Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3365 - 3375
Received 20 January 2021; Accepted 08 February 2021.

Dynamic Statistical Data Based Intrusion Detection Scheme in Manet using Fuzzy Rules

A. Anthony Paul Raj [1*], J. K. Kani Mozhi [2]

[1]Research Scholar, Periyar University, Salem, Tamil Nadu, India
[2] Assistant Professor, Dept. of Computer Applications, Sengunthar Arts & Science College, Tiruchengode, Tamil Nadu, India, drjkkanimozhi@gmail.com
* paulraj.apr@gmail.com

ABSTRACT

The Mobile Adhoc Network (Manet) has been well analyzed and explored towards the problem of intrusion detection. To detect the intrusion attack, there exist numerous techniques to handle this issue; even though, they struggle to achieve expected performance. To improve the performance an efficient dynamic statistical data based intrusion detection scheme is presented in this paper. The method handles the intrusion detection according to the statistics about the network which represent the various features like traffic, latency, and throughput, number of service access and so on. According to these statistics, the incoming packet has been analyzed to measure time domain legitimate score (TDLS). The TDLS measure represents the suitability of the incoming packet and represents the trustworthy also. The value of TDLS is measured based on the fuzzy rule available where there are number of rules being generated and maintained according to the statistics considered. Based on the statistic values a specific rule has been selected to measure TDLS value. According to the value of TDLS, the method performs intrusion detection and improves the performance also.

Keywords
Intrusion Detection; Manet; Network Statistics; QoS; TDLS; Trust; MMTA

1.Introduction

The Mobile Adhoc Network (Manet) is the most dominant network being used in modern day computing. The users are allowed to access any service through their mobile devices which encourage them to access various services independent of their location whenever they like. However, the identity and integrity of the user becomes more complicated because, the security of the services and data becomes more risky. Like any other network, the Manet also subject to face number of threats like eavesdrops, modification, spoofing and so on. The network threats in Manet has been handled in variety of ways as simple, the host based approach are used towards this issue. Still, the malicious nodes and adversaries are capable of performing threats and attacks to the services or data being transmitted in the network. Any mobile adhoc network is compound with list of mobile nodes and static base stations.

The mobility of the nodes is not planned and they can move on any direction at different speed. This increases the change in topology and influences the network conditions. Also, this dynamic topology introduces higher frequency of link failure, increases the frequency of route discovery which in turn reflects on the quality of service of the network. For example, consider there is little mobility in the network, then there will be less link failure and the latency will be less. When the frequency of link failure occurs due to higher mobility then route discovery frequency will be

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3365 - 3375
Received 20 January 2021; Accepted 08 February 2021.

higher and in turn it increases the latency and reduces the throughput performance. So this network statistics should be considered for intrusion detection. This paper introduces such an approach which works based on the statistics of topology. The quality of service (Qos) of Manet highly depending on variety of factors . The presence of intrusion attack really affects the QoS of Manet.

By monitoring the QoS parameters, the presence of attack can be identified and the method can make necessary decision in controlling the threat and improves the quality of service of the network. When there exist a intrusion attack, the throughput performance will be reduced and latency will be increased. If there exist a packet drop attack then it affect the throughput performance similarly, the presence of modification attack introduces higher latency. The presence of payload attack introduces higher latency. All these must be considered in detecting the intrusion attack. By considering all these, a fuzzy effected real time statistics based intrusion detection scheme is presented in this paper. The method estimates, time domain legitimate score based on the statistics being considered at the current time and the fuzzy rule at the time.

2. Related Works

There are various methods of intrusion detection has been presented earlier to support Manet. This section explores set of methods associated to the issue. Multi-level behavioral analysis technique used for to detected attack in several states. Such approach is presented in [1], which maintains different packages towards to analysis the user's behavior and generated based on data and features of various levels. Such generated levels are used in detecting intrusion attack. The principal component analysis (PCA) has been used in several problems. The same has been adapted to the problem of intrusion detection which is used to perform feature selection and the classification is performed using naïve bayes classifier [2]. The deep learning networks are used in intrusion detection in [3], which considers the change in behavior of users and by monitoring such changes the intrusion attack has been detected. The flow of data in any network can be used in detecting intrusion attack; such flow based scheme is presented in [4], which classify the incoming flow of packets towards intrusion attack. The classification is performed according to the earlier traffic data in detecting intrusion attack. Similarly, in [9], the author presented an intrusion detection scheme which uses flow of packets and based on the repeating flow the detection is performed. A Chi square feature selection algorithm is presented in [5] to support intrusion detection where the classification is performed using support vector machine.

