DOI: 10.17812/IJRA.9.36 (1)2022

International Journal of Research and Applications
Oct - Dec © 2022 Transactions 9(36): 2601-2607

eISSN : 2349 – 0020
pISSN : 2394 – 4544
www.ijraonline.com

COMPUTERS RESEARCH ARTICLE

Anomaly traffic detection using Network Traffic Analysis in Android based Mobile Devices

Santosh Kumarhenge [1] and R. Madhudevi [2]
[12] Department of Computer Science and Engineering,
Priyadarshini Institute of Technology & Science, Guntur, Andhra Pradesh-522017.
[1] hingesanthosh@gmail.com and [2] madhuridevichandu@gmail.com

ABSTRACT

Anomaly network traffic detection is a powerful network security tool that may identify a variety of known attacks, now a day Computing quick grow than wide spread use have increased the complexity and change ability of opens networks and service sharing situations, which has exacerbated security issues. There are several flaws, though. A fresh possibility for the advancement of anomaly network traffic detection is presented by deep learning. The spatial and temporal characteristics of network traffic cannot yet be fully learned by the current deep learning models, and performance of the classifier must be improved. This paper suggests a concurrent circuit layout with 3 layers anomalous Mechanism for detecting internet congestion (MDIC) that integrates chronological and geographical information to close this gap. The Scalable Manifold Classifier and Photon Stochastic Enhancing Network methods were utilized in our study (LGBM).

Keywords: Network, Classifier, Anomaly, Android

1. INTRODUCTION

To increase the precision of network traffic classification, MDIC learns the chronological and geographical properties out of congestion and completely combines combining two characteristics utilizing pattern hybrid method. Based on this, a better approach of extracting raw traffic features is suggested. It can ameliorate dataset imbalance, cut down on unnecessary functionality, or expedite network realignment. An object with one or more sensing's and, optionally, one or more actuators and the ability to process and network sensed data. A sensing hub is made up of numerous components similar to one another such as geographically scattered and interacts with one another. Each of these hubs includes a transceiver, an energy source, a microprocessor (microcontroller) that processes sensing signals, a sensing element (sensing), and a microprocessor. Dispersed across artifact, sensing hubs with its relevant sensing does allow it to acquire data on the object and control operations which actually occur here on thing.

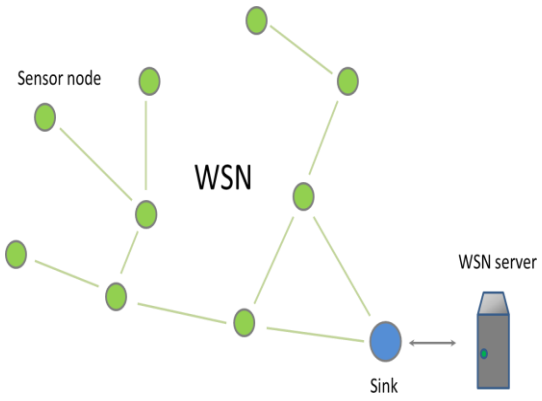

Fig. 1: Overview of the network architecture

An illustration of a WSN is shown in the image above. A WSN having 12 IOT devices and just a routing drain which functions as just a turnstile may be observed here Network sinks often link to a server that is processing data received from a network and have a stationary power source was directly integrated, if client & WSN were put within the identical item. When it is essential to offer an unauthorized connection to WSN, web drain also serves as a gate, and it is feasible to communicate with WSN over worldwide networks like the Internet.

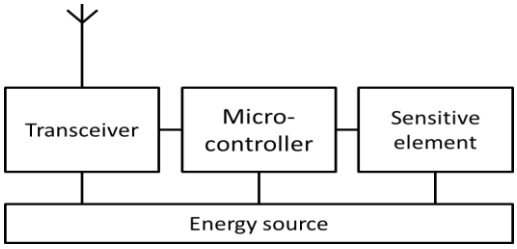

Fig 2: Sensor hum inner structure

Some Sample Applications:

