Network Security: Approach Based on Network Traffic Prediction

Sheetal Thakare[1(✉)], Anshuman Pund[2], and M. A. Pund[3]

[1] Department of Computer Engineering,
Bharati Vidyapeeth College of Engineering, Navi Mumbai, India
sheetal.thakare@gmail.com
[2] Head Information Security, IDBIIntech, Navi Mumbai, India
anshuman.pund@idbiintech.com
[3] Department of Computer Science and Engineering,
Prof. Ram Meghe Institute of Technology & Research,
Amravati University, Badnera, Amravati, India
mapund@mitra.ac.in

Abstract. Considering the network security aspect, one of the best way of preventing network infrastructure against anomalous activities is to monitor its traffic for suspicious activities. The reliable resource to accomplish this task is past network flow data, which can be analyzed to detect congestions, attacks or anomalies to ensure effective QoS of network infrastructure. Network traffic prediction involves analysis of past network flow data by capturing-storing data, preprocessing data, analyzing it based on various parameters & forming behavior patterns for various nodes in network. Once the patterns are observed for different nodes in network, their future communication can be predicted. Upon prediction of anomalous behavior, the preventive action will be initiated without wasting much of a time. Thus reducing the MTTR (mean time to respond) is the outline of our paper. The importance of network traffic data, traffic prediction methods and literatures available on topic are studied in this paper.

Keywords: Network traffic prediction · ARMA · SARIMA · Time series model

1 Introduction

The various components of network infrastructure like firewalls, bridges, switching and routing devices, etc. produce traffic data related to network. These data are also called as network flow data. Analysis of network performance can be efficiently done using this data. The obtained analysis would be a valuable resource for network security teams for further network enhancement and optimization. The network flow data reflects real-time view of the network traffic, integrated with peripheral devices and point solutions. Peripheral devices form outermost defense line, preventing entry of most of malicious things into the network. Still 100% capture/prevention of the malicious things is impossible. Only single anomaly can wreak dangerous havoc and on getting inside, peripheral devices will be of no help. Even though localized solutions

A. P. Pandian et al. (Eds.): ICCBI 2018, LNDECT 31, pp. 41–55, 2020.
https://doi.org/10.1007/978-3-030-24643-3_5

enhance security by encountering specific problems, broad-based protection is still unreachable for them. Thus even if various components are already present, to strengthen network security, network traffic data analysis and prediction is required (Fig. 1).

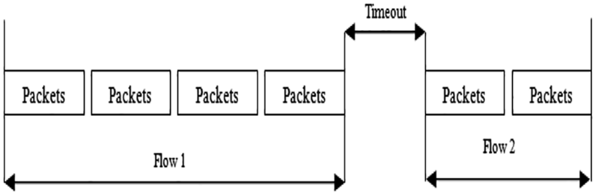


Fig. 1. Network traffic data flow

2 The Importance of Network Traffic Data

A huge amount of data is been produced by traffic that goes from network infrastructure. This is termed as network flow data. It is a good measure for analyzing performance of network. But if this network flow data is scanned to a very root level, it will act as utmost important resource for securing network from various kinds of attacks. Network infrastructure can be optimized with the output of network flow analysis as well as strength will be added to the existing defense mechanism implemented in infrastructure. Strengthening of defense mechanism is possible if mitigating actions can be initiated within no time lag upon attack. This scenario is possible if attack or anomalous behavior can be known or predicted beforehand. Past flow analysis data will help for prediction of anomalous behaviors. If upon prediction, mitigating or preventive actions can be recommended implicitly, then time required to respond to different anomalous network situations will improve drastically.

Other advantages of network flow data analysis are listed below [19] (Table 1).

