PSO based Intrusion Detection System

Manjot Kaur[1], Dr. Amandeep Verma[2]

[1]sranmanjot2014@gmail.com
[2]vaman71@gmail.com
[1,2]PURCITM Phase7, Mohali

***Abstract*— In this technology era every applications depends on networks, it may be local or Internet, Intranet or Extranet, wired or wireless. All networks require strong security consideration to ensure confidentiality and integrity of communication. This paper discusses network security and related issued specifically at Transport layer, which enables true end to end communication between peers. As security is never 100%, security threats and vulnerability continues growing and becomes major concern for business and industries. Transport layer security concern with authentication, confidentiality, integrity and availability. However, Transport Layer Security (TLS), the standard protocol for encryption in the Internet, assumes that all functionality resides at the endpoints, making it impossible to use in-network services that optimize network resource usage, improve user experience, and protect clients and servers from security threats. Re-introducing in-network functionality into TLS sessions today is done through hacks, often weakening overall security.**

***Keywords*— WSN, RFD, Routing in WSN**

I. INTRODUCTION

An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.

An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

There are a multiple ways detection is performed by IDS. In signature-based detection, a pattern or signature is compared to previous events to discover current threats. This is useful for finding already known threats, but does not help in finding unknown threats, variants of threats or hidden threats.

Another type of detection is anomaly-based detection, which compares the definition or traits of a normal action against characteristics marking the event as abnormal.

There are three primary components of IDS:

- Network Intrusion Detection System (NIDS): This does analysis for traffic on a whole subnet and will make a match to the traffic passing by to the attacks already known in a library of known attacks.
- Network Node Intrusion Detection System (NNIDS): This is similar to NIDS, but the traffic is only monitored on a single host, not a whole subnet.
- Host Intrusion Detection System (HIDS): This takes a “picture” of an entire system’s file set and compares it to a previous picture. If there are significant differences, such as missing files, it alerts the administrator.

II. BASIC NETWORK SECURITY REQUIREMENT

Security is represented through accomplishment of some basic security properties, namely, confidentiality, integrity, availableness, authentication and responsibleness (nonrepudiation)[3][5]. All security threats and attacks will be classified below following properties in broad sense.

Confidentiality: it's a property of protective the information from all users aside from those supposed by the owner of the data. The non supposed uses area unit usually known as unauthorized users. It be passive attach. Passive attach is tough to sight however simple to use victimisation Cryptography and/or Stenography [5]. will|we will|we are able to} guarantee confidentiality victimisation cryptography secret writing in order that throughout transit one can see it however not comprehend it.

Integrity: making certain integrity suggests that protective info from unauthorized sterilization. It falls below active attack. you can not stop user to change knowledge however detection of this alteration is incredibly simple. Once detected user will solve the problem like not settle for such packet. we will calculate on time hash as sender aspect before causation packet over network. Then at receiver aspect conjointly calculate hash supported received message so check each hash, if same than no break however if not same then stop the communication.

Availability: availableness making certain reliable and timely access to and use of knowledge and repair isn't denied to legitimate/authorized user. it's the property of protective info from non-authorized temporary or permanent with holding of knowledge [3]. availableness concern at the majority layers of OSI. currently each day attack on availableness will increase in no time and mitigating it at explicit layer is incredibly onerous. however here we tend to speak availableness problems solely at transport layer which may mitigate selectively applicable security solutions like firewall, intrusion detection system etc.

Authentication: it's property through that we will verify or check real entity. It ensures that user is World Health Organization they determine themselves which every inputs incoming at the system comes from a trusty supply [3]. Authentication will be making certain by several techniques like, login-password, biometric, Certificate primarily based, OTP etc.

Fig 1: Position of Transport Layer and it Security in respect to OSI model

Accountability: It concern with the tracing actions of entity unambiguously. responsibleness concern with keeping record and audit checking concerning non-repudiation, isolate fault, IDP, recovery and proceedings. As we all know security ne'er 100% realizable we've to trace potential breaches. it's terribly essential for rhetorical evident and/or analysis conjointly [3].

III. RELATED WORK

In this section, we have a tendency to summarize and discuss connected authentication ways employed in follow or projected within the literature to boost positive identification authentication on the net and gift their limits.