- Ecology and biodiversity surveillance
- Seismo Surveillance
- Evaluation of Local Infrastructure Condition
- Soil And underground water Detection
- Immediate Rescue Effort
- Supervision of Economic Processes
- Spying programs and peripheral protection
- Complex Climatic Management Automation
- Automated Building Climate Control

2. LITERATURE REVIEW

NL-IDS: Wireless Sensing Networks 'Network Layer Intrusion Detection System Based on Trust Jayaram Pradhan and Uma Shankar Ghugar IEEE 2021. Security in wireless sensing networks (WSN) has become crucial in recent years, as WSN applications depend on hub-to-hub information flow. Many security vulnerabilities have been revealed as a consequence of the network's open adoption. The attackers disrupt the security system by assaulting the multiple protocol layers of the WSN. The route finding technique raises doubts about the overall security of the AODV routing protocol. The data must be transported safely in order to reach its destination. To facilitate the process and identify Black hole attackers in the network, we presented a trust-based intrusion detection system (NL-IDS) for the network layer in WSN. The sensing hub trust is judged based on the key factor fluctuation at the network layer induced by the black hole attack. The watchdog strategy is utilized, in which a sensing hub establishes a periodic trust value and constantly watches the neighboring hub. The values of the network layer's trust metrics are then gathered and employed to generate the overall trust value of the sensing hub (past and previous trust values) (past and previous trust values). This NL-IDS technique is effective in detecting the rogue hub in Black hole attacks at the network layer. We tested the model in MATLAB R2015a to assess NL-IDS performance, and the results reveal that NL-IDS beat Wang et al. in terms of detection accuracy and false alarm rate.

Colin C. Murphy, Philip J. Harris, and George D. O'Mahon IEEE 2021. Examining Wireless Sensing Networks' Exposure to a Malicious Matched Protocol Attack. Wireless networks based on commercial off-the-shelf (COTS) devices and standardized protocols have lately started to be welcomed by safety-critical, Internet of Things (IoT), and space-based applications, presenting the security concern of hostile incursions inevitable. Malicious intrusions that go undetected may result in a full loss of services or other major implications. Every service must function effectively for any safety-critical application, as any failure can risk privacy or safety. As a consequence, all intrusions must be found and neutralized in order for these life-critical services to remain accessible and operating.

IEEE 2021: Haruo Yokota, Chia-Mu Yu, Sy-Yen Kuo, and Nesrine Berjab Spatio-temporal and multivariate attribute correlation-based abnormal-hub detection in wireless sensor networks. In Data in wireless sensing networks (WSNs) could be prone to errors and malicious assaults, rendering it untrustworthy. This vulnerability presents complications for

software that monitor the environment by delivering false notifications. In order to offer a trustworthy system, we must detect aberrant hubs. We present a unique paradigm for clustered heterogeneous WSNs that can identify aberrant hubs in this work. It utilizes observable spatiotemporal (ST) and multivariate-attribute (MVA) sensing correlations while taking prior knowledge of the monitored environment into account. The acquired data is analyzed by computing the cross correlation across sensing streams using ST correlations.

A Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensing Networks IEEE 2021 participants include Salwani Abdulla, Amjad Mehmood, Akbar Khanan, Muhammad Muneer Umar, Khairul AkramZainolAriffin, and Houbing Song. Wireless sensing networks, by definition, are more sensitive to security assaults than traditional networks. WSN advances have resulted in the deployment of numerous security-focused protocols. The majority of these protocols are inefficient in terms of placing an undue computational and energy consumption pressure on tiny hubs in WSNs. This paper presents a knowledge-based and context-aware strategy for dealing with intrusions produced by malevolent hubs. The knowledge base in the base station, where the system is stored, functions as a repository for network hub events.

Haibin Zhang, Jiajia Liu, and Nei Kato's paper, "Threshold Tuning-Based Wearable Sensing Fault Detection for Reliable Medical Monitoring Using Bayesian Network Model," was published in IEEE 2021. False alarms, incorrect medical diagnoses, and potentially fatal errors in judgment can all come from erroneous sensing data since the medical body sensing network (BSN) typically has limited resources and susceptible to environmental impacts and hostile attacks.