Table 1. Importance of network traffic data

Network Perceptibility	Network traffic data provides complete internal perceptibility of network
Identified and Unidentified Attacks Detection	Handling know attacks is a huge task along with detection of unknown attacks, e.g. toxic data exfiltration, specially when data is unstructured
Detection of legal user acting unethically	Insider (a legitimate user) can be a hidden threat, which will be detected with who- what- where- when analysis of network flow data
Fasten response time for threat events	To save the network infrastructure from damage quick incident response is the need of hour
Capture policy violations	Network flow analysis captures violations and alerts on policy violations
Support tracing of affected nodes	Network flow analysis can trace nodes communicated with critical data containers, alerts are obtained for such transaction with familiar threats
Network Operations collaborate smoothly	User experience and network system functionality can be reviewed using network data analysis, further helping in capacity planning. Also NetOps and SecOps teams can collaborate smoothly using this analysis resolving problems faster and without pointing fingers at each other
Unefficient node detection	Node responding very slow can be found out and upgraded

(*continued*)

Table 1. (*continued*)

Information Outflow detection	Personal or confidential information flowing out of the network can be captured
Improved resource uasage record	Improved resource usage records can be maintained with real-time network bandwidth usage statistics
Node grouping	Depending on data flow, nodes or devices can be clubbed into logical groups for easier report maintenance

3 Techniques for Network Traffic Prediction

The techniques can be divided as statistical & composite techniques. Statistical techniques use linear & non linear time series data models. Composite (statistical plus other domain) are based on data mining, neural network, Hadoop, PSO etc. Some have used term decomposed models when time series is decomposed into four components. Linear time series techniques are AR (Auto Regressive) and MA (Moving Average). When combined together, they create ARMA (Auto Regressive Moving Average) model [22–24] (Fig. 2, Table 2).

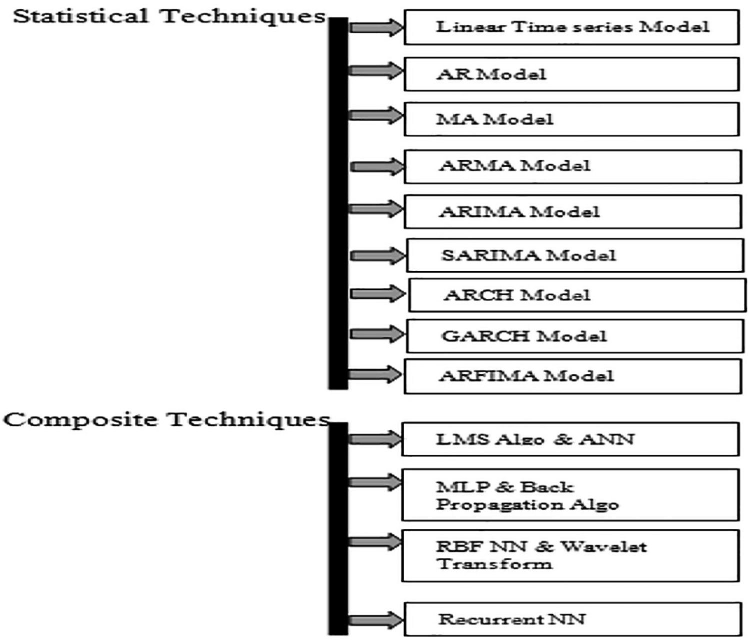
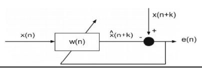
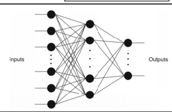
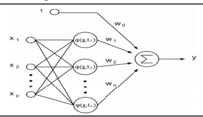
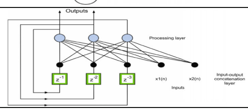


