Android." International Journal of Wireless and Mobile Networks 5.6 (2013): 69.
2. M. Hosein. "Using Wireless Technology for Quick Distribution of Wireless and Mobile Course Notes and Other Resources." GSTF Journal on Computing Oct2015, Vol4 Issue3, p60-70.

3. D. Granger, and M. Hosein. "WI-FI DIRECT AS A MOBILE STUDENT QUIZZING PLATFORM–A Case Study." Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2018.
4. M Hosein and K Ramdass. "Wi-fi Direct Applications within a Post Covid Classroom–Bridging the Gap between Fully Online and Face to Face Learning." 2022 International Conference on Information Networking (ICOIN), 464-469.
5. J. Aqui and M. Hosein, "Investigating simultaneous wireless connections for a quiz management system-A case study," Global Journal of Computer Science and Technology, pp. 1–11, 2021.
6. J. Aqui and M. Hosein, "An approach to establishing simultaneous server-side connections for NFC/bluetooth enabled Quiz Management Systems," Global Journal of Computer Science and Technology, pp.1–11, 2021.
7. J. Aqui and M. Hosein, "A probabilistic determination of resilience of QMS's simultaneous server-side connections approaches/ methodologies," 2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC), 2021.
8. H. Michael and A. Jedidiah, "Mobile Adhoc Networks - An Overview of Risk Identification, Intrusion Detection and Machine Learning Techniques used," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICMNWC56-175.2022.10031757.
9. J. Aqui and M. Hosein, "Mobile Ad-hoc Networks Topic Modelling and Dataset Querying," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICM-NWC), Tumkur, Karnataka, India, 2022, pp. 1-6, doi: 10.1109/ICM-NWC56175.2022.10031921.
10. A. Jedidiah and H. Michael, "Mobile Adhoc Networks - Establishing Initial Risk Profiles utilizing ML Techniques," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICMNWC561-75.2022.10031628.
11. J. S. Rojas, A. Pekar, A. Rendon, and J. C. Corrales, "Smart user consumption profiling: Incremental learning-based OTT service degradation," IEEE Access, vol. 8, pp. 207426–207442, 2020.
12. T. Sudtasan and H. Mitomo, "Effects of OTT services on consumer's willingness to pay for optical fiber broadband connection in Thailand, "in Proc. 27th Eur. Regional Conf. Int. Telecommun. Soc., 2016, pp. 1–11.
13. V. Carela-Espan˜ol, "Network traffic classification?: From theory to practice," Ph.D. dissertation, Dept. d' Arquitectura Computadors, Univ. Polite`cnica Catalunya, Barcelona, Spain, 2014.
14. I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018.
15. Brown, C., Cowperthwaite, A., Hijazi, A., and Somayaji, A. (2009). Analysis of the 1999 darpa/lincoln laboratory ids evaluation data with netadhict. In 2009 IEEE SCISDA, pages 1–7.
16. S. Mishra, "Network intrusion detection system," Kaggle.com, 18-Nov-2022. [Online]. Available: https://www.kaggle.com/datasets/shalini31mishra/network-intrusion-detection-system. [Accessed: 07-Apr-2023].
17. N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 2015, pp. 1-6, doi: 10.1109/Mil-CIS.2015.7348942.
18. N. Moustafa and J. Slay, "The evaluation of NETWORK ANOMALY DETECTION SYSTEMS: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," Information Security Journal: A Global Perspective, vol. 25, no. 1-3, pp. 18–31, 2016.
19. N. Moustafa, J. Slay and G. Creech, "Novel Geometric Area Analysis Technique for Anomaly Detection Using Trapezoidal Area Estimation on Large-Scale Networks," in IEEE Transactions on Big Data, vol. 5, no. 4, pp. 481-494, 1 Dec. 2019, doi: 10.1109/TBDATA.2017.2715166.
20. N. Moustafa, G. Creech, and J. Slay, "Big Data Analytics for Intrusion Detection System: Statistical decision-making using finite Dirichlet mixture models," Data Analytics and Decision Support for Cybersecurity, pp. 127–156, 2017.
21. A. Mitrokotsa and C. Dimitrakakis, "Intrusion detection in manet using classification algorithms: The effects of cost and model selection," Ad Hoc Networks, vol. 11, no. 1, pp. 226–237, 2013.
22. G. sah, S. Singh, and S. Banerjee, "Intrusion detection system using classification algorithms with feature selection mechanism over real-time data traffic," 2022.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 23 Issue 3 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Mobile Adhoc Networks and Networking-An Overview of Existing Intrusion Prevention Techniques and Predictive Intrusion Prevention

By Michael Hosein & Jedidiah Aqui

University of the West Indies St. Augustine

Abstract- Intrusion Prevention in computer networking refers to the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. It involves actively monitoring network traffic, identifying potential threats or anomalies, and taking action to mitigate or block those threats. In the realms of Mobile Adhoc Networks and computer networking, substantial work has pointed to the gaps experienced with respect to proactively identifying and mitigating risks and network malicious behaviours and attacks. This paper seeks to highlight the existing intrusion detection and prevention techniques currently being utilized in MANETS and general computer networking and how the introduction of the novel Risk Profile approach based on Axiom theory can be utilized or integrated to improve the accuracy of existing models of Intrusion Detection and Prevention systems.

Index Terms: *IDS, IPS, manets, attacks, anomalous, risk, Malicious.*

GJCST-E Classification: *ACM Code: C.2.2*

Strictly as per the compliance and regulations of:

Mobile Adhoc Networks and Networking–An Overview of Existing Intrusion Prevention Techniques and Predictive Intrusion Prevention

Michael Hosein [α] & Jedidiah Aqui [σ]

Abstract- Intrusion Prevention in computer networking refers to the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. It involves actively monitoring network traffic, identifying potential threats or anomalies, and taking action to mitigate or block those threats. In the realms of Mobile Adhoc Networks and computer networking, substantial work has pointed to the gaps experienced with respect to proactively identifying and mitigating risks and network malicious behaviours and attacks. This paper seeks to highlight the existing intrusion detection and prevention techniques currently being utilized in MANETS and general computer networking and how the introduction of the novel Risk Profile approach based on Axiom theory can be utilized or integrated to improve the accuracy of existing models of Intrusion Detection and Prevention systems. With a dual purposed aim of bolstering public confidence in utilizing MANETs and improving the security posture of networks which depend heavily on Security controls to protect their information and assets.

Index Terms: IDS, IPS, manets, attacks, anomalous, risk, Malicious.

I. Introduction

Intrusion prevention, as mentioned previously, refers to the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. Furthermore, the primary goal of network intrusion prevention is to protect the network infrastructure, systems, and data from various types of attacks, such as denial- of- service (DoS) attacks, malware infections, unauthorized access attempts, and network exploits.

While the majority of intrusion detection and prevention systems and frameworks strive to achieve the aforementioned objectives, research highlights a persistent gap in IDPS—specifically, the challenge of accurately predicting and preventing potential future attacks without a notable increase in false positives. Addressing this, there is a crucial demand for the development of predictive intrusion prevention techniques that move beyond reliance solely on knowledge-based approaches derived from past attack types. Instead, there is a call for incorporating probability and risk- based criteria, empowering IDPS to proactively anticipate and thwart potential attacks before their occurrence.

In the investigations detailed in [1], [2] and [3] evidence of a lack of risk based approaches within MANETS were unearthed and a solution founded upon 'Axiom Theory' was developed to provide the probabilistic means required to establish the full picture of risk associated with a MANET and establish an accurate numerical value of Risk associated with the given MANET. In the upcoming papers [4] and [5], the developed solution was tested against current MANET and network traffic which stemmed from numerous real world networks such as:

- Public MANETS
- Military Network Traffic
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Mobile Networks
- VANETS

Whereby it was able to produce accurate representations of risk levels associated with the pertinent networks based on the Axiom criteria used in the Risk Profile formula.

The focus of this paper is to firstly establish the state of contemporary predictive Intrusion Detection and Prevention techniques via the review of literature and related works and secondly to integrate the 'Axiom Based' Risk Profile approach of the previous papers into Intrusion Detection and prevention systems and frameworks to address the aforementioned problem, enable or further bolster the accuracy of their prediction capabilities and establish another layer of controls in accurately addressing risk within Manets and computer Networking with the integration of both impact based and likelihood based data.