Therefore, it is Important to identify and eliminate inaccurate sensing data as much as possible before using it to make medical diagnoses. For body sensing fault detection, the majority of research on the subject directly used fault detection techniques created in conventional wireless sensing networks (WSN).BSNs, on the other hand, use a very small number of sensing's to collect essential data, lacking the information redundancy offered by densely placed sensing hubs in conventional WSNs.

Design, analysis, and evaluation of a Light-Weight Counter measure against Forwarding Misbehavior in Wireless Sensing Networks IEEE2021:Cong Pu, Sunho Lim. Wireless sensing networks (WSNs) are vulnerable to various denial-of-services (DoS) attacks that primarily target service availability by disrupting network routing protocols or interfering with ongoing communications due to the lack of centralized coordination, physical protection, and security requirements of inherent network protocols. In this research, we offer a light weight defense against a selective forwarding attack dubbed SCAD, here a single check point hub is deployed at random to look for malicious hubs' forwarding misbehavior. To swiftly recover from unexpected packet losses caused by poor channel quality or forwarding misbehavior, the suggested counter measure is integrated with timeout and hop-by-hop retransmission techniques. Additionally, we provide a straightforward analytical model togetherwithits numerical false detection rateresult.

3. PROBLEM STATEMENT AND METHODOLOGY

Problem Statement: Burglar alarm is another word for IDS. For example, the house's lock system guards against theft. If, on the other hand, a lock is damaged and someone tries to enter the property, the burglar alarm detects the damage and warns the owner by sounding an alarm. Furthermore, firewalls are fairly excellent at screening incoming Internet traffic to circumvent the firewall. External users, for example, may access the Intranet by dialing using a modem linked to the organization's private network; the firewall is unable to identify this sort of access. An intrusion prevention system (IPS) is a network security/threat prevention device that analyses network traffic flows to identify and prevent vulnerability exploitation. Prevention systems are grouped into two types: host and network (NIPS) (HIPS) (HIPS). These technologies monitor network activity and react automatically to safeguard systems

and networks. IPS has an issue with false positives and negatives. False positives are events that produce an IDS warning despite the absence of an attack. When an attack occurred, a false negative is described as an incidence that does not elicit an alarm. Single points of failure, signature changes, and encrypted traffic are just a few of the bottlenecks that inline operation could generate. IDS monitor the activity of the system or network.

Methodology: Companies has utilized intrusion detection systems (IDS) to gather and assess different sorts of attacks on the hosting computer or networks. Detecting & recognizing prospective risks violations is especially critical as they may comprise both intrusions—attacks from outside the organization—and misuses—attacks from within. We recommended the integrated method in this study, which differs substantially from most earlier studies that concentrated solely on deploying one system, either detection or prevention, as well as either Intruder detection or Signature based detection. The integrated model contains the two systems Intrusion Detection (ID) and Intrusion Prevention (IP), as well as those that benefit from well-known techniques: Intruder Detection and Intrusion Prevention (ID) (ID). Some studies have mixed the two approaches into a hybrid strategy, such as the study just mentioned, were the scientists employed ID based on fingerprints, but their approach lack preventative capacities even then.

Existing System:

Support Vector Machine (SVM):

To detect an ideal hyper plane for different distinct examples in a high dimensional space is the main process of the SVM. There are numerous hyper planes that can realize this paradigm. The data that corresponds to the ideal choice surface and is closest to the closed surface, the support vector, is what this procedure depends on. By creating a hyper plane to partition the data and planning the input vectors into a high dimensional space, it does classification. Most non-convex, unconstrained minimization problems as well as quadratic programming issues are solved with this method. The classifier process's most effective method is the SVM.