Mehmood, A. et al. [1] proposed a knowledge-based context-awareapproach for handling the intrusions generated by malicious nodes. The system operates on a knowledgebase, located at the base station, which is used to store the events generated by the nodes inside the network.The events are categorized and the cluster heads (CHs) are acknowledged to block maliciously repeatedactivities generated. The CHs can also get informational records about the maliciousness of intruder nodesby using their inference engines. The mechanism of events logging and analysis by the base station greatlyaffects the performance of nodes in the network by reducing the extra security-related load on them.

Jiguang, L. et al. [2] explored a novel method which has a relative stable detection performanceunder different moving speeds and extracted a novel feature representing the fluctuation of the whole channelfrom channel state information at the physical layer of 802.11n wireless networks, and utilize a probabilitytechnique to detect human motion. A hidden Markov model is leveraged as the classifier to make human detection a probability problem and implemented the system using off-the-shelf WiFi devices and evaluate itin two scenarios. As indicated in the evaluation results, our approach is an appropriate method for intrusiondetection.

Teng, S. et al. [3]presented an adaptive collaboration intrusion detection method toimprove the safety of a network. A self-adaptive and collaborativeintrusion detection model is built by applying the Environmentsclasses,agents, roles, groups, and objects (E-CARGO) model. Theobjects, roles, agents, and groups are designed by using decisiontrees (DTs) and support vector machines (SVMs), and adaptivescheduling mechanisms are set up. The KDD CUP 1999 data setis used to verify the effectiveness of the method. The experimentalresults demonstrate the feasibility and efficiency of the proposedcollaborative and adaptive intrusion detection method. Also, theproposed method is shown to be more predominant than themethods that use a set of single type support vector machine(SVM) in terms of detection precision rate and recall rate.

Tao, P. et al. [4]proposed the FWP-SVM-genetic algorithm (GA)(feature selection, weight, and parameter optimization of support vector machine based on the geneticalgorithm) based on the characteristics of the GA and the SVM algorithm. The algorithm first optimizesthe crossover probability and mutation probability of GA according to the population evolution algebra andfitness value; then, it subsequently uses a feature selection method based on the genetic algorithm with aninnovation in the fitness function that decreases the SVM error rate and increases the true positive rate.Finally, according to the optimal feature subset, the feature weights and parameters of SVM are simultaneouslyoptimized.

Peng. H. et al. [5] presented an SDN-based flow detection method, builds structuresfor detecting anomaly SDN flows and performs classification detection on the flows using the double P-valueof transductive confidence machines for K-nearest neighbors algorithm. The experimental results show thatthe algorithm proposed achieves a lower false positive rate, higher precision, and better adaptation to theSDN environment than do other algorithms of the same type.

Alaparthy, V.T. and Morgera, C.D. et al. et al. [6] made an effort to securea wireless sensor network (WSN) using an immune theory technique called Danger Theory. In other words,a multi-level intrusion detection system (IDS) is designed based on the functions of various immune cells.This is realized by monitoringWSNparameters, such as energy, volume of data and frequency of data transferand developing an output based on their weights and concentrations which is a suitable basis for IDS designin WSNs.

Ali. M.H. et al. [7] proposed a developed learning model for fast learning network (FLN) based on particle swarm optimization (PSO) and named as PSO-FLN. The model has been applied to the problem of intrusion detection and validated based on the famous dataset KDD99. Our developed model has been compared against a wide range of meta-heuristic algorithms for training extreme learning machine and FLN classifier. PSO-FLN has outperformed other learning approaches in the testing accuracy of the learning.

Naik. N. et al. [8] presented a dynamic fuzzy rule interpolation (D-FRI) approach by exploiting such interpolated rules in order to improve the overall system’s coverage and efficacy. The resulting D-FRI system is able to select, combine, and generalize informative, frequently used interpolated rules for merging with the existing rule base while performing interpolative reasoning. Systematic experimental investigations demonstrate that D-FRI outperforms conventional FRI techniques, with increased accuracy and robustness. Furthermore, D-FRI is herein applied for network security analysis, in devising a dynamic intrusion detection system (IDS) through integration with the Snort software, one of the most popular open source IDSs. This integration, denoted as D-FRI-Snort hereafter, delivers an extra amount of intelligence to predict the level of potential threats. Experimental results show that with the inclusion of a dynamic rule base, by generalising newly interpolated rules based on the current network traffic conditions, D-FRI-Snort helps reduce both false positives and false negatives in intrusion detection.