Comparative studies on various methods of intrusion detection attacks and integrated systems have been analyzed in [6], and present a comparative study of them around various parameters. Similarly in [7], the author presented an Ada boost weak classifier for the detection of intrusion attack where the feature selection is performed with radial basis function and support vector machine is used as classifier. Further an ensemble based approach is presented for intrusion detection where the core vector machine is used as classifier [8]. Similarly In [10], a random sample based negative selection algorithm is used towards intrusion detection. Hybrid approaches are always efficient in performing intrusion detection and such approach is presented in [11], where machine learning algorithms are hybridized and named Do-IDS. The genetic algorithm is used as the classifier. Similarly in [13], different machine learning algorithms are covered towards intrusion detection. In [12], a comparative study of different open source tools which supports intrusion detection has been presented. In [14], a recursive feature elimination based intrusion detection system is presented which uses NSLKDD data set for evaluation. In [15], a

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3365 - 3375
Received 20 January 2021; Accepted 08 February 2021.

time series data based intrusion detection system is presented which uses the network traffic generated at different time space belongs to various protocols of traffic. Different machine learning algorithms are used to evaluate the performance.

In [16], discuss a pattern based network intrusion detection system where the patterns are generated with frequent pattern technique and the classification is performed using apriori rules. In [17], the author discusses a Multi Model Transmission Analysis (MMTA) based intrusion detection which acts over the result of trust weight. The MMTA algorithm produces noticeable result in intrusion detection. In [18-19]Intelligence Intrusion Detection Using PSO with Decision Tree Algorithm for Adhoc Network. The methods discussed in the literature do not support high performance in intrusion detection. They produces higher false ratio which motivate the author in designing more strategic approach.

3.Dynamic Statistical Data Based Intrusion Detection Scheme using Fuzzy Rules

The proposed DSD-IDS (Dynamic Statistical Data) based intrusion detection system works based on the statistics of network data which is being monitored and obtained in different time domain. Based on the statistical data the method generates fuzzy rule according to the statistical data available. The method monitors the network conditions on traffic, latency, throughput, payload and hop count. Using this information, the method generates fuzzy rule which has been used to measure TDLS value to perform intrusion detection.

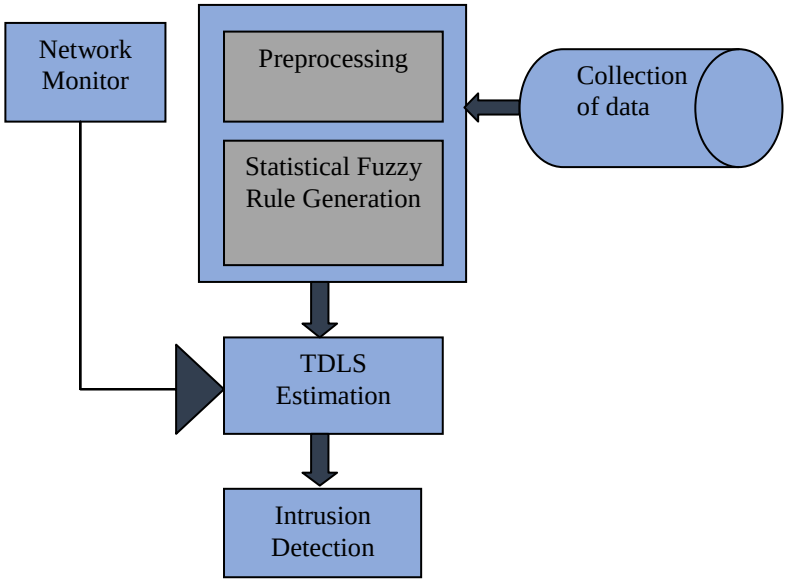

Figure 1: Architecture of proposed Dynamic Statistical data based intrusion detection scheme

The functional architecture of proposed dynamic statistical data based intrusion detection scheme has been presented in Figure 1. The functional components are discussed in detail in this section.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3365 - 3375
Received 20 January 2021; Accepted 08 February 2021.