4. PROPOSED SYSTEM

Light Gradient Boosting Machine Classifier (LGBM): LGBM stands for Lighting Gradients Boost Machinery, a name invented by Microsoft. It is a networked xgboost system that is freeware and available to the public. This is based on decision trees and has been used in classification, rating, and other supervised learning tasks. LightGBM supports the GBT, GBDT, GBRT, GBM, MART, and RF algorithms. LightGBM has various benefits over Adaboost, such as patchy optimisation, concurrent learning, different failure causes, normalisation, bagging, and quick termination. The structure of the trees in the two differs greatly. Unlike earlier versions, LightGBM builds a forest column by column rather than levels per layer. Plants, on the other hand, grow leaf by leaf. It picks the leaf that it feels will result in the greatest loss reduction. Moreover, unlike XGBoost and other implementations, LightGBM does not employ the well-known sorted-based decision tree learning technique, which finds the appropriate split point based on sorted feature values. LightGBM, on the other hand, employs a highly optimised decision tree learning technique based on histograms, as shows in figure 3, which delivers considerable benefits in terms of accuracy and efficiency.

The LightGBM algorithm's Gradient-Based One-Side Sampling (GOSS) and Exclusive Feature Bundling (EFB) approaches enable it to run quicker while retaining good accuracy.

5. SYSTEM ARCHITECTURE

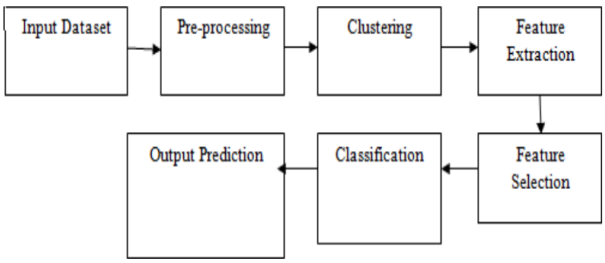

Fig 3 : Ssystem Aarchitecture

6. SYSTEM IMPLEMENTATION

a. Module Description

There are 8 components in the system. They are

- Incomingpacket
- PacketCapture
- Packetscanner
- Packetanalyzer
- Labeling
- Trainingmodel
- Prediction:
- Output

b. Flowchart

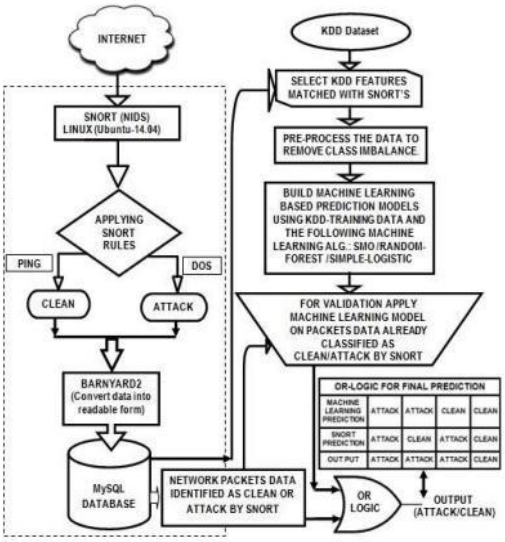

Fig 4 : flow chart

c. Algorithm of Proposed Work

a. This information is partitioned into little overlap or quasi pieces.

b. Utilizing traditional procedures, determine the qualities.

c. The feature extraction values for each key point are kept in a matrix.

d. Use filtering algorithms to locate relevant traits that are near together.

e. Propose the idea of shifting vectors to locate important spots with equivalent movement.

f. Measure the occurrences of the precise shift key location using the count vectors & put your count at 1 and figure 4.

g. Using the threshold level prior techniques, similar places were determined.

d. Probable Solutions to this Problem :

1) Most Trivial Option is: (Brute **Force)** to install each application in devices or emulator and Categorize manually.
2) Using Machine Learning Techniques: ML on the Categorized Benign Application (we generated from APK pure) to teach the model to categorize any given application to app type.

and then Categorizing **Malware Apps** using the above trained Model.

Model can be trained in 2 ways:

a) Using List of API calls as the Input Feature

or

b) Using Graphs as the Input Feature (Generated from Call Graphs)

i) Which will contain sub graphs with malicious intent?

7. DISCUSSION

Android apps for malicious actions and sensor data logging while such actions are taken place.