Ghafi, I. et al. [9]proposed a novel unsupervised methodology to dynamically generate the BPA values, based on both the Gaussian and exponential probability density functions, the categorical probability mass function, and the local reachability density. Then, D-S is used to fuse the BPA values to classify whether the Wi-Fi frame is normal (i.e., non-malicious) or malicious.

IV. PSO

Particle Swarm Optimization (PSO) is a computational method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality. It solves a problem by having a population of candidate solutions, here dubbed particles, and moving these particles around in the search-space according to simple mathematical formulae over the particle's position and velocity. Each particle's movement is influenced by its local best known position, but is also guided toward the best known positions in the search-space, which are updated as better positions are found by other particles. This is expected to move the swarm toward the best solutions.

PSO is a metaheuristic as it makes few or no assumptions about the problem being optimized and can search very large spaces of candidate solutions. However, metaheuristics such as PSO do not guarantee an optimal solution is ever found. Also, PSO does not use the gradient of the problem being optimized, which means PSO does not require that the optimization problem be differentiable as is required by classic optimization methods such as gradient descent and quasi-newton methods.

V. Encryption Schemes in TLS

However, we tend to found that causation a ClientKey-Exchange at the side of a DH certificate allows a brand new shopper impersonation attack.

Server-Gated Crypto (SGC) OpenSSL servers have a gift feature referred to as SGC that permits shoppers to restart a acknowledgment when receiving a ServerHello. additional code scrutiny reveals that the state created throughout the primary exchange of greeting messages is then purported to be discarded fully. However, we tend to found that some items of state that indicate whether or not some extensions had been sent by the shopper or not will linger from the primary ClientHello to the new acknowledgment. Export RSA In gift export RSA ciphersuites, the server sends a signed, however weak (at most 512 bits) RSA modulus within the ServerKeyExchange message. However, if such a message is received throughout a acknowledgment that uses a stronger, non-export RSA ciphersuite, the weak transient modulus can still be accustomed write the client’s pre-master secret. This ends up in a brand new downgrade and server impersonation attack referred to as FREAK.[5]

Static DH we tend to equally observe that OpenSSL shoppers permit the server to skip the ServerKeyExchange message once a DHE or ECDHE ciphersuite is negotiated. If the server certificate contains, say, associate degree ECDH public key, and therefore the shopper doesn't receive a ServerKeyExchange message, then it'll mechanically rollback to static ECDH by victimisation the general public key from the server’s certificate, leading to the loss of forward-secrecy.[5]

VI. Research Gaps

In Knowledge Base IDS (KB-IDS) primarily focuses on the analysis ofevents generated by different nodes in a WSN. The eventsare stored in a knowledge base located at the base station.The whole network is divided into a number of clusters andin each cluster a node is nominated as the head. The CHscommunicate with the base station and forward events datato the knowledge base through inference engines. The systemis quite effective as it does not use heavy security algorithmsthat put an additional computation and storage load on all thenodes inside a network. KB-IDS puts a load on a single nodeinside the cluster. More importantly, the traffic is monitoredand any suspicious event generated by an attacker node isblocked by the CHs due to storing knowledge about the natureof events.

- For increasing the performance of the proposed system, the events are also processed and grouped into different patterns. The system also supports the switching of CHs(Cluster Heads) with other member nodes whenever needed.
- This approach can be further expanded by distributing the load of the CH(Cluster Head) on all the nodes. The knowledge and events processing can be handled by advanced computational algorithms.

VII. Results

Accuracy: It is a description of systematic errors, a measure of statistical bias; as these cause a difference between a result and a "true" value, ISO calls this trueness.

Accuracy(A) = (TP+TN)/(TP+TN+FP+FN)

Precision: It is a description of random errors, a measure of statistical variability.