3.1.Preprocessing

The preprocessing function works as a supportive tool for intrusion detection system. The tool reads the traces generated based on earlier communication and service access performed by various users of the network. Whenever a user accesses the network service, there will be a log generated to the trace about the service access. It generates much information to the log like service accessed, user id, time, date, payload size, hop count detail and so on.
Such log has been preprocessed in this stage. The method reads the log and identifies the different features to be present in each log. Further, each log has been verified for its posses about all the features. If the log contains all the features, then it has been considered as complete, otherwise it is considered as noisy and has been removed from the log. The noise removed data set has been used to generate statistical fuzzy rule.

Consider the data collection contains K number of traces, and then first the method identifies the list of features available in the trace. It has been identified as follows:

$$\text{Feature List Flist} = \int_{i=1}^{\text{size (Dataset)}} \sum(\text{Features} \in \text{Dataset(i)}) \ni \text{Flist} \quad \text{-- (1)}$$

Now, for each trace Ti from data set, the method verifies the presence of all the features, if it contains all the features then it is added to the preprocessed data set. Otherwise, it has been eliminated from the set.

$$\text{Preprocessed set Prds} = \int_{i=1}^{\text{size (Dataset)}} \text{if Dataset(i)} \in \forall \text{Features(Flist)} \rightarrow \text{Prds} \cup \text{Dataset(i)} \quad \text{-- (2)}$$

Preprocessed data set has been used to generate the statistical fuzzy rule set.

3.2.Statistical Fuzzy Rule Generation

The statistical fuzzy rule represents the range of values on different features of quality of service. It has been generated based on the throughput ratio of the network at different time stamp. At each time stamp, the method measures the throughput performance of the service. The method collects the traces on different time stamp and measures the throughput performance, latency, payload, hop count and so on. Based on the values, the method estimates the minimum and maximum value on each Qos parameter. According to the values computed, the method generates fuzzy rule which is used towards intrusion detection.

The time stamp logs are split from the trace as follows:

First the list of time stamp is identified as below:

$$\text{Identify total time stamp Tts} = \sum_{i=1}^{\text{size (Prds)}} \text{Prds(i).Timestamp} \ni \text{Tts}$$

Once the list of time stamp are identified, then the logs belongs to specific time stamp Ti is identified as follows:

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3365 - 3375
Received 20 January 2021; Accepted 08 February 2021.

Time stamp log Tsl = $\sum_{i=1}^{size\ (Prds\ )} Prds(i).TimeStamp == Ti$

Similarly, the logs belong to each time stamp Tk has been identified. Now, at each time stamp Tk, the QoS value has been measured as follows:

Throughput Rate Tr = $\frac{\sum_{i=1}^{size\ (Tsl\ )} Tsl\ (i).state == Success}{Size\ (Tsl\ )}$

Payload Rate Pr = $\frac{\sum_{i=1}^{size\ (Tsl\ )} Tsl\ (i).payload}{Size\ (Tsl\ )}$

Hop count rate Hcr = $\frac{\sum_{i=1}^{size\ (Tsl\ )} Tsl\ (i).Hopcount}{Size\ (Tsl\ )}$

Latency Rate Lr = $\frac{\sum_{i=1}^{size\ (Tsl\ )} Tsl\ (i).Latency}{Size\ (Tsl\ )}$

Frequency support Fr = $\sum_{i=1}^{size\ (Prds\ )} Prds(i).Timestamp == Ti$

Now we have number of values at each time stamp. According to that, the method estimates the minimum and maximum value on each feature considered. Now, we have the fuzzy rule as follows:

	Throughput	**Payload**	**Hop count**	**Latency**	**Frequency**
Minimum	82	25	8	11	65
Maximum	95	60	15	17	120

Table 1: Example Statistical Fuzzy Rule Generated

The Table 1, shows the statistical fuzzy rule generated towards intrusion detection based on the TDLS measure estimated.