Fig. 2. Network traffic prediction techniques

Table 2. Network traffic prediction techniques details

Statistical Techniques	**Linear time series Model**	Data points are listed in time order, forming a sequence of equally spaced points in time[22].	{z(t)} = {z(1), z(2), ..., z(N)} = {z1, z2, ..., zN }
		t = 1, 2, ..., N, t denotes instances of time when observations are taken, z_i = N observation/ sample realization(i=1 to N)	
	AR Model	Future behavior is predicted using past behavior**.** The prerequisite is correlation between time series data values and succeeding - proceeding values. A*uto*regressive means use only past data to model the behavior.	$\mathbf{X_t = c + \sum_{i=1}^{p} \varphi_i X_{t-i} + \varepsilon_t}$
		X=predictor variable, ε_t= white noise error terms	
	MA Model	Moving-average (MA) model uses univariate time series data. The current as well as past values determine output variable linearly.	$\boldsymbol{X_t = \mu + \varepsilon_t + \theta_1 \varepsilon_{t-1} + \dots + \theta_q \varepsilon_{t-q}}$
		X=predictor variable, ε_t= white noise error terms, μ= series mean , θ_q =model parameters	
	ARMA Model	Two parts of model are an autoregressive (AR) part and a moving average (MA) part. AR part regresses variable on its own lagged values. MA part models error term as a linear combination of error terms at various times in the past. ARMA(*p*,*q*) has *p* as order of the autoregressive part and *q* as order of the moving average part.	$\mathbf{X_t = c + \varepsilon_t + \sum_{i=1}^{p} \varphi_i X_{t-i} + \sum_{i=1}^{q} \theta_i \varepsilon_{t-i}}$
		X=predictor variable, ε_t= white noise error terms, μ= series mean , θ_q =model parameters	
	ARIMA Model	Auto-Regressive Integrated Moving Average(ARIMA). Stationarized series part forecasting equation means "autoregressive, forecast errors means "moving average", and "integrated" means time series differenced to be stationary.	$\mathbf{\hat{y}_t = \mu + \phi_1 y_{t-1} + \dots + \phi_p y_{t-p} - \theta_1 e_{t-1} - \dots - \theta_q e_{t-q}}$
		θs =moving average parameters, y = d^{th} difference of Y, If d=2: $y_t = (Y_t - Y_{t-1}) - (Y_{t-1} - Y_{t-2}) = Y_t - 2Y_{t-1} + Y_{t-2},$ μ= series mean	
	SARIMA Model	Seasonality represents regular pattern of changes in time series, repeating over S, number of time periods after which pattern repeats.	$\Phi(B^S)\varphi(B)(x_t - \mu) = \Theta(B^S)\theta(B)w_t$
		S= number of time periods between repeat ion of patterns, B=backshift operator to produce previous element	
	ARCH Model	Autoregressive conditionally heteroscedastic(ARCH) models variance of a time series. Suitable when increased variations are short in period.	$\boldsymbol{Var(y_t \mid y_{t-1}) = \sigma_t^2 = \alpha_0 + \alpha_1 y_{t-1}^2}$
		y_t =model variance at time t,	
	GARCH Model	Generalized autoregressive conditionally heteroscedastic(GARCH) models variance at time *t* using past squared observations and past variances.	$\boldsymbol{\sigma_t^2 = \alpha_0 + \alpha_1 y_{t-1}^2 + \beta_1 \sigma_{t-1}^2}$
		y_t =model variance at time t,	
	ARFIMA Model	Autoregressive fractionally integrated moving average(ARFIMA) models allow differencing parameter WITH non-integer values. Time series with long memory are modeled by them.	$\boldsymbol{(1 - \sum_{i=1}^{p} \phi_i B^i)(1-B)^d X_t = (1 + \sum_{i=1}^{q} \theta_i B^i)\varepsilon_t}$
		B=backshift operator to produce previous element	
Composite Techniques	**LMS Algo & ANN**	The LMS(Least Mean Square) algorithm trains neural network, minimizing cost (error) function estimates there by encouraging present information storage only[21]. ANN(Adaline neural network) are use only for linearly separable problems.	
	MLP & Back Propagation Algo	MLP (Multilayer Perceptron) neural network resembles to one layer perceptron and it is trained using back propagation algorithm[21].	
	RBF NN & Wavelet Transform	Multilayer network is used for RBF neural network containing one sensory nodes layer, then hidden nodes layer with one output layer.	
	Recurrent NN	Recurrent neural networks(NN) are beneficial for situations where output of one stage acts as input for other and outputs can be random real number from predecided interval.	

4 Network Traffic Prediction System

4.1 System Architecture

See Fig. 3.