II. Literature Review

In this section, we look at the state of the current body of research surrounding MANET and Network predictive intrusion prevention techniques. An overview of the frameworks and systems currently in use will be conducted whereby a comparative analysis and introduction to MANET Risk Profile via axiom theory

Author α σ: Department of Computing and Information Technology University of the West Indies. St. Augustine, Trinidad and Tobago. e-mail: aqui2_jed@yahoo.com

would be discussed in the "Results and Discussion" and "Future Work" section.

In the work done by [6] a review of Network Intrusion Detection Systems (NIDS) was conducted whereby the commonly faced problem of false positives and the generation of a high volume of low-quality alerts was further dissected. This lead to the critical review of the state-of-the- art cyber- attack prediction solution which was based on NIDS Intrusion Alerts, its models and limitations. The solution utilized a technique known as 'intrusion alert correlation (AC) which included similarity-based, statistical- based, knowledge-based, and hybrid-based approaches.

The paper further elaborates that the technique deployed places reliance on raw networking alerts recieved and subsequently seeks to identify the association between different alerts and classifies or contextualize information into their pertinent categories all in an effort to predict a forthcoming alert/attack. The paper highlighted the current state of NIDS post-processing approaches to overcome the limitations of NIDS. The below diagram represents the taxonomy of existing alert correlation approaches which are classified as:

- *Statistical-based:* The basic idea of these approaches is that relevant attacks have similar statistical features, and a proper classification can be found by detecting these similarities.
- *Knowledge-based:* Based on two main components which are, scenario-based approaches to predict multi-step attacks and concequence-based which observe and control implications of alerts and existing knowledge in the network and then predict the security event.
- *Similarity-based:* Defined as the similarity between two alerts or alert clusters. This approach is known to cluster similar alerts in time to reduce the amount of alerts and increase its ability to discover known attacks.

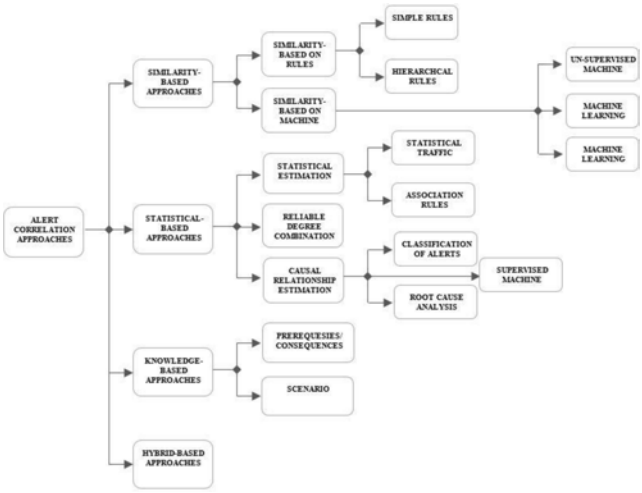

Fig. 1: Showing the taxonomy of Alert Correlation Approaches

As heavy reliance was placed on alerts and alert correlation, to address the limitations of the previously stated model, an alert correlation model was developed to ensure effective, efficient and accurate alerts were utilized for intrusion classification and prediction as shown in the below figure:

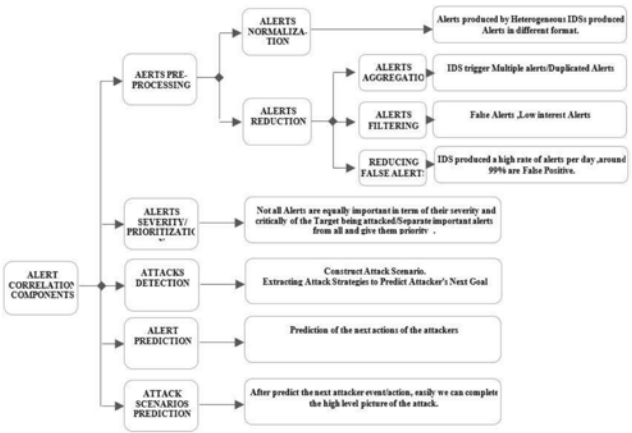

Fig. 2: Showing the Mapping of Alerts Correlation Components with Research Problems

In the work done by [7] another angle to intrusion detection and prevention from the traditional approach was taken. The proposed solution was aimed at cyber-attacks such as Stuxnet [8] and Maroochy [9] which target critical infrastructure to affect physical processes to cause harm. Rather than examine network packet behaviour or the possibility of anamolous behaviour or malicious attacks within the network, this approach utilized a payload analysis-based Intrusion prevention system. The embedded process prediction Intrusion Prevention System (EPPIPS) examined packets that were destined for a programmable Logic Controller (PLC) which interacted with a physical process. If the EPPIPS predicted that these packets or programs were indeed harmful it would potentially prevent or limit the harm.

The paper further postulates that the EPPIPS system acts as a middleman or proxy process within the PLC to act as the innermost layer of defense relative to the PLC in the case of any cyber-attacks. It addresses the immediate risk of a malicious payload that can interact with a Supervisory Control and Data Acquisition (SCADA) system and cause destruction, inefficiencies, and sabotage of cyber-physical systems. The work can be viewed as a variant of existing IDSs and IPSs as it focuses primarily on detecting malicious payloads that are sent to SCADA systems via the programmable Logic Controller. Emphasis is therefore placed on the calculation of possible effects that these malicious payloads can incur on the system and depending on the pertinent risk, possible preventative measures are enforced by the EPPIPS.

The studies done in [10] an examination of the numerous cyber attacks and their increasing frequencies was under- taken. It was noted that despite the existence of advanced cyber-defence systems, attacks and intrusions were still very prevalent. The studies highlighted the current or traditional operations of defence systems which attempt to:

- Block previously known attacks
- Stop ongoing attacks
- Detect occurred attacks

and their inability to minimize the damage caused by an attack which is catastophic. This pointed to the need for not only for improved intrusion detection systems but also intrusion prediction. The paper highlighted the need for more robust intrusion prediction systems by examining and investigating existing intrusion prediction systems as well as the current intrusion detection systems. The usage of improved prediction techniques was proposed with an aim of improving security capabilities for defence systems. The paper primarily sheds light on the gaps of existing intrusion defence systems as well as the necessary improvements required for intrusion prediction systems.

In [11] an ensembles approach towards intrusion detection and prediction was utilized to improve anomaly detection accuracy in a network intrusion environment. The paper indicates that the learning mechanism is based on automated machine learning and the prediction model is based on the Kalman filter. This approach was developed in light of the expeditious rise in the development of network and communication technologies. The paper highlighted that with an increase in pervasive computing networks such as the Internet of Things (IoT), an enormous amount of data is generated.

The data generated is considered to be high-dimensional as it consists of a variety of meta-data fields which pertain to the type of network the data was captured from. Additionally, IoT creates another challenge as diverse datasets which stem from various IoT devices makes it difficult for rule-based approaches for analysis of enormous data. The proposed IDS based on the ensemble of prediction and learning mechanisms is based on autoML. It is based on autoML to address the issue of nonlinear and high dimentional data. The paper highlighted that work had been done in both Convolutional neural networks (CNN) and long short-term memory (LSTM) in separate streams. Whereby, for data nonlinearity has been addressed in CNN and LSTM [12], [13], [14] and high dimensional data in CNN and LSTM are handled by a deep learning paradigm, [15], [16], [17].