3.3.TDLS Estimation

The time division legitimate support (TDLS) represents the trustworthy of the incoming packet being received. It is measured according to the features of the packet being received like payload, hop count and the user frequency of access. Using these measures, the method computes the TDLS value according to the range values present in the statistical rule generated. Estimated TDLS value has been used to perform intrusion detection.

Algorithm:

Input: Packet P, Preprocessed Data set Prds
Output: TDLS

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3365 - 3375
Received 20 January 2021; Accepted 08 February 2021.

Start

Read Packet P, Preprocessed set Prds.
Extract features from packet namely
Payload = $\sum \text{Bytes} \in P$
Hop-count = $\sum \text{Hops} \in P.\text{Route}$
User u = P.User
User Trace ut = $\int_{i=1}^{\text{size (Prds)}} \text{Prds(i).User} == u$
Rule R = Generate Statistical Fuzzy Rule.
Compute Payload Score Ps = $\int \text{payload} < R.\text{payload.min}, R.\text{payloada.max} > 1,0$
Compute hop-count score Hs = $\int \text{hopcount} < R.\text{hopcount.min}, R.\text{hopcount.max} > 1,0$
Compute frequency score Fs = $\int \text{frequency} < R.\text{frequency.min}, R.\text{frequency.max} > 1,0$
Compute latency score Ls = $\int \text{latency} < R.\text{latency.min}, R.\text{latency.max} > 1,0$
Compute TDLS = $\frac{\text{ls}}{\text{Hs}} \times \frac{\text{ps}}{\text{Fs}}$

Stop

The above discussed algorithm represents how the value of TDLS is measured to support the detection of intrusion attack. The method estimates various score values on different features and based on that the method estimates the TDLS value.

3.4.TDLS Intrusion Detection

The proposed TDLS method performs intrusion detection based on the trace generated by earlier access. The method reads the trace and performs preprocessing to eliminate the noisy records. Further, the method generates statistical fuzzy rule based on various features of like latency, payload and hop count with frequency. Using the rule generated, the method estimates the TDLS measure for the incoming packet. Based on the value of TDLS, the method classifies the incoming packet as genuine or malicious.

Algorithm:

Input: Network Log Nl, Packet P
Output: Boolean

Start

Read Nl, P.
Preprocessed set Prds = Preprocessing (Nl)
TDLS = Estimate TDLS(Prds, P)
If TDLS>Th then
    Return true.
Else
    Return false
End

Stop

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3365 - 3375
Received 20 January 2021; Accepted 08 February 2021.

The above discussed algorithm represents how the method estimates TDLS measure and based on the value of TDLS, the method performs intrusion detection.

4. Evaluation Results

The proposed dynamic statistical data based intrusion detection scheme has been implemented and its performance has been evaluated under different circumstances.

Parameter	Value
Tool Used	Advanced Java
Topology Area	1000 meters
MAC Protocol	IEEE 802.11
Routing Protocol	AODV
Mobility Model	Random way point
Transmission range	100 meters
Packet Type	UDP
Packet Size	512 bytes
Mobility speed	3 m/s
Number of Nodes	150
Total iteration	40
Simulation Time	10 minutes

Table 2: Details of Experiment

The details of simulation being used for the performance measurement of proposed TDLS algorithm is presented in Table 2.

4.1.Intrusion Detection Accuracy

The performance on intrusion detection is measured based on the accuracy of detection. For it is measured according to the number of correct classification on specific number of malicious packets.

$$\text{Intrusion detection accuracy} = \frac{\text{Number of Correct Detection Performed}}{\text{Total Number of Intrusion Attack Generated}}$$

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3365 - 3375
Received 20 January 2021; Accepted 08 February 2021.