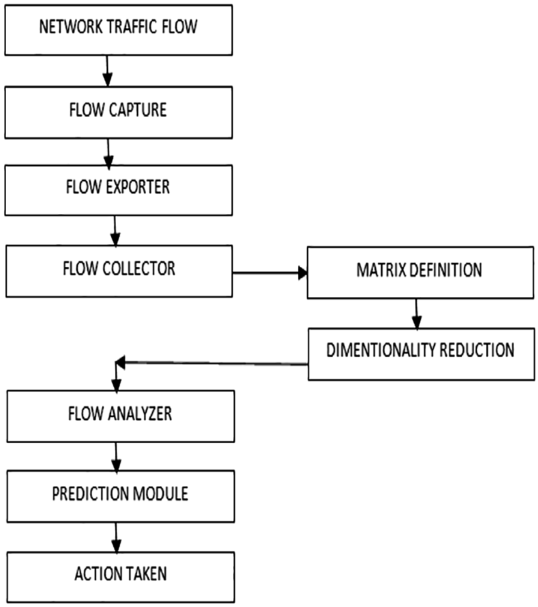


Fig. 3. Prediction system architecture

4.2 Algorithm for Prediction

Step 1: **FLOW CAPTURE -** Packet flow or network flow is captured and stored temporarily to analyze it.
Step 2: **FLOW EXPORTER-** The exporter creates flow registers from network traces.
Step 3: **FLOW COLLECTOR-** The Flow collector generates statistics from the stored file data.
Step 4: **FLOW ANALYZER-** The behavior profiling of each device is created.
Step 5: **PREDICTION MODULE-** Guesses future network flow data & behavior of related nodes.
Step 6: **ACTION TAKEN-** Application or invocation of various security policies, safeguarding actions as per type of attacks will be initiated.

5 Performance Evaluation Metrics

See Tables 3 and 4.

Table 3. Types of metrics used to evaluate network traffic prediction model [28]

Error Type	Formula	Result	Error direction shown	Positive and negative errors effect canceled	Extreme errors penalized	Dependency on measurement scale	Affected by data transformation	Desirable value
The Mean Forecast Error (MFE)	$\mathrm{MFE} = \frac{1}{n}\sum_{t=1}^{n} e_t$	finds the average deviation of forecasted values from actual ones. • the exact amount of positive and negative errors remains unknown • forecasts on proper target are denoted by zero MFE, but may contain error	✓	✓	X	✓	✓	nearest to zero
The Mean Absolute Error (MAE) or Mean Absolute Deviation (MAD)	$\mathrm{MAE} = \frac{1}{n}\sum_{t=1}^{n} \lvert e_t \rvert.$	finds the average absolute deviation of forecasted values from actual ones. • represents magnitude of overall error as a result of forecasting	X	X	X	✓	✓	smallest
The Mean Absolute Percentage Error (MAPE)	$\mathrm{MAPE} = \frac{1}{n}\sum_{t=1}^{n} \left\lvert \frac{e_t}{y_t} \right\rvert \times 100.$	This measure represents the percentage of average absolute error occurred	X	X	X	X	✓	nearest to zero
The Mean Percentage Error (MPE)	$\mathrm{MPE} = \frac{1}{n}\sum_{t=1}^{n} \left(\frac{e_t}{y_t} \right) \times 100$	MPE represents the percentage of average error occurred, while forecasting. • Thus like MFE, by obtaining a value of MPE close to zero, we cannot conclude that the corresponding model performed very well. • It is desirable that for a good forecast the obtained MPE should be small	✓	✓	X	–	–	smallest

(*continued*)

Table 3. (*continued*)

Error Type	Formula	Result	Error direction shown	Positive and negative errors effect canceled	Extreme errors penalized	Dependency on measurement scale	Affected by data transformation	Desirable value
The Mean Squared Error (MSE)	$\mathrm{MSE} = \frac{1}{n}\sum_{t=1}^{n} e_t^2$	It is a measure of average squared deviation of forecasted values. • MSE gives an overall idea of the error occurred during forecasting. • MSE emphasizes the fact that the total forecast error is in fact much affected by large individual errors, i.e. large errors are much expensive than small errors. • Although MSE is a good measure of overall forecast error, but it is not as intuitive and easily interpretable as the other measures discussed before	X	X	✓	✓	✓	smallest
The Sum of Squared Error (SSE)	$\mathrm{SSE} = \sum_{t=1}^{n} e_t^2$	It measures the total squared deviation of forecasted observations, from the actual values	X	X	✓	–	–	smallest
The Signed Mean Squared Error (SMSE)	$\mathrm{SMSE} = \frac{1}{n}\sum_{t=1}^{n} \left(\frac{e_t}{\lvert e_t\rvert}\right) e_t^2$	It is same as MSE, except that here the original sign is kept for each individual squared error	✓	✓	✓	✓	✓	smallest
The Root Mean Squared Error (RMSE)	$\sqrt{\mathrm{MSE}} = \sqrt{\frac{1}{n}\sum_{t=1}^{n} e_t^2}$	RMSE is nothing but the square root of calculated MSE	X	X	✓	✓	✓	smallest