The automated neural architecture search paradigm was shown as improving the accuracy of the learning model using parameter optimization and an optimal Kalman filter-based IDS is produced using, measuring and updating errors. It was found that the usage of the o-DNN and Kalman filters together created the ensemble intrusion detection model which was based on the weighted voting mechanism. The below is a conceptual diagram of the ensemble IDS:

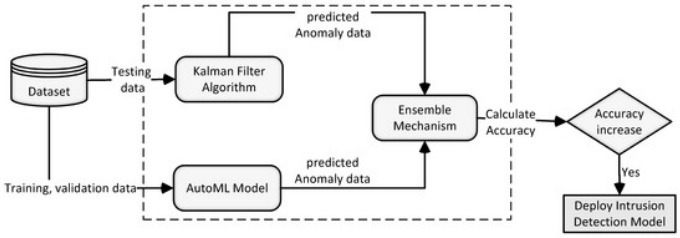

Fig. 3: Showing the Conceptual Diagram of Ensemble of Learning and Prediction Mechanism for Anomaly Detection

The paper [18] focuses on the development of an intrusion prevention system to overcome the static signature detecting mechanisms to identify intruders that exists in all host-based IPSs. This system was proposed within the context of quick evolution of IPS to provide high levels of security such as, which may replace existing security solutions, such as firewalls and anti-viruses. The solution encompasses a four-tier host based IPS that uses data mining technique known as "Decision Tree". This technique is utilized in the capacity of a detecting mechanism in the IPS. The IPS's decision tree consist of choices such as:

- Most infected computer resource by intruders
- Most targeted computer resource by intruders

As opposed to static signature databases. The paper sheds light on three experiments conducted with the proposed solution in an effort to assess the effectiveness of the IPS to classify untruders correctly.

In paper [19] the work explores the absence of widely accepted metrics for assessing information security issues and identifies the lack of empirical data validation as a contributing factor. The authors investigate the potential use of metrics derived from security devices, specifically intrusion detection and prevention system (IDPS) alert events, as indicators of security incidents. By analyzing IDPS data from a large organisation with 40,000 computers, the researchers conducted an empirical case study. The findings suggest that alert characteristics can effectively depict trends in certain security concerns, thereby serving as indicators of security performance. This information can aid security experts in prioritizing security inspections and developing new rules for incident prevention.

The paper did not focus directly on specific intrusion prevention systems but rather the indicators of key security events and incidents. The general approach encompassed analyzing 'big-data' which consisted of security alerts which were captured from 40,000 endpoint devices in the organisation. This paper focuses more on indicators of security performance versus the ability to pro-actively identify and remediate risk within the network.

The research [20] introduces a system called E-NIPS (Event-based Network Intrusion Prediction System) that goes beyond the capabilities of intrusion detection systems (IDSs) by not only detecting attacks but also predicting future potential attacks. The system is designed to partition network penetration scenarios into multiple phases based on the sequence of events during an attack. Each phase consists of attack classes that serve as precursors to attack classes in the subsequent phase. Attack classes represent sets of attacks with similar objectives, enabling generalization of network penetration scenarios and reducing the prediction engine's workload. The prediction of future attacks is based on the detection of attack classes in earlier phases of a penetration scenario.

The proposed automatic intrusion prediction system aims to provide critical time for network fortification, alert networkadministrators about possible attacks, and mitigate the dam- age caused by attacks. The paper describes the architecture, operation, and implementation of E-NIPS, and evaluates a prototype implementation using commonly occurring network penetration scenarios. The experimental results demonstrate that the prototype effectively provides valuable information about the occurrence of future attack events.

Finally, the work done by [21] can be viewed as the closest model towards the proposed predictive intrusion Detection and prevention approach/system of this thesis. The research takes a closer examination on cloud computing and the associated risks involved. The paper goes on to speak on the fact that cloud computing is the new paradigm which exploits already existing computing technologies in a new framework. Therefore alluding that cloud computing also inherited computing problems that are still challenging. The paper focuses on the challenge of cloud computing security as it requires strong security systems to protect the system and the valuable data stored and processed in it.

In addressing the security concerns of cloud computing, the topic of intrusion prevention was explored whereby it was found that typical IDPSs do posses limitations such as:

- Attacks being detected at the time that the damage of the attack was already done.
- Inability to deal with the speed and diversity of emerging cyber threats/attacks.

The proposed solution of this paper involves an Intrusion prediction system which is capable of sensing an attack before it happens in cloud or non-cloud environments. The primary workings of this system ensure 2 core activities:

- Assessing the host systems vulnerabilities
- Monitoring the network traffic for attack preparations.

These core activities are executed in the newly proposed method of statistical selective analysis for network traffic searching for an attack or intrusion indication which forms part of the first module. The second module of the system consists of vulnerability assessements which search for weak-nesses and faults in the identified system and subsequently measures the probability that the system can be compromised via a cyber-attack. And the third module also known as the prediction module performs the combination of outputs from the first and second modules, performs a risk assessment and subsequently gives a reading on the probability of an attack for that given network.

What should be noted with this system, is the method in which risk is calculated as well as the inputs required for a fair-accurate risk calculation. A comparative analysis would be done in the "Discussion" section which dissects the uniqueness of the proposed risk calculation of this paper and the risk profile calculation using axiom theory.

III. Methodology

The methodology deployed in this research of the existing body of studies in the field of:

- Intrusion Prevention systems and methodologies
- Intrusion Prediction systems and methodologies
- Predictive Intrusion Detection and Prevention systems and methodologies

Consist primarily of qualitative research and analysis geared towards further understanding and discussing the current uses and applications of IDS and IDPS systems. Emphasis was placed on the methods and systems that utilized probability or predictive based methods to ascertain risk levels within networks.

This methodology ensured that Risk Management and Risk Predictions and response plans were observed not only in the sphere of MANETS but in the general area of computer networking. The over-arching aim was to establish a position on contemporary IDS and IDPS systems which utilized similar approaches or techniques in ascertain risk levels and further compare this work to the developed "MANET Risk Profile determination via axiom theory" of the current thesis.

The work done can be seen as the foundation for introducing an integration of the "MANET Risk Profile" approach in the realm of general networking as well as an additional layer of control in identifying and proactively remediating potential network threats.

IV. Discussion

Based on the qualitative analysis conducted it was found that there was a plethora of different ways in which intrusion detection and intrusion prediction occurred. It was observed in one approach that primary reliance was placed on intrusion alerts with the aim of identifying associations among alerts, categorizing them accordingly and forming the basis for a more accurate Intrusion Prediction. In this model, this information was identified as an input into an Intrusion Detectionn System (IDS).

In another paper, it was observed that the role of intrusion detection and prevention was primarily focused on malicious attacks that target physical equipment and infrastructure. Instead of the usual approach of examining network traffic and trying to analyze packet behaviour or identify possibly malicious nodes, the paper focused on analyzing malicious payloads that were destined for the programmable Logic Controller in physical machines. The proposed intrusion prevention solution acted as a middleman or an additonal layer of control between transmitted payloads and the PLC of Supervisory control and Data Acquisition (SCADA) equipment.

Furthermore it was observed that other papers utilized a combination of techniques in addressing both the early detection and prevention of intrusions before they occur such as using an ensembles approach which utilized automated machine learning for the threat learning module and Kalman filtering for threat prediction. Another utilized a decision tree methodology whereby the technique was utilized in the capacity of a detecting mechanism in the IPS and some of the choices would have ranged from "most infected computer resource by intruders" to "most targeted computer resource by intruders".

Another noteable approach observed was the usage of event based network intrusion detection, which in design, was aimed at partitioning network penetration scenarios into multiple phases based on the sequence of events during an attack. A subsequent categorization of attacks into attack classes was done and utilized for generalizing network penetration scenarios and further inmproving the efficiency of the system's prediction module. In this approach reliance was placed on network penetration testing activities and results to further bolster the accuracy of attack predictions.

The work conducted can be noted as substantial, however there were some noteable re-occurring themes that were observed and stated below:

- Most of the observed intrusion prediction models were within the domain of general networking and not Mobile Adhoc Networks.
- Most of the identified approaches whilst different methods of executions were observed, they lacked the actual calculation of Risk and correlation to a numerical risk score.

One of the cornerstones of the Axiom Theory Risk Score calculation is the numerical representation of Risk which can subsequently be categorized accordingly and give an accurate picture of risks associated with a given MANET. Of all papers researched, [21] was identified as one of the closest models to the proposed method of risk calculation. Part of the methodology of proactively identifying and implementing controls to prevent attacks on the network was the usage of a risk scoring calculation. Risk was calculated via the below formula:

$$Risk = Ex\ P\ (Th_{\infty})$$

Whereby:

- Ex = The level of exposure
- Th_{∞} = The probability of an absolute threat

This method of Risk calculation assimilated both threat and likelihood factors into the calculation of risk, however when compared to the Axiom Theory Risk Calculation, some stark observations and differences were noted. [19]'s approach was aimed primarily at resolving cloud and to an extent non-cloud intrusions within the domain of a typical cloud or network architecture setup. This setup would comprise of network devices such as:

- Switches
- Routers
- Modems
- Firewalls

This method is not suitable for MANETS as MANETS are infrastructureless and do not consist of a typical network setup but rather interconnected and rapidly changing endpoint nodes.