APPNAME	BENIGNACTION	MALICIOUSACTION
Calc	Calculator	Spammessage
TacGame	Play	downloads
Recorder	Recorder	Stealdatafrom nearbymobile

Image1: App Name

Sensitive APIs

API Calls
Landroid/telephony/TelephonyManager->getSubscriberId
Landroid/util/AttributeSet->getAttributeBooleanValue
Landroid/util/AttributeSet->getAttributeUnsignedIntValue
Landroid/net/NetworkInfo->getExtraInfo
Landroid/view/animation/AlphaAnimation->startNow
Ljava/util/GregorianCalendar->get
Landroid/content/pm/PackageManager->getInstalledPackages
Landroid/telephony/TelephonyManager->getSimSerialNumber

Image2: Sensitive API

8. EXPERIMENTAL RESULTS

a) The instrumentation with malware dataset

This equation is supplied in Python 3.6.9. We leveraged the totally open Machine Learning software, frequently applied in numerous applications of malware classification to know whether application is malicious or benign. We also tested with test beds, which serves as middleware and is visible at the top of it, this Test bed image collection has thousands of frames in malware families, the bulk of which are out from m a l w a r e databases. Our research used the training technique involved both training and validation stages. As a result, the whole training sample was split into two parts: 80 percent for training the model and 0.20 percent for validation.

a) The suggested Visual Geometry malware model performance

The Visual Geometry Malware approach's effectiveness is measured using the Accurateness, Recognize, Support, Exactness and Mean. The training malware dataset is initially stored with its labels. We capped 100 periods for network deep raining using testbed1 and testbed2. The supplied technology has the benefit of maintaining the superior model. We used 20% of the full sample for testing purposes. The paper outcomes are then contrasted against the confusion matrix, as represented in Image 1, Image 2, which is generated. Image 3 and Image 4 depicts the suggested Visual Geometry Malware switch teaching model's categorization efficiency & lost outcome. Table I presents the different measurement test bed methods done entirely using the Visual Geometry Malware model. The supervised learning approach recommended for using the Visual Geometry Malware switch teaching model achieves 0.95% training classification accuracy/precision and 1.00%validation classification and validation accuracy/precision.

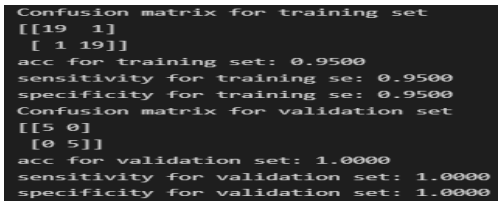

Image3: Confusion Matrix

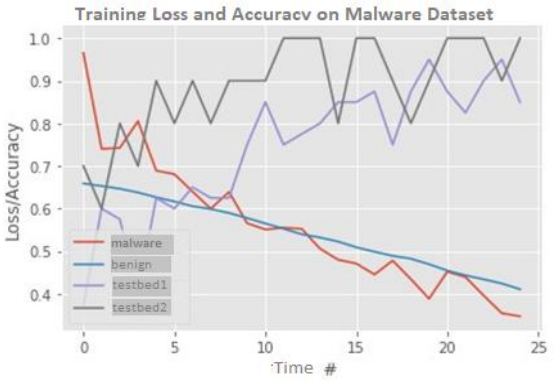

Image 4: Visual Geometry Malware detection efficiency training & loss as a function of periods

Predicament of Wellness	Accurateness	Exactness	Recognize	Mean
Malware	100%	1.00	0.95	0.50
Benign	95%	0.70	1.00	0.95
Testbed1	70%	0.25	1.00	1.00
Testbed2	80%	0.30	1.00	1.00

Table 1: The Suggested Visual Geometry Malware Model Performance

9. CONCLUSION

The scientific community and business organizations are equally interested in intrusion detection at the moment. Based on a proposed taxonomy and examples of previous and present initiatives, we have provided background information on the state-of-the-art of IDS at the moment. This taxonomy also emphasizes new research and effectively addresses both earlier and more recent discoveries. Each of its techniques has pros and cons of its own. We think that no single criterion can be employed as a complete defense against infiltration into a computer network. It does not exist in a single form that can be applied as a universal defense against all potential assaults. Building and maintaining computer systems and networks that are resistant to attacks is both technically challenging and expensive.

10. FUTURE SCOPE

Other machine learning algorithms should be taken into account in future study to find more effective ways to apply the classification methodology to the datasets. It is advised that additional study bed neon other parameters that can increase detection accuracy.