(*continued*)

Table 3. (*continued*)

Error Type	Formula	Result	Error direction shown	Positive and negative errors effect canceled	Extreme errors penalized	Dependency on measurement scale	Affected by data transformation	Desirable value
The Normalized Mean Squared Error (NMSE)	$\mathrm{NMSE} = \frac{\mathrm{MSE}}{\sigma^2} = \frac{1}{\sigma^2 n}\sum_{t=1}^{n} e_t^2$	NMSE normalizes the obtained MSE after dividing it by the test variance. • It is a balanced error measure and is very effective in judging forecast accuracy of a model. • The smaller the NMSE value, the better forecast	X	X	✓	–	–	smallest
The Theil's U-statistics	$\mathrm{U} = \frac{\sqrt{\frac{1}{n}\sum_{t=1}^{n} e_t^2}}{\sqrt{\frac{1}{n}\sum_{t=1}^{n} f_t^2}\sqrt{\frac{1}{n}\sum_{t=1}^{n} y_t^2}}$	It is a normalized measure of total forecast error. • $0 \leq \mathrm{U} \leq 1$;U = 0 means a perfect fit	–	–	–	✓	✓	nearest to zero

Table 4. Network traffic prediction literature study summary

Paper	Methodology	Feature Set	Advantages	Limitations	Futurescopre	Data Set	Evaluation Metric
Introduction to Time Series and Forecasting (2nd Edition) 2002	Auto-regressive integrated moving average (ARIMA)	Autoregressive (AR) - the Historical values; The Moving Average (MA)– the error component	Forecast future network traffic Is accurate within certain threshold	A complex Process and time consuming	Not Applicable		
Towards Forecasting Low Network Traffic for Software Patch Downloads: An ARMA model forecast using CRONOS 2010	Auto-regressive moving average (ARMA)	Auto-regressive moving average	Suitable for short range Forecasting in order to initiate small sized software patch Downloads	Paper does not initiate any form of data transfer. Arma time series model provides suitable forecasting for the Network traffic on a single broadband line	.NET platform can be used to reduce complexity of manual task.	From backbone internet	MAE, MSE, NMSE
Impact of Utilizing Forecasted Network Traffic for Data Transfers 2011	Auto-regressive moving average (ARMA)	Auto-regressive moving average, Arma (6,4) with step size of 30 s	Studies the impact of actual initiation of file transfers When the network traffic is forecasted to be low. This model is Capable of forecasting for short range network traffic. A technique to divide the files into Smaller sizes and transferring them when low network traffic Is forecasted would lead towards a better efficient use of Network bandwidth	Large file not transferred	Forecasting network Traffic can be used to enable more efficient large file transfers	From backbone internet	MSE

(*continued*)

Table 4. (*continued*)