Another observation was the overhead required to sustain the model would require large amounts of resources for processing of data and analyzing packet behaviour to feed into the prediction module. This type of calculation assumes that the environment would primarily be a cloud environment where resources are easily scalable per network requirements. This may not be suitable for an infrastructureless setup such as manets which have very limited resources and is dynamic.

Whilst the method of acquiring information to generate the risk score was very detailed, a point noted in the score's calculation was that the score would increase by 1 point for every scan performed on a network device. When observed this has the potential to skew the final Risk Score and subsequently skew the prediction results.

When observing the Axiom Theory Risk Profile formula, in its design and also its performance, it was observed that it was easily adaptable to MANETS as it was lighter weight in terms of the inputs required to generate the score as well as easily customizable as Axioms could be added or removed depending on the level of granularity required for the specific MANET.

It was also noted that the Axiom Theory Risk Profile formula had an additional advantage of acting as a second or third layer of defence in organisational networks, due to its level of flexibility and adaptability in terms of the classifying criteria for risk. This means that it can be easily integrated with Next Generation Firewalls (NGFWs) to further bolster the accuracy of intrusion prevention and enforce predictive intrusion prevention based on the Risk Apetite of a given organisation.

V. Conclusion

In summary, this paper's examination underscores the substantial body of work and research in the dynamic field of intrusion detection, prevention, and prediction. Notably, diverse methods have been devised and implemented in various contexts, some geared towards anticipating intrusions, while others focus on fortifying network infrastructure and physical systems reliant on network communications. Despite these advancements, significant gaps persist, particularly in the domain of ascertaining risk scores to enhance the efficacy of predictive intrusion detection and prevention systems. A notable observation is that the majority of predictive methods in this domain are applied in the broader context of general computer networking, lacking specificity tailored to the unique challenges presented by Mobile Ad-Hoc Networks (MANETs). The inherent infrastructureless nature of MANETs adds complexity to enforcing robust risk management compared to traditional network setups with diverse network devices, as discussed. Furthermore, one of the examined papers revealed a method employing a risk score approach in intrusion prediction and prevention. However, upon comparison with the Axiom-based Risk Score methodology, a discernible disparity emerged in its adaptability across various network types and the perceived level of accuracy when juxtaposed with the latter. These findings underscore the need for targeted approaches, specifically tailored to the distinct characteristics of MANETs, to advance the field of predictive intrusion detection and prevention.

VI. Future Work

The Forthcoming Endeavors in this Research Will Entail Seamlessly Integrating the Manet Axiom Theory this Incorporation Signifies an Augmented Layer of Control and Predictive Analysis within Contemporary Predictive Intrusion Detection, Serving as a Proactive Measure to thwart Suspected Attacks. The Primary Context for this Integration is within Corporate Network Settings, Where an Assortment of Intrusion Prevention Systems-Including Network Intrusion Prevention Systems (Nips), Wireless Intrusion Prevention Systems (Wips), and Host Intrusion Prevention Systems (Hips)-is Routinely Employed. This Model is Poised for Smooth Integration into Next-Generation Firewalls (Ngfws), Enhancing their Capacity to Predict and Identify Malicious Network Behavior With Heightened Accuracy and Efficiency. Consequently, it Fortifies the Enforcement of Rules Aimed at Preventing Unauthorized Entry into the Network.

References Références Referencias

1. M. Hosein and J. Aqui, "Mobile Adhoc Networks - An Overview of Risk Identification, Intrusion Detection and Machine Learning Techniques used," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICM-NWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICMNWC56175.2022.10031757.

2. J. Aqui and M. Hosein, "Mobile Ad-hoc Networks Topic Modelling and Dataset Querying," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-6, doi: 10.1109/ICM-NWC56175.2022.10031921.
3. J. Aqui and M. Hosein, "Mobile Adhoc Networks - Establishing Initial Risk Profiles utilizing ML Techniques," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICMNWC 56-175.2022.10031628.
4. J. Aqui and M. Hosein, "Mobile Adhoc Network Risk Profiles An overview of Existing Network Traffic Datasets to determine Ideal Axiom Criteria," unpublished.
5. J. Aqui and M. Hosein, "Mobile Adhoc Network Risk Profiles Establishing MANET and Network Risk Profiles," unpublished.
6. Albasheer, H.; Md Siraj, M.; Mubarakali, A.; Elsier Tayfour, O.; Salih, S.; Hamdan, M.; Khan, S.; Zainal, A.; Kamarudeen, S. Cyber- Attack Prediction Based on Network Intrusion Detection Systems for Alert Correlation Techniques: A Survey. Sensors 2022, 22, 1494. https://doi.org/10.3390/s22041494.
7. A. W. Werth and T. H. Morris, "Intrusion prevention for payloads against cyber-physical systems by predicting potential impacts," Journal of Cyber Security Technology, vol. 6, no. 3, pp. 113–148, 2022. doi:10.1080/23742917.2022.2088113
8. R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," IEEE Security and amp;amp; Privacy Magazine, vol. 9, no. 3, pp. 49–51, 2011. doi:10.1109/msp.2011.67
9. M. Abrams and J. Weiss, "Malicious control system cyber security attack case study: Maroochy Water Services, Australia," MITRE.
10. M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, Information Fusion for Cyber-Security Analytics. SPRINGER INTERNATIONAL PU, 2018.
11. Imran, F. Jamil, and D. Kim, "An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments," Sustainability, vol. 13, no. 18, p. 10057, 2021. doi:10.3390/su131810057.
12. Y. Jiang, F. Yang, H. Zhu, D. Zhou, and X. Zeng, "Nonlinear CNN: Improving cnns with quadratic convolutions," Neural Computing and Applications, vol. 32, no. 12, pp. 8507–8516, 2019. doi:10.1007/s00521019-04316-4
13. J. Gonzalez and W. Yu, "Non-linear system modeling using LSTM Neural Networks," IFAC-PapersOnLine, vol. 51, no. 13, pp. 485–489, 2018. doi:10.1016/j.ifacol.2018.07.326.
14. Y. Tan et al., "LSTM-based anomaly detection for non-linear dynamical system," IEEE Access, vol. 8, pp. 103301–103308, 2020. doi:10.1109/access.2020.2999065.
15. P. Shamsolmoali, D. Kumar Jain, M. Zareapoor, J. Yang, and M. Afshar Alam, "High-dimensional multimedia classification using deep CNN and extended residual units," Multimedia Tools and Applications, vol. 78, no. 17, pp. 23867–23882, 2018. doi:10.1007/s11042-018-6146-7.
16. O. Cheikhrouhou et al., "One-dimensional CNN approach for ECG arrhythmia analysis in fog-cloud environments," IEEE Access, vol. 9, pp. 103513–103523, 2021. doi:10.1109/access.2021.3097751.
17. K. Praanna, S. Sruthi, K. Kalyani, A. S.Tejaswi, "A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data," J. Inf. Comput. Sci. 2020, 10, 1362–1370.
18. A. Al-hamami and T. Alawneh, "Developing a host intrusion prevention system by using Data Mining," 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2012. doi:10.1109/acsat.2012.103.
19. R. S. Miani, B. B. Zarpelao, B. Sobesto, and M. Cukier, "A practical experience on evaluating intrusion prevention system event data as indicators of security issues," 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), 2015. doi:10.1109/srds.2015.17.
20. P. Kannadiga, M. Zulkernine, and A. Haque, "E-NIPS: An event based network intrusion prediction system," Lecture Notes in Computer Science, pp. 37–52. doi:10.1007/978-3-540-75496-1.3.
21. "Intrusion prediction system for cloud computing and network based systems," Guide books, https://dl.acm.org/doi/book/10.5555/AAI28329182 (accessed Jul. 13, 2023).