Precision(P) = TP / (TP + FP)

Recall: Recall (also known as sensitivity) is the fraction of relevant instances that have been retrieved over total relevant instances in the image. Both precision and recall are therefore based on an understanding and measure of relevance.

Recall (R) = TP / (TP + FN)

True positive (TP) = the number of cases correctly identified as true

False positive (FP) = the number of cases incorrectly identified as true

True negative (TN) = the number of cases correctly identified as false

False negative (FN) = the number of cases incorrectly identified as false

Table 1: Comparative Study for Existing and Proposed approaches

No of Keywords	Accuracy (Proposed)	Accuracy (Existing)	Recall (Existing)	Recall (Proposed)	Precision (Existing)	Precision (Proposed)	F-Measure (Existing)

DS1	90	83	0.89	0.96	0.9	0.94	0.87	0.92
DS2	90	85	0.86	0.94	0.82	0.92	0.86	0.9
DS3	92	88	0.83	0.92	0.82	0.92	0.83	0.9

Table 1 is the comparative study for the statistical analysis and Proposed approaches in IDS. From the table it is clear that the Proposed values of results are better than that of statistical analysis. From table 1 it is clear that the values of accuracy, recall, precision and F-Measure are better in case of Proposed approaches that are nearly 84, 0.92, 0.93 and 0.87 approx.

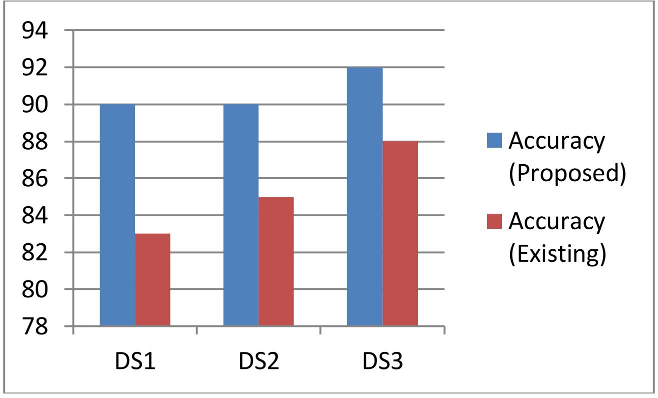

Fig 1: Comparative Study of Accuracy in Existing and proposed approach

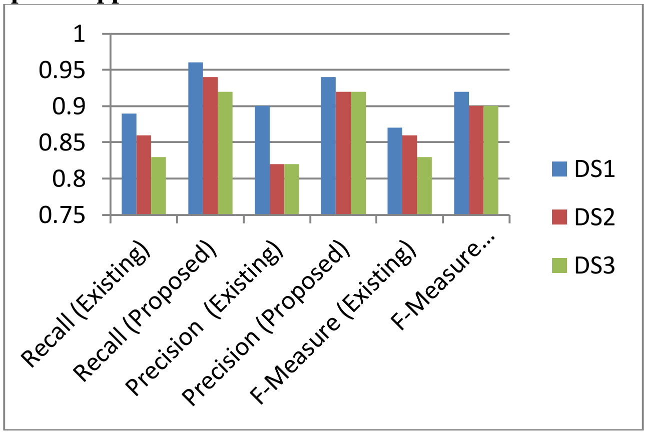

Fig 2: Comparative Study of Precision, F-Measure, Recall in Existing and proposed approach

Fig 1 and 2 is representation of comparison of F-Measure Precision, Recall and Accuracy in existing and proposed approach. From fig it is shown that the F-Measure and Precision in proposed approach is better as compared to existing in all 3 datasets and noted an improvement of approx 11%.

VIII. CONCLUSION

In network security Intrusion Detection System plays an important role to prevent attacks. Existing approaches developed a classifier ensemble method for intrusion detection that is diversified by using two different approaches i.e. different feature sets and training sets or both. The methodology also makes use of re-sampling technique that emphasizes the attack of rare category. In these approaches the re-sampling count for accuracy in quite high so that the memory consumption is high and inefficient resource utilization which results into lower throughput. To avoid these drawbacks proposed approach adjust of the ensemble size dynamically according to the size of dataset may be done.