Paper	Methodology	Feature Set	Advantages	Limitations	Futurescopre	Data Set	Evaluation Metric
Prediction of Internet Traffic Based on Elman Neural Network 2009	Neural Network	Time-series measurements Up time	Efficient method for modeling and prediction of traffic. System operations are unaffected by small errors. Provides improved prediction compared with other predictor, nonlinear function approximation capability is better	Normalized Mean square error (nmse) rate greater than farima, ann	NMSE can be improved using	From backbone internet	MAE, MSE, NMSE
PHAD: Packet Header Anomaly Detection 2004	Anomaly detection algorithm (PHAD)	Packet header fields	Attacks with exploits at the transport layer and below are detected, better detection as compared to other models	Training data set attacks reduce PHAD's performance	Needs in depth examination of application layer for performance enhancement	1999 DARPA	Prediction Accuracy
Virtual Network Topology Adaptability based on Data Analytics for Traffic Prediction 2016	The VNT - Virtual network topologies reconfiguration approach based on data analytics for traffic prediction (VENTURE)	Machine learning algorithm based on artificial neural network (ANN)	Minimizing TCO, deactivation of transponders for low traffic hours is possible. Results in low energy requirements with light paths release from optical layer yielding low cost	More transponders need to be installed	Not given	Synergy test-bed	Time Complexity
Traffic Prediction for Dynamic Traffic Engineering 2015	Auto-regressive integrated moving average (arima), seasonal arima (sarima)	Range of short-term fluctuation is found using standard deviation	Traffic variations are predicted using monitored data for long durations. Short duration variations are also considered to counter prediction uncertainty. Changes due to temporal traffic induce uncertainty along with prediction errors	The sampling disadvantages are- inducing sampling errors, and Flows escape unsampled. It is a slow complex process	Predicted traffic needs to be investigated by Sophisticated models	Traffic traces from Education network in the United States	MAPE

(*continued*)

Table 4. (*continued*)

Paper	Methodology	Feature Set	Advantages	Limitations	Futurescopre	Data Set	Evaluation Metric
Advancing Network Flow Information Using Collaborative Filtering 2017	Collaborative Filtering algorithms	Communication of different devices, flow based data	Collaborative Filtering algorithms provide network security domain with an innovative Manner to predict future flows	Better Results in precision but worse in recall	Plan to apply Specific cold-start techniques in order to mitigate rating distribution effect	Unb iscx	Precision, Recall
Prediction of Network Traffic by using Dynamic BiLinear Recurrent Neural Network 2011	Neural Network-*Dynamic-Bilinear Recurrent Neural Network*	–	D-BLRNN predicts with low performance degradation. Comparatively better than other Neural networks in predicting Ethernet network traffic. Bursty traffic prediction possible	Not given	Not given	Ethernet network traffic data set	*NMSE*
Network Traffic Analysis and Prediction Based on APM 2009	Accumulation predicting model (APM)	Seasonal time Series (t),length of each season(d), partial accumulation	Less complicated than ARIMA. AP M is good with stable Seasonal pattern time series	Applicable to stable seasonal pattern time series mostly.	Not given	Chinese mobile network operator	MAPE
ANFIS Method for Forecasting Internet Traffic Time Series	Adaptive neurofuzzy Inference system (ANFIS)	Internet traffic time series	Statistical indicators of method are best. Real data of network fits well into this model with different times condition.	Not given	Not given	From backbone internet over tcp/ip	RMSE, AARE
Identification and Prediction of Internet Traffic Using Artificial Neural Networks,2010	*Artificial neural network*	*Internet traffic data over IP networks,* Levenberg-Marquardt (LM) and the Resilient back propagation (Rp) algorithms using statistical criteria	Traffic over IP network managed very well by this model	Not given	Not given	From backbone internet	RMSE, SI, the Relative Error, MAPE

(*continued*)

Table 4. (*continued*)

Paper	Methodology	Feature Set	Advantages	Limitations	Futurescopre	Data Set	Evaluation Metric
Network Traffic Prediction and Result Analysis Based on Seasonal ARIMA and Correlation Coefficient, 2010	Multiplicative Seasonal autoregressive integrated moving average model (ARIMA) is employed to make traffic series prediction		Yields high precision results. Handles series with seasonal features also	Not given	Not given	heilongjiang province mobile network in china	MAPE
Multi-Scale High-Speed Network Traffic Prediction Using k-Factor Gegenbauer ARMA Model,2004	K-Factor Gegenbauer ARMA	Spectrum of the zero-mean traffic data	Better than AR model	Not given	Useful for building congestion control schemes	LRD series. MPEG and JPEG of star wars movie, Ethernet and Internet traffic	MAE, SER
A Network Traffic Flow Prediction with Deep Learning Approach for Large-scale Metropolitan Area Network,2018	Stacked denoising autoencoder prediction model (SDAPM)	Partition ratio, noise ratio of Gaussian, input data dimension, number of hidden units, binary masking noise probability	Better predictions than MLP. Results are promising.	Not given	Not given	2015 china united network communications two months traffic flow	MAE, MRE, RMSE
Interactive Temporal Recurrent Convolution Network for Traffic Prediction in Data Centers, 2017	Gated recurrent unit (GRU) model, interactive temporal recurrent convolution network (ITRCN)	Minutes, source port, destination port, sun traffic(bytes)	Works with interactive and non interactive network traffics with great accuracy.	Not Given	Can be tested to note influence of days variance on model effectivemess.	Yahoo! Data sets,	RMSE
Network Traffic Prediction Based on Hadoop,2014	Hadoop platform, Echo State Network (ESN), Recurrent Neural Network (RNN)	Phone number, time stamp, the type of application, Location Area Code (LAC), traffic volume	Large scale network records can be processed with ease by parallel prediction models building.	Prediction effected by fluctuation and noise of data series	Not given	Mobile operator data set in china	NMSE, RMSE, MAE