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 23 Issue 3 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Mobile Adhoc Networks and Networking – Integrating Risk Profiles into Intrusion Prevention Systems to Improve Predictive Intrusion Prevention

By Aqui Jedidiah & Hosein Michael

University of the West Indies St. Augustine

Abstract- Intrusion Prevention in computer networking refers to the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. It involves actively monitoring network traffic, identifying potential threats or anomalies, and taking action to mitigate or block those threats. In the realms of Mobile Adhoc Networks and general computer networking, substantial work has pointed to the gaps experienced with respect to proactively identifying and mitigating risks and network malicious behaviours and attacks. Further research was conducted to establish the current state of contemporary intrusion detection, prediction and prevention techniques and their effectiveness to pro-actively identify and mitigate network attacks and malicious activity. However, it was found that the techniques utilized were very few or required futher accuracy improvements and for the identified effective techniques, they required substantial amount of data processing power and a robust network architecture to support its implementation.

Index Terms: *IDS, IPS, manets, attacks, anomalous, risk, malicious, prediction.*

GJCST-E Classification: *ACM Code: C.2.0*

Strictly as per the compliance and regulations of:

Mobile Adhoc Networks and Networking – Integrating Risk Profiles into Intrusion Prevention Systems to Improve Predictive Intrusion Prevention

Aqui Jedidiah [α] & Hosein Michael [σ]

Abstract- Intrusion Prevention in computer networking refers to the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. It involves actively monitoring network traffic, identifying potential threats or anomalies, and taking action to mitigate or block those threats. In the realms of Mobile Adhoc Networks and general computer networking, substantial work has pointed to the gaps experienced with respect to proactively identifying and mitigating risks and network malicious behaviours and attacks. Further research was conducted to establish the current state of contemporary intrusion detection, prediction and prevention techniques and their effectiveness to pro-actively identify and mitigate network attacks and malicious activity. However, it was found that the techniques utilized were very few or required futher accuracy improvements and for the identified effective techniques, they required substantial amount of data processing power and a robust network architecture to support its implementation. The work of this paper, introduces the integration of the MANET Risk Scoring methodology based on Axiom theory into the realm of general networking. All in an effort to increase the efficiency and accuracy of existing predictive intrusion prevention systems such as next generation Firewalls in corporate networks.

Index Terms: *IDS, IPS, manets, attacks, anomalous, risk, malicious, prediction.*

I. Introduction

Intrusion Prevention as mentioned previously in the abstract, involves the set of techniques and technologies used to detect and prevent unauthorized access, malicious activities, and attacks on a network. The common or normal uses of typical intrusion detection and prevention systems saw the usage of techniques to detect attacks and prevent their effects after occurrence within a given network. This however was viewed as a short-comming of these models of intrusion detection and prevention systems as their response times were inadequate and often occurred after damage was already done to the existing network infrastructure.

Author α σ: Department of Computing and Information Technology University of the West Indies St. Augustine, Trinidad and Tobago.
e-mail: aqui2_jed@yahoo.com

According to papers [1] and [2] the general reactive approach to intrusion detection and prevention was due to a lack of risk-based studies and the prevalence of impact-based studies in the realm of mobile adhoc networks (MANETS). This view was seen as as siloed and thus to address this gap, a solution founded upon 'Axiom Theory' was developed in [3]. This theory proved vital for solving the issues of probability-based approaches in addressing risk within manets and creating a new model for predictive intrusion prediction and prevention for MANETS.

After the probabilistic method of risk score generation for MANETS was established in [3], it was then tested on several real-world network traffic and Manet datasets as per the work of [4] and [5] which would have stemmed from various sources such as, *Public MANETS, Military Network Traffic, Intrusion Detection Systems, Intrusion Prevention Systems, Mobile Networks, VANETS*. The results produced a Risk Profile or Risk Score(a numerical representation of risk) followed by a classification criteria for the given MANET in question and also established a new and accurate lightweight method for risk calculation for infrastructure-less networking setups such as MANETS.

The prospects of having an easily scalable method of calculating risks within MANETS also posed a new method or in some cases another layer of control within general network studies surrounding predictive intrusion detection and prevention. The work of [6] saw an overview of existing predictive network intrusion detection and prevention systems and techniques. It was found that whilst there were various ways in which systems predicted netwoork intrusions or malicious behaviour there was little to no systems in place to accurately predict and prevent an attack before it occurred on the network with the exception of one [7] which undertook a similar methodology but was seen as not easily adoptable or scalable for different networking contexts.

The work of this paper focuses on proposing a method to integrate the axiom-theory risk score calculation methodology into the field of general networking which speaks to typical network setups

which consists of many tools and devices both hardware and software that make up the network. It also disects the key diffrerences in approaches deployed in [7] and the proposed system to address the issue of scalability, practicality and applicability to a plethora of varying networks.

II. Literature Review

In this section, a summary of the previous research conducted in [6] is stated as this paper's work can be viewed as the proposition of the solution to address the gaps identified in the previous paper.

In the work done by [8] a review of Network Intrusion Detection Systems (NIDS) was conducted whereby the commonly faced problem of false positives and the generation of a high volume of low-quality alerts was further dissected. This lead to the critical review of the state-of-the-art cyber- attack prediction solution which was based on NIDS Intrusion Alerts, its models and limitations. The solution utilized a technique known as 'intrusion alert correlation (AC) which included similarity-based, statistical-based, knowledge-based, and hybrid-based approaches.

In the work done by [9] another angle to intrusion detection and prevention from the traditional approach was taken. The proposed solution was aimed at cyber-attacks such as Stuxnet [10] and Maroochy [11] which target critical infrastructure to affect physical processes to cause harm. Rather than examine network packet behaviour or the possibility of anamolous be- haviour or malicious attacks within the network, this approach utilized a payload analysis-based Intrusion prevention sys- tem. The embedded process prediction Intrusion Prevention System (EPPIPS) examined packets that were destined for a programmable Logic Controller (PLC) which interacted with a physical process. If the EPPIPS predicted that these packets or programs were indeed harmful it would potentially prevent or limit the harm.

The studies done in [12] an examination of the numerous cyberattacks and their increasing frequencies was under- taken. It was noted that despite the existence of advanced cyber-defence systems, attacks and intrusions were still very prevalent. The studies highlighted the current or traditional operations of defence systems which attempt to:

- Block previously known attacks
- Stop ongoing attacks
- Detect occurred attacks

and their inability to minimize the damage caused by an attack which is catastophic.

In [13] an ensembles approach towards intrusion detection and prediction was utilized to improve anomaly detection accuracy in a network intrusion environment. The paper indicates that the learning mechanism is based on automated machine learning and the prediction model is based on the Kalman filter. This approach was developed in light of the expeditious rise in the development of network and communication technologies. The paper spoke to the increase in pervasive computing networks such as the Internet of Things (IoT), which generated an enormous amount of data which is considered high-dimensional as it consisted of a variety of meta-data fields. This created a challenge for rule-based approaches to analyse the data.

The proposed IDS based on the ensemble of prediction and learning mechanisms is based on autoML. It is based on autoML to address the issue of nonlinear and high dimentional data. The paper highlighted that work had been done in both Convolutional neural networks (CNN) and long short-term memory (LSTM) in separate streams. Whereby, for data nonlinearity has been addressed in CNN and LSTM [14], [15], [16] and high dimensional data in CNN and LSTM are handled by a deep learning paradigm, [17], [18], [19].The automated neural architecture search paradigm was shown as improving the accuracy of the learning model using parameter optimization and an optimal Kalman filter-based IDS is produced using, measuring and updating errors. It was found that the usage of the o-DNN and Kalman filters together created the ensemble intrusion detection model which was based on the weighted voting mechanism.

The paper [20] focused on the development of an intrusion prevention system to overcome the static signature detecting mechanisms to identify intruders that exists in all host-based IPSs. This system was proposed within the context of quick evolution of IPS to provide high levels of security such as, which may replace existing security solutions, such as firewalls and anti-viruses. The solution encompasses a four- tier host based IPS that uses data mining technique known as *"Decision Tree"*. This technique is utilized in the capacity of a detecting mechanism in the IPS. The IPS's decision tree consist of choices such as:

- Most infected computer resource by intruders
- Most targeted computer resource by intruders

As opposed to static signature databases. The paper sheds light on three experiments conducted with the proposed solution in an effort to assess the effectiveness of the IPS to classify untruders correctly.