In this research, we proposed novel frameworks and developed methods which perform better. However, in order to improve the overall performance of our system we used the domain knowledge for selecting better features for training our models. This is justified because of the critical nature of the task of intrusion detection. Using domain knowledge to develop better systems is not a significant disadvantage; however, developing completely automatic systems presents an interesting direction for future research

IX. REFERENCES

[1]. Mehmood, A.; Khanan A.; Umar, M.M.; Abdullah S.; Ariffin, K.A.Z.; Song, H.; "Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensor Networks", Special Section on Security Analytics and Intelligence for Cyber physical systems, IEEE, ISSN: 2169-3536, vol. 6, 2018, Page: 5688-5694

[2]. Jiguang, L.; Man, D.; Yang, W.; Du, X.; Yu, M.; "Robust WLAN-Based Indoor Intrusion Detection Using PHY Layer Information", IEEE, ISSN: 2169-3536, vol. 6, 2018, Page: 30117-30127

[3]. Teng, S.; Wu, N.; Zhu, H.; Teng, L.; Zhang, W.; "SVM-DT-Based Adaptive and Collaborative Intrusion Detection", IEEE/CAA Journal of AutomaticaSinica, vol. 5, No: 1, 2018, Page: 108-118

[4]. Tao, P.; Sun, Z.; Sun, Z.; "An Improved Intrusion Detection Algorithm Based on GA and SVM", Special Section on Human-Centered Smart Systems and Technologies, IEEE, vol. 6, 2018, Page: 13624-13631

[5]. Peng, H.; Sun, Z.; Zhao, X.; Tan, S.; Sun, Z.; "A Detection Method for Anomaly Flow in Software Defined Network", IEEE, ISSN: 2169-3536, vol. 6, 2018, Page: 27809-27817

[6]. Alaparthy, V.T.; Morgera, C.D.; "A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory", IEEE, ISSN: 2169-3536, vol. 6, 2018, Page: 47364-47373

[7]. Ali. M.H.; Mohammed, B.A.D.A.; Ismail, A.; Zolkipli, M.F.; "A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization", IEEE, ISSN: 2169-3536, vol. 6, 2018, Page: 20255-20261

[8]. Naik, N.; Diao, R.; Shen, Q.; "Dynamic Fuzzy Rule Interpolation and Its Application to Intrusion Detection", IEEE Transactions on Fuzzy Systems, vol. 26, No: 4, 2018, Page: 1878-1892

[9]. Ghafi, I.; Kyriakopoulos, G. K.; Aparicio-Navarro, F.J.; Lambotharan, S.; Assadhan, B.; Binsalleeh, H.; "A Basic Probability Assignment Methodology for

Unsupervised Wireless Intrusion Detection”, IEEE, vol. 6, 2018, Page: 40008-20023

[10]. Juillerat,N., Enforcing Code Security in Database Web Applications using Libraries and Object Models, LCSD 2007,Canada, ACM 1-58113-000-0/00/004, pp:12-28

[11]. Shalini, S. and Usha S., Prevention of Cross-Site Scripting attacks (XSS) on Web Applications in the Client Side, International Journal of Computer Science Issues, vol. 8, Issue: 4, No: 1, 2011, pp: 23-28

[12]. Weinberger, J. , Saxena, P. , Akhawe, D., Finifer,M., Shin,R. and Song,D., A Systemmatic Analysis of XSS Sanitization in Web Application Frameworks,ESORICS, vol. 4, issue: 1, 2011, pp:237-241

[13]. Lomte, R.M and Bhura, S.A., Survey of different Web Application Attacks & Its Preventive Measures, IOSR Journal of Computer Engineering (IOSR-JCE), vol. 14, Issue: 5, 2013,pp: 278-287

[14]. Chavan, S.B and Meshram,B.B., Classification of Web Application Vulnerabilities, International Journal of Engineering Science and Innovative Technology (IJESIT), vol. 2, Issue 2, 2013, pp: 743-749.

[15]. Garg, A. and Singh, S., A Review on Web application Security Vulnerabilities, International Journal of Advance Research in Computer Science and Software Engineering, vol. 3, Issue: 1, 2013, pp: 875-880