(*continued*)

Table 4. (*continued*)

Paper	Methodology	Feature Set	Advantages	Limitations	Futurescopre	Data Set	Evaluation Metric
Network Traffic Prediction Based on Particle Swarm Optimization, 2016	Hybrid flexible nueral tree & Particle swarm optimization	Variance of size of received packet & receiving packet, number of SYN, RST, FIN packets etc.	The proposed hybrid model based on PSO outperforms SVM & FNT based methods	Not given	Not given	The internet traffic flow data	SVM classifier based method & FNT based method error rates
One new Research on Method of intelligent substation Network Traffic Prediction,2014	A gray neural network model		Network training data required is very small. Yields small errors high accuracy	Not given	Initial network parameters optimization should be studied	Substation network traffic	MSE, prediction error, prediction accuracy

6 Conclusion

With the ever growing network traffic, present is the era of big data. This data can be explored and utilized for prediction of network traffic. This prediction will help to reduce time to respond in case of anomalies. So in this paper we studied and surveyed various network traffic prediction techniques. Prediction methods based on statistic, neural network are discussed. Performance metrics used in various previous studies [10, 13, 16, 18] etc. have been enlisted. The tabular view of surveyed papers focuses on prediction techniques for network traffic. Standard datasets used by the implemented algorithms and metrics used to evaluate the results are grouped in the research works surveyed. Such a review paper would help to provide an insight into the topic to new researchers.

References

1. Wang, J.-S., Wang, J.-K., Zeng, M.-H., Wang, J.-J.: Prediction of internet traffic based on Elman neural network. In: Control and Decision Conference (CCDC ’09), pp. 1248–1252. IEEE (2009)
2. Poo, K.H., Tan, I.K., Chee, Y.K.: Bittorrent network traffic forecasting with ARMA. Int. J. Comput. Netw. Commun. **4**(4), 143 (2012)
3. Mahoney, M.V., Chan, P.K.: PHAD: packet header anomaly detection for identifying hostile network traffic. Technical report, PHAD (2001)
4. Morales, F., Ruiz, M., Gifre, L., Contreras, L.M., López, V., Velasco, L.: Virtual network topology adaptability based on data analytics for traffic prediction. J. Opt. Commun. Netw. **9**(1), A35–A45 (2017)
5. Otoshi, T., Ohsita, Y., Murata, M., Takahashi, Y., Ishibashi, K., Shiomoto, K.: Traffic prediction for dynamic traffic engineering. Comput. Netw. **85**, 36–50 (2015)
6. Park, D.-C., Woo, D.-M.: Prediction of network traffic using dynamic bilinear recurrent neural network. In: Fifth International Conference on Natural Computation (ICNC 2009), vol. 2, pp. 419–423. IEEE (2009)
7. Sadek, N., Khotanzad, A.: Multi-scale high-speed network traffic prediction using k-factor Gegenbauer ARMA model. In: 2004 IEEE International Conference on Communications, vol. 4, pp. 2148–2152. IEEE (2004)
8. Yu, Y., Song, M., Ren, Z., Song, J.: Network traffic analysis and prediction based on APM. In: 2011 6th International Conference on Pervasive Computing and Applications (ICPCA), pp. 275–280. IEEE (2011)
9. Yu, Y., Wang, J., Song, M., Song, J.: Network traffic prediction and result analysis based on seasonal ARIMA and correlation coefficient. In: 2010 International Conference on Intelligent System Design and Engineering Application (ISDEA), vol. 1, pp. 980–983. IEEE (2010)
10. Chabaa, S., Zeroual, A., Antari, J.: Anfis method for forecasting internet traffic time series. In: Microwave Symposium (MMS), 2009 Mediterrannean, pp. 1–4. IEEE (2009)
11. Chabaa, S., Zeroual, A., Antari, J.: Identification and prediction of internet traffic using artificial neural networks. J. Intell. Learn. Syst. Appl. **2**(03), 147 (2010)
12. Brockwell, P.J., Davis, R.A.: Introduction to Time Series and Forecasting. Springer Texts in Statistics, 2nd edn. Springer, New York (2002). https://doi.org/10.1007/b97391. ISBN 0-387-95351-5. SPIN 10850334