In paper [21] the work explored the absence of widely accepted metrics for assessing information security issues and identifies the lack of empirical data validation as a contributing factor. The authors investigated the potential use of metrics derived from security devices, specifically intrusion detection and prevention system (IDPS) alert events, as indicators of security incidents. By analyzing IDPS data from a large organisation with 40,000 computers, the researchers conducted an empirical case study. The findings

suggested that alert characteristics can effectively depict trends in certain security concerns, thereby serving as indicators of security performance. This paper focuses more on indicators of security performance versus the ability to pro-actively identify and remediate risk within the network.

The research [22] introduced a system called E-NIPS (Event-based Network Intrusion Prediction System) that went beyond the capabilities of intrusion detection systems (IDSs) by not only detecting attacks but also predicting future potential attacks. The system was designed to partition network penetration scenarios into multiple phases based on the sequence of events during an attack. Each phase consisted of attack classes that served as precursors to attack classes in the subsequent phase. Attack classes represented sets of attacks with similar objectives, enabling generalization of network penetration scenarios and reducing the prediction engine's workload. The prediction of future attacks was based on the detection of attack classes in earlier phases of a penetration scenario. The proposed automatic intrusion prediction system aimed to provide critical time for network fortification, alert network administrators about possible attacks, and mitigate the damage caused by attacks.

III. Methodology

The methodology of the proposed solution is envisioned within the context of an enterprise network. Two main approaches would be considered.

Approach 1: whereby the Axiom Theory predictive intrusion prevention system is placed before the enterprise's edge firewall as the first line of defence.

Approach 2: whereby the Axiom Theory predictive intrusion prevention system is placed after the enterprise's edge firewall as the second line of defence.

The primary technique of intrusion prevention utilized within this context is known as.

- *Policy Based - Intrusion Prevention*- This method employs security policies defined by the enterprise and blocks activity that violates those policies. This requires an administrator to set up and configure security policies.

There would also be to a lesser extent some elements of 2 other types of intrusion prevention techniques known as.

- *Signature Based - Intrusion Prevention* - This method matches the activity to signatures of well-known threats. However, one of the main drawbacks to this method is that it can only stop previously identified attacks and won't be able to recognize new ones.
- *Anomaly-based - Intrusion Prevention* - This method monitors for abnormal behavior by comparing random samples of network activity against a baseline standard. It is more robust than signature-based monitoring, but it can sometimes produce false positives.

However, the principle reason for utilizing a policy-based technique is due to the fact that the Axiom-Based approach for risk categorization acts as the first layer of defence before reaching the enterprise's firewall according to Approach 1. The following figure 1 is an example of an enterprise network layout.

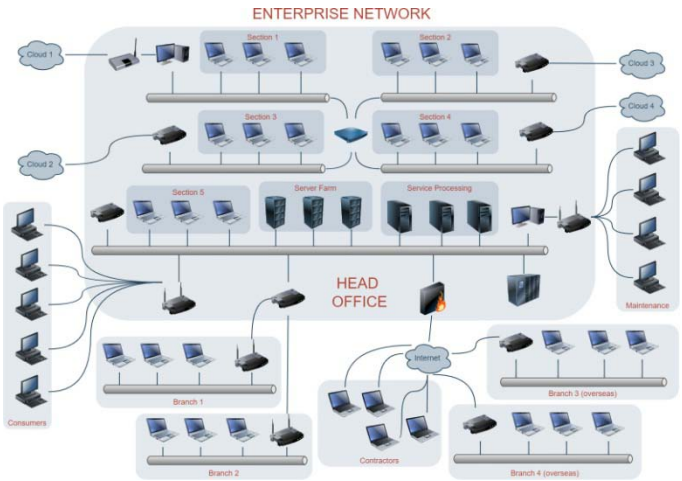

Fig. 1: Showing an Enterprise Network Setup

Approach 1

With the implementation of Approach 1, the enterprise network would now contain a change to the topology specifically between the internet and the firewall as shown in the below figure 2:

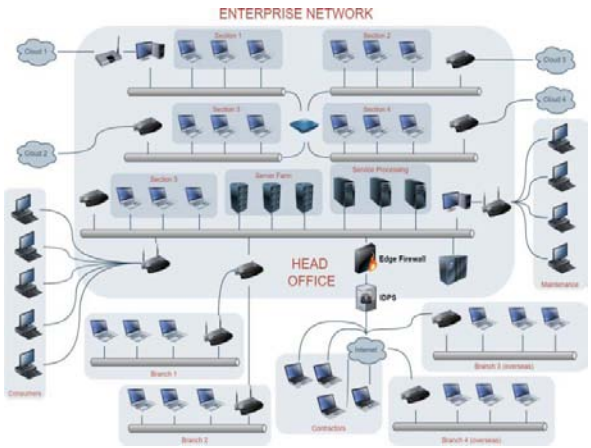

Fig. 2: Showing an Enterprise Network Setup - Approach 1

This change is necessary as the IDPS would act as the first line of defence and begin filtering and categorizing network packets entering the Head Office of the enterprise. This therefore allows the firewall to undertake a policy-based approach to incoming network traffic as it can now add additional rule categories to allow/prevent network traffic with a risk score of a particular value.

In this approach the IDPS would generate risk scores for incoming traffic and this in turn would be filtered to the firewall for processing and decision making for entry into the network. This alludes that the IDPS acts as the first-line of defence in the capacity of classifying incoming network traffic based on the defined Axioms, with the most generic axioms identifying malicious and anomalous packet behaviours and/or device types which are trying to send traffic to the internal network.

In approach 1's application of the axiom-based IDPS, the predictive capabilities are coined with the functions of the edge firewall to prevent attacks or malicious activity from causing harm to the network pro-actively. This also forms the basis of next generation firewalls which integrate with Intrusion detection and prevention systems.

Approach 2

With the implementation of Approach 2, the enterprise network would now contain a change to the topology specifically between the edge firewall and the Enterprise network as shown in the below figure 3:

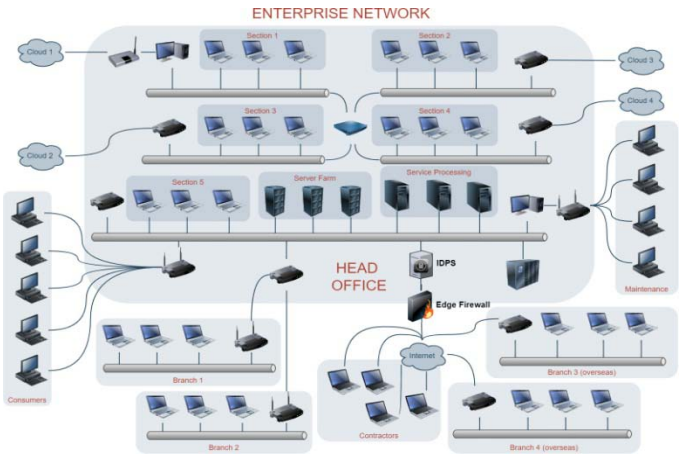

Fig. 3: Showing an Enterprise Network Setup - Approach 3

In this approach the IDPS acts as the second line of defence within the network and takes on the role of classifying risk and remediating accordingly as per risk apetite. Being the second line of defence means that there is a lesser chance of encountering network traffic that qualifies for any of the prescribed axioms. However, as the firewall aligns primarily with the Policy-based method of intrusion detection, this scenario allows for the IDPS to leverage both the Signature based and Anomaly Based methods of intrusion prevention more.

By leveraging both of these methods, it allows for the second line of defence within the network to continue performing background checks and/or

forensics whilst the firewall un- dertakes the majority of overhead in filtering and preventing malicious network traffic from entering. The combination of both the firewall and IDPS within this capacity also makes for a substantially stronger Network Architecture as the components work in parallel similar to next-generation firewalls.

IV. Discussion

In the "Methodology" section, it was observed that two (2) main approaches were proposed for the usage of the Axiom Theory predictive intrusion detection and prevention within the context of an Enterprise Network. They consisted of:

Approach 1: The Intrusion Detection and Prevention System was placed before the edge firewall, situated between the internet and the firewall as the first line of defence within the network.