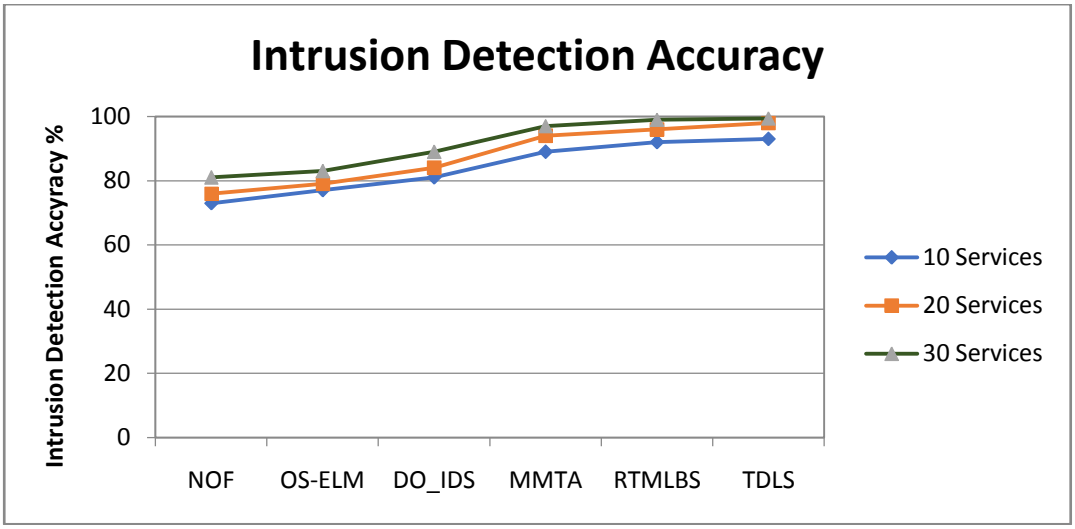

Figure 2: Comparison on intrusion detection performance

The accuracy of intrusion detection produced by different method has been measured and presented in Figure 2. The proposed TDLS algorithm has produced higher accuracy than other methods.

4.3.False Classification Ratio

The false ratio of any algorithm represents the lack of performance in detecting the attack accurately. It is measured using the below formula:

False Ratio = (TF+FT) / (Total Number of Requests)
Here TF = True classified as False, FT = False Classified as True

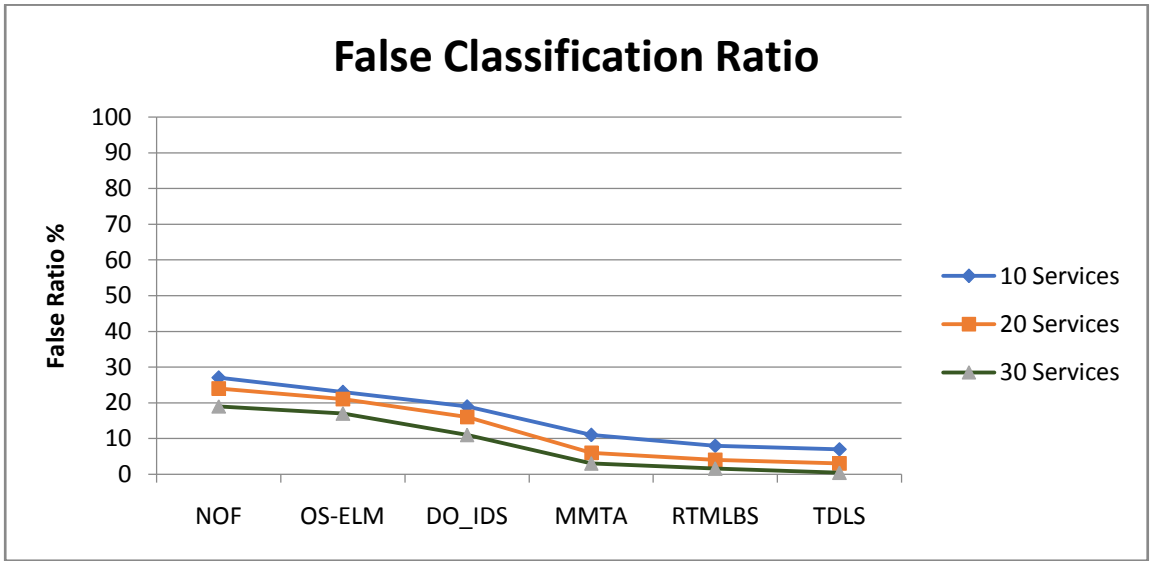

Figure 3: Comparison on False Classification Ratio

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3365 - 3375
Received 20 January 2021; Accepted 08 February 2021.