13. Tan, I.K.T., Hoong, P.K., Yik, C.: Towards forecasting low network traffic for software patch downloads: an ARMA model forecast using CRONOS. In: Second International Conference on Computer and Network Technology. IEEE (2010). https://doi.org/10.1109/ICCNT.2010.3588. 978-0-7695-4042-9/10 $26.00 © 2010
14. Hoong, N.K., Hoong, P.K., Tan, I.K.T., Seng, L.C.: Impact of utilizing forecasted network traffic for data transfer. In: 13th International Conference on Advanced Communication Technology (ICACT2011), 13–16 February 2011. INSPEC Accession Number: 11930338, Electronic ISBN: 978-89-5519-155-4, Print ISSN: 1738-9445
15. Yonghao, W., Cong, L., Jin, W., Guiping, Z.: One new research on method of intelligent substation network traffic prediction. In: 2014 Fifth International Conference on Intelligent Systems Design and Engineering Applications (2014). Electronic ISBN: 978-1-4799-4261-9
16. Monian-Fa: Network traffic prediction based on particle swarm optimization. In: 2015 International Conference on Intelligent Transportation, Big Data and Smart City, 19–20 December 2015. Electronic ISBN: 978-1-5090-0464-5
17. Cui, H., Yao, Y., Zhang, K., Sun, F., Liu, Y.: Network traffic prediction based on Hadoop. In: 2014 International Symposium on Wireless Personal Multimedia Communications (WPMC), 7–10 September 2014. Electronic ISSN: 1882-5621
18. Cao, X., Zhong, Y., Zhou, Y., Wang, J., Zhu, C., Zhang, W.: Interactive temporal recurrent convolution network for traffic prediction in data centers. In: Special Section on Advanced Data Analytics For Large-Scale Complex Data Environments, pp. 2169–3536 (2017). https://doi.org/10.1109/ACCESS.2017.2787696
19. https://www.flowtraq.com/network-flow-analysis-for-maximum-security/
20. Hall, J., Mars, P.: Limitations of artificial neural networks for traffic prediction in broadband networks. In: Proceedings of the Third IEEE Symposium on Computers and Communications, ISCC 1998, Cat. No. 98EX166, 30 June–2 July 1998. Print ISBN: 0-8186- 8538-7
21. Vieira, F.H.T., Costa, V.H.T., Gonçalves, B.H.P.: Neural network based approaches for network traffic prediction. In: Yang, X.-S. (ed.) Artificial Intelligence, Evolutionary Computation and Metaheuristics, SCI 427, pp. 657–684. Springer, Berlin (2013)
22. https://en.wikipedia.org/wiki/Time_series
23. http://www.statisticshowto.com/autoregressive-model/
24. https://en.wikipedia.org/wiki/Autoregressive_model
25. https://en.wikipedia.org/wiki/Moving-average_model
26. https://en.wikipedia.org/wiki/Autoregressive%E2%80%93moving-average_model
27. https://onlinecourses.science.psu.edu/stat510/node/67/
28. Adhikari, R., Agrawal, R.K.: An Introductory Study on Time Series Modeling and Forecasting. LAP LAMBERT Academic Publishing, 29 January 2013. ISBN-10: 3659335088, ISBN-13: 978-3659335082