REFERENCES

1) I.F. Akyildizetal., "Wireless Sensor Networks: A Survey, "Elsevier Comp. Networks, vol.3, no. 2, 2019, pp. 393–422
2) G.Li, J.He, Y. Fu. "Group-based intrusion detection system in wireless sensor networks "Computer Communications, Volume31, Issue18 (December2019).
3) Michael Brownfield, "Wireless Sensor Network Denial of Sleep Attack", Proceedings of the2019 IEEE Workshop on Information Assurance and Security United States Military Academy, WestPoint, NY.
4) Farooq Anjum, Dhanant Subhadra bandhu, Saswati Sarkar*, RahulShetty, "On Optimal Placement of Intrusion Detection Modules in Sensor Networks", Proceedings of the First International Conference on Broadband Networks (BROADNETS19).
5) Parveen Sadotraetal, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.9, September-2019, pg. 23-28
6) K. Akkaya and M.Younis, —A Survey of Routing Protocols in Wireless Sensor Networks, ‖in the Elsevier Ad Hoc Network Journal, Vol. 3/3 pp. 325-349, 2019.
7) A. Abduvaliyev, S. Lee, Y.K Lee, "Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks", IEEE International Conference on Electronics and Information Engineering, Vol.2, pp. 25-29, August 2019.
8) Parveen Sadotra and Chandrakant Sharma. A Survey: Intelligent Intrusion Detection System in Computer Security. International Journal of Computer Applications 151(3):18-22, October2019.
9) I.F. Akyildizetal., "Wireless Sensor Networks: A Survey, "Elsevier Comp.Networks, vol.3, no. 2,2019, pp. 393–422
10) G.Li, J.He, Y. Fu. "Group-based intrusion detection system in wireless sensor networks "Computer Communications, Volume31, Issue18(December2019)
11) Michael Brownfield, "Wireless Sensor Network Denial of Sleep Attack", Proceedings of the2019 IEEE Workshop on Information Assurance and Security United States Military Academy, WestPoint, NY.
12) Farooq Anjum, Dhanant Subhadrabandhu, SaswatiSarkar*,RahulShetty,"OnOptimalPlacementofIntrusionDetectionModulesinSensorNetworks",ProceedingsoftheFirstInternationalConferenceon Broadband Networks(BROADNETS19).
13) ParveenSadotraetal,InternationalJournalofComputerScienceandMobileComputing,Vol.5Issue.9,September-2019, pg. 23-28
14) K.AkkayaandM.Younis,—ASurveyofRoutingProtocolsinWirelessSensorNetworks,‖intheElsevier Ad Hoc Network Journal, Vol. 3/3 pp. 325-349, 2019.
15) A. Abduvaliyev, S. Lee, Y.K Lee, "Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks" ,IEEE International Conference on Electronics and Information Engineering,Vol.2, pp. 25-29, August 2019.
16) Parveen Sadotra and Chandrakant Sharma. A Survey: Intelligent Intrusion Detection Systemin Computer Security. International Journal of Computer Applications 151(3):18-22, October2019.
17) A.Araujo,J.Blesa,E.Romero,D.Villanueva,"Securityincognitivewirelesssensornetworks.Challengesandopenproblems",EURASIPJournalonWirelessCommunicationsandNetworking,February 2019.
18) A.Becher,Z.Benenson,andM.Dorsey,\Tamperingwithmotes:Real-worldphysicalattacksonwireless sensor networks." in SPC (J. A. Clark, R. F. Paige, F. Polack, and P. J.Brooke, eds.),vol.3934 of Lecture Notes in Computer Science, pp. 104{118, Springer,2019.
19) I.KrontirisandT.Dimitriou,\Apracticalauthenticationschemeforin-networkprogramminginwirelesssensornetworks,"inACMWorkshoponReal-WorldWirelessSensorNetworks,2019.
20) M. Ali Aydın *, A. HalimZaim, K. Gokhan Ceylan "A hybrid intrusion detection systemdesignforcomputernetworksecurity"ComputersandElectricalEngineering35(2019)517–526.