The false ratio produced by different method has been measured and presented in Figure 3 where the proposed TDLS algorithm produced less false ratio than others.

Method	Detection Rate %	False Ratio %
NOF	81	19
OS-ELM	83	17
DO_IDS	89	11
MMTA	93	7
RTMLBS	96	4
TDLS	99	1.0

Table 3: Performance on various measures

The Table 3, shows the values of different QoS measures estimated under different number of services. The proposed TDLS method has produced higher performance than other methods.

4.4.Time Complexity

The time complexity is the measure which shows the time taken for the detection or classification of incoming packet.

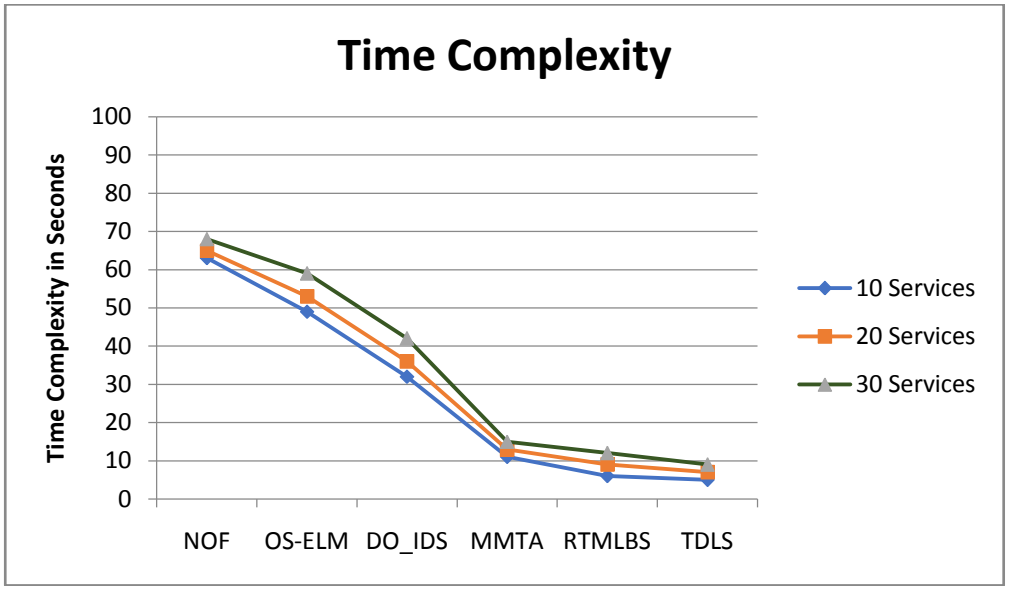

Figure 4: Comparison on time complexity

The performance on time complexity has been measured and presented in Figure 4. The proposed TDLS algorithm has produced less time complexity than other methods.

5.Conclusion

This paper introduced a dynamic statistical data based intrusion detection system with fuzzy rule. The method generates the fuzzy rule by preprocessing the earlier traces of service access and based on that the method computes the time division legitimate score (TDLS) value for the incoming packet. Based on the value of TDLS, the method classifies the class of the packet received. The proposed method improves the performance of intrusion detection and reduces the false alarm ratio with less time complexity.