Approach 2: The Intrusion Detection and Prevention System was placed after the firewall, situated between the edge firewall and the enterprise network as the second line of defence within the network.

Before delving further into both approaches however, the observations noted from the system implemented in [7] must be discussed. The paper [7] was noted as having a similar approach by way of establishing a risk score and categorizing Risk based on criteria of a heat map. Whilst the work was substantial, some stark differences and/or gaps were noted with respect to this approach and the proposed axiom solution:

- The solution was developed primarily for predicting and mitigating cloud security events and to an extent non- cloud security events.
- The solution was not easily deployable for varying Network Architectures such as VANETS, MANETS or peer to peer network as it required substantial meta-data to calculate the risk score.
- The solution requires considerable compute power for big data processing as it consists of 2 main modules for assessing the host's vulnerabilities and monitoring attack preparations within the network
- Whilst the method of acquiring information to generate the risk score was very detailed, a point noted in the score's calculation was that the score would increase by 1 point for every scan performed on a network device. When observed this has the potential to skew the final Risk Score and subsequently skew the prediction results.

The Axiom-Based Risk Profile approach answers the concerns and shortcommings of the aforementioned gaps not only within the situation of Mobile Ad-Hoc networks and Vehicular Ad-Hoc networks but by merit of the previously stated approaches 1 and 2 it is easily integrateable with differing Network Architectures. This is possible because of the light- weight but accurate nature of the solution, the original design was primarily catering to the security needs of infrastructure- less networks such as MANETS. The aforementioned approaches 1 and 2 were examples of its integration within an Enterprise Network setting to further enhance the proactive security risk mitigation capabilities.

When observing Approach 1, it is noted that the role the proposed predictive IDPS (PIDPS) is more on the basis of classifying malicious/anomalous network behaviour, nodes and activities to inform the edge firewall. The predictive capability and pro-active prevention of network attacks is enforced by the egde firewall based on the Axiom criteria that it is allowed and prevented in its policy-based rule-sets which dictate the decision making process. In this approach the core function of the IDPS is predictive detection and informing for subsequent action-taking.

However, Approach 1 can also be used in another dynamic whereby the overhead is utilized by the IDPS to not only observe and classify network events and behaviours but also to execute the pertinent actions required based on the network traffic risk-levels. By enforcing this strategy, much overhead is reduced on the firewall as the heavy processing occurs at the IDPS level firstly. Axiom theory, allows for the scalability of processing of the risk classification approach by adding to the pool of axioms for classifying data. In other words the IDPS can both proactively detect and prevent malicious and anomalous network activity without the intervention of the firewall.

When observing Approach 2, it is noted that the role of the PIDPS centers on the basis of the traffic entering the network after passing through the edge-firewall. The majority of traffic processing is handled by the edge-firewall. This means that risk classification would occur at the second layer of defence as opposed to the first, by this occurring, the PIDPS acts as a secondary control before traffic enters and leaves the network. This means that greater levels of forensics and data processing can occur in the background as most of the processing of incoming traffic is handled by the firewall. It also means that machine learning techniques for network data processing is much more feasible with this approach as the PIDPS can be utilized to further bolster the resilience of the Network's Security posture and also form the basis for more accurate firewall ruleset updates based on new/emerging threats.

Approach 2 also allows for the classification of risk per-taining to network traffic leaving the Enterprise network. This therefore means that in the event a malicious user was able to infaltrate the Enterprise's network, the PIDPS is likely to identify this behaviour, classify and prevent from leaving the network and/or traversing the Network's Architecture to infect or affect other Network devices and services.

V. Conclusion

In conclusion, the research underscores the substantial benefits of incorporating the MANET Axiom Theory Risk Calculation methodology into the domain of Enterprise Networking. The comparative analysis revealed that both proposed approaches (1 and 2) of the Predictive Intrusion Detection and Prevention System (PIDPS) introduce an additional layer of control within the Enterprise's Network. Furthermore, they effectively address the limitations identified in a cloud-based approach that employs a similar technique-deriving a risk score, categorizing risk, and leveraging this information to predict and prevent intrusions in a network. A standout feature of the Axiom-Theory approach is its notable adaptability and scalability. This characteristic allows its application to transcend the constraints of infrastructure-less networking, extending its utility to general networking topologies that comprise numerous network devices and software. This versatility implies that enhancing the predictive detection and prevention of network threats can be achieved with heightened accuracy and scalability, tailoring the methodology to meet the specific requirements of diverse networks.

VI. Future Work

The future trajectory of this research will involve the implementation of the proposed approaches to seamlessly integrate Axiom-Based Risk Calculation into a standard network architecture. This signifies a crucial advancement, serving as the next phase in augmenting the capabilities of "next-generation firewalls" to anticipate and thwart network intrusions. Beyond fortifying firewall capabilities, this endeavor is positioned as an essential system/methodology designed to rectify the deficiency of accurate risk-based data, which is pivotal for synergizing with impact-based data in the realm of Network Security.

The overarching objective is to develop a functional model or prototype for implementation within an Enterprise Network. Subsequent to this development, rigorous testing will ensue to assess the accuracy of the generated results. This testing phase is integral in evaluating and quantifying the effectiveness of seamlessly integrating the innovative risk-based approach into the broader landscape of general networking.

References Références Referencias

1. M. Hosein and J. Aqui, "Mobile Adhoc Networks - An Overview of Risk Identification, Intrusion Detection and Machine Learning Techniques used," 2022 IEEE 2nd International Conference on Mobile Net-works and Wireless Communications (ICMNWC), Tumkur, Karnataka,India,2022,pp.1-5,doi:10.1109/ICMNWC56175.2022.10031757.
2. J. Aquiand M. Hosein,"Mobile Ad-hoc Networks Topic Modelling and Data set Querying, "2022IEEE 2nd International Con-ference on Mobile Networks and Wireless Communications (ICM-NWC), Tumkur, Karnataka, India, 2022, pp. 1-6, doi: 10.1109/ICM-NWC56175.2022.10031921.
3. J. Aqui and M. Hosein, "Mobile Adhoc Networks - Establishing InitialRisk Profiles utilizing ML Techniques," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICM-NWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICM-NWC56175.2022.10031628.
4. J. Aquiand M. Hosein, "Mobile Adhoc Network Risk Profiles- An overview of Existing Network Traffic Datasets to determine Ideal Axiom Criteria, "unpublished.
5. J. Aquiand M. Hosein, "Mobile Adhoc Network Risk Profiles-Establishing MANET and Network Risk Profiles, "unpublished.
6. M. Hoseinand J. Aqui, "Mobile Adhoc Networks and Networking – An overview of Existing Intrusion Prevention techniques and predictive intrusion prevention, "unpublished.
7. "Intrusion prediction system for cloud computing and network based systems, "Guidebooks, https://dl.acm.org/doi/book/10.5555/AAI28329182. (access-ed Jul.13,2023).
8. Albasheer, H.; Md Siraj, M.; Mubarakali, A.; Elsier Tayfour, O.; Salih, S.; Hamdan, M.; Khan, S.; Zainal, A.; Kamarudeen, S. Cyber-Attack Prediction Based on Network Intrusion Detection Systems for Alert Correlation Techniques: A Survey. Sensors 2022, 22,1494.https://doi.org/10.3390/s22041494.
9. A. W. Werth and T. H. Morris, "Intrusion prevention for pay loads against cyber-physical systems by predicting potential impacts, "Journal of Cyber Security Technology, vol. 6, no.3, pp.113–148, 2022. doi:10.1080/23742917.2022.2088113.
10. R. Langner, "Stuxnet: Dissecting a cyber warfare weapon," IEEE Security and amp; amp; Privacy Magazine, vol. 9, no. 3, pp. 49–51, 2011. doi:10.1109/msp.2011.67
11. M. Abrams and J. Weiss, "Malicious control system cyber security attack case study: Maroochy Water Services, Australia, "MITRE.
12. M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, Information Fusion for Cyber-Security Analytics. SPRINGER INTERNATIONAL PU, 2018.
13. Imran, F. Jamil, and D. Kim, "An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments," Sustainability, vol. 13, no. 18, p. 10057, 2021.doi:10.3390/su131810057.