References

[1] A. Anthony Paul Raj, J. K. Kani Mozhi, (2021). "Real-Time Multi Level Behavioral Analysis Model for Efficient Intrusion Detection in Manet". Malaya Journal of Matematik, Vol. S, No. 1. Pp. 140-144.
[2] Bing Zhang. (2018). Network Intrusion Detection Method Based on PCA and Bayes Algorithm, HINDAWI (SCN).
[3] S. Ramesh, C. Yaashuwanth, K. Prathibanandhi, Adam Raja Basha, T. Jayasankar, "An optimized deep neural network based DoS attack detection in wireless video sensor network", Journal of Ambient Intelligence and Humanized Computing (2020), https://doi.org/10.1007/s12652-020-02763-9
[4] E. Massato Kakihata.(2017). "Intrusion Detection System Based On Flows Using Machine Learning Algorithms. IEEE (LAT). volume 15. pp. 1988-1993.
[5] Suad Mohammed Othaman.(2018).Intrusion detection model using machine learning algorithm on Big Data environment. Springer Open (JBD). Volume 5. Number 34.
[6] G.Mani, V.Nivedhitha, N.S.Pradeep, T.Jayasankar and K.Vinothkumar , "Reliable Wormhole Detection System (RWDS) Based Secure Routing and Authentication for Environmental Monitoring", Journal of Green Engineering (JGE) Vol.10, No.3, pp.734-749,March 2020.
[7] Dai JianJian, (2018). A Novel Intrusion Detection System based on IABRBFSVM for Wireless Sensor Networks ELSEVIER (PCS), Volume 131.Pp 1113-1121.
[8] T.H. Divyasree. (2018). A Network Intrusion Detection System Based On Ensemble CVM Using Efficient Feature Selection Approach, ELSEVIER (PCS), Volume 143, , Pp 442-449.
[9] Kassim S. Mwitondi.(2018).An iterative multiple sampling method for intrusion detection, (ISJAGP).Volume 27. issue 4.
[10] Ruirui Zhang. (2019).Intrusion Detection in Wireless Sensor Networks with an Improved NSA Based on Space Division, HINDAWI (JS).
[11] Jiadong Ren. (2019).Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms. HINDAWI(SCN).
[12] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki. (2019) ."Network Intrusion Detection for IoT Security Based on Learning Techniques," IEEE (CST), volume 21, number 3, pp. 2671-2701.
[13] Wajdi Alhakami. (2019). Alerts Clustering for Intrusion Detection Systems: Overview and Machine Learning Perspectives.(IJACSA). Volume 10. Number 5.
[14] Ripon Patgiri (2018).An Investigation on Intrusion Detection System Using Machine Learning, Research Gate,

[15] Vinayakumar. 2017, R "Applying convolutional neural network for network intrusion detection." (ICACCI), PP 1222-1228.
[16] Bekti CahyoHidayanto, Network Intrusion Detection Systems Analysis using Frequent Item Set Mining Algorithm FP-Max and Apriori, ELSEVIER, Procedia Computer Science, Volume 124, 2017, PP 751-758.
[17] A. Anthony Paul Raj, J. K. Kani Mozhi (2018). Multi Model Transmission Analysis Based Efficient Intrusion Detection System for Improved Performance. Volume-8 Issue-6, Pp 4363 - 4367.
[18] Jiadong Ren. (2019).Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms, HINDAWI, Security and Communication Networks.
[19] R.ArunPrakash, W. R. Salem Jeyaseelan, T.Jayasankar, "Detection, Prevention and Mitigation of Wormhole Attack in Wireless Ad Hoc Network by Coordinator", Appl. Math. Inf. Sci. Vol.12, No.1, Jan 2018, pp.233–237.
DOI: http://dx.doi.org/10.18576/amis/120123
[20] R. Kiruba Buri and T. Jayasankar," Intelligence Intrusion Detection Using PSO with Decision Tree Algorithm for Adhoc Network", Bioscience Biotechnology Research Communications, Special Issue Recent Trends in Computing and Communication Technology, Vol. 12, No.2, March (2019),pp.27-34.

Authors Profile

A. Anthony Paul Raj completed his B.Sc., B.Ed. in Computer Science from, Pope John Paul II College of Education. He completed his M.Sc. in Computer Science from St. Joseph College in Trichy. Bharathidasan University awarded him an M.Phil in Computer Science. He is a Ph.D. Research Scholar at Periyar University. He has 13 years of experience as an Assistant Professor. Network stability is one of his core concerns.

Dr. J. K. Kani Mozhi working as an Assistant Professor, in PG - Department of Computer Applications, Sengunthar Arts & Science College, She has 19 years of teaching experience. Her area of interest is Image processing, Network Security and Data Mining.