14. Y. Jiang, F. Yang, H. Zhu, D. Zhou, and X. Zeng, "Nonlinear CNN: Improving cnns with quadratic convolutions," Neural Computing and Applications, vol. 32, no. 12, pp. 8507–8516, 2019. doi: 10.1007/s00521-019-04316-4.
15. J. Gonzalez and W. Yu, "Non-linear system modeling using LSTM Neural Networks," IFAC-Papers OnLine, vol. 51, no. 13, pp. 485–489, 2018. doi:10.1016/j.ifacol.2018.07.326.
16. Y. Tanetal.,"LSTM-based anomaly detection for non-lineardy-namical system, "IEEE Access, vol. 8, pp. 103301–103308, 2020. doi: 10.1109/access.2020.2999065.
17. P. Sham solmoali, D. Kumar Jain, M. Zareapoor, J. Yang, and M. Afshar Alam, "High-dimensional multimedia classification using deep CNNand extended residual units," Multimedia Tools and Applications, vol.78,no.17, pp.23867–23882, 2018. doi:10.1007/s11042-018-6146-7.
18. O. Cheikhrouhou et al., "One-dimensional CNN approach for ECGarrhythmia analysis in fog-cloud environments," IEEE Access, vol. 9, pp.103513–103523, 2021.doi:10.1109/access.2021.3097751.
19. K. Praanna, S. Sruthi, K. Kalyani, A. S. Tejaswi, "A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data, "J. Inf. Comput. Sci. 2020,10,1362–1370
20. A. Al-hamami and T. Alawneh, "Developing a host intrusion prevention system by using Data Mining, "2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2012. doi:10.1109/acsat.2012.103.
21. R. S. Miani, B. B. Zarpelao, B. Sobesto, and M. Cukier, "A practical experience one valuating intrusion prevention system event data as indicators of security issues," 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), 2015. doi: 10.1109/srds.2015.17.
22. P. Kannadiga, M. Zulkernine, and A. Haque, "E-NIPS: Anevent-based network intrusion prediction system,"Lecture Notes in Computer Science, pp.37–52. doi: 10.1007/978-3-540-75496-1.3.
23. 'Intrusion prediction system for cloud computing and network based systems, "Guide books, https://dl.acm.org/doi/book/10.5555/AAI28-329182 (accessed Jul.13).

Global Journals Guidelines Handbook 2023

www.GlobalJournals.org

Memberships

Fellows/Associates of Computer Science Research Council

FCSRC/ACSRC Memberships

Introduction

FCSRC/ACSRC is the most prestigious membership of Global Journals accredited by Open Association of Research Society, U.S.A (OARS). The credentials of Fellow and Associate designations signify that the researcher has gained the knowledge of the fundamental and high-level concepts, and is a subject matter expert, proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice. The credentials are designated only to the researchers, scientists, and professionals that have been selected by a rigorous process by our Editorial Board and Management Board.

Associates of FCSRC/ACSRC are scientists and researchers from around the world are working on projects/researches that have huge potentials. Members support Global Journals' mission to advance technology for humanity and the profession.

FCSRC

Fellow of Computer Science Research Council

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL is the most prestigious membership of Global Journals. It is an award and membership granted to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Fellows are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Fellow Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A FCSRC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Fellows can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Fellows receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Fellows can use the honored title of membership. The “FCSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FCSRC or William Walldroff, M.S., FCSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Fellow members of FCSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All fellows get a dedicated page on the website with their biography.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Fellows receive discounts on future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Fellows get secure and fast GJ work emails with unlimited forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, fellows receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Fellows are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All fellows receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 60% of sales proceeds

Fellows can publish articles (limited) without any fees. Also, they can earn up to 70% of sales proceeds from the sale of reference/review books/literature/publishing of research paper. The FCSRC member can decide its price and we can help in making the right decision.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Fellow members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

Access to Editorial Board

Become a member of the Editorial Board

Fellows may join as a member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. Additionally, Fellows get a chance to nominate other members for Editorial Board.

Career | Credibility | Exclusive | Reputation

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 5 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 10 GB free secure cloud access for storing research files.

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL is the membership of Global Journals awarded to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Associate membership can later be promoted to Fellow Membership. Associates are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Associate Members.

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A ACSRC member gets access to a closed network of Tier 2 researchers and scientists with direct communication channel through our website. Associates can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Associates receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Associates can use the honored title of membership. The “ACSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., ACSRC or William Walldroff, M.S., ACSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Associate members of ACSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Associates receive discounts on future publications with Global Journals up to 30%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Associates get secure and fast GJ work emails with 5GB forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, associates receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Associates are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All associates receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 30-40% of sales proceeds

Associates can publish articles (limited) without any fees. Also, they can earn up to 30-40% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Associate members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 2 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 5 GB free secure cloud access for storing research files.

Associate	Fellow	Research Group	Basic
$4800 **lifetime designation**	$6800 **lifetime designation**	$12500.00 **organizational**	APC **per article**
Certificate, LoR and Momento **2** discounted publishing/year **Gradation** of Research **10** research contacts/day **1 GB** Cloud Storage **GJ** Community Access	**Certificate,** LoR and Momento **Unlimited** discounted publishing/year **Gradation** of Research **Unlimited** research contacts/day **5 GB** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**Certificates,** LoRs and Momentos **Unlimited** free publishing/year **Gradation** of Research **Unlimited** research contacts/day **Unlimited** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**GJ** Community Access

Preferred Author Guidelines

We accept the manuscript submissions in any standard (generic) format.

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from https://globaljournals.org/Template.zip

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at submit@globaljournals.org or get in touch with chiefeditor@globaljournals.org if they wish to send the abstract before submission.

Before and during Submission

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct,* along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author's email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s') names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

Policy on Plagiarism

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors' institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures

- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

Authorship Policies

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

Preparing your Manuscript

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.

Manuscript Style Instruction (Optional)

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11'", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

Structure and Format of Manuscript

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

a) A title which should be relevant to the theme of the paper.
b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
d) An introduction, giving fundamental background objectives.
e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
f) Results which should be presented concisely by well-designed tables and figures.
g) Suitable statistical data should also be given.
h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
j) There should be brief acknowledgments.
k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.

Format Structure

It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

All manuscripts submitted to Global Journals should include:

Title

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

Author details

The full postal address of any related author(s) must be specified.

Abstract

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Keywords

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, “What words would a source have to include to be truly valuable in a research paper?” Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

Numerical Methods

Numerical methods used should be transparent and, where appropriate, supported by references.

Abbreviations

Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

Formulas and equations

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

Tables, Figures, and Figure Legends

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.

Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

Preparation of Eletronic Figures for Publication

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

Color charges: Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

Tips for writing a good quality Computer Science Research Paper

Techniques for writing a good quality computer science research paper:

1. Choosing the topic: In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

2. Think like evaluators: If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

3. Ask your guides: If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

4. Use of computer is recommended: As you are doing research in the field of computer science then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

5. Use the internet for help: An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.

6. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

7. Revise what you wrote: When you write anything, always read it, summarize it, and then finalize it.

8. Make every effort: Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

9. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

10.Use proper verb tense: Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

11. Pick a good study spot: Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

12. Know what you know: Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

13. Use good grammar: Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

14. Arrangement of information: Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

15. Never start at the last minute: Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

16. Multitasking in research is not good: Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

17. Never copy others' work: Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

18. Go to seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

19. Refresh your mind after intervals: Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.

20. Think technically: Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

21. Adding unnecessary information: Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

22. Report concluded results: Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

23. Upon conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

Final points:

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

The introduction: This will be compiled from reference matter and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

The discussion section:

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear: Adhere to recommended page limits.

Mistakes to avoid:

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.
- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

Title page:

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

Abstract: This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

Reason for writing the article—theory, overall issue, purpose.

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

Approach:

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

Introduction:

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.

The following approach can create a valuable beginning:

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

Approach:

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

Procedures (methods and materials):

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

Materials may be reported in part of a section or else they may be recognized along with your measures.

Methods:

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

Approach:

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

What to keep away from:

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

Content:

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

What to stay away from:

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

Approach:

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

Figures and tables:

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

Discussion:

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."

Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.

Segment draft and final research paper: You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

Written material: You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350