A Survey on Hidden Markov Model for IT Service Management

V. Vijayalakshmi[1] (Assistant Professor)
Department of Computer Science and Engineering
CCET (affiliated to Pondicherry University)
Puducherry, India
vivenan09@gmail.com

P. Mahalakshmi[2] (M.Tech-Final Year)
Department of Computer Science and Engineering
CCET (affiliated to Pondicherry University)
Puducherry, India
mahalakshmi2012@gmail.com

S. Thamizharasan[3] (M.Tech-Final Year)
Department of Computer Science and Engineering
CCET (affiliated to Pondicherry University)
Puducherry, India
sthamizhit@gmail.com

Abstract—Network management refers to the actions, techniques, proceedings, and tools that are related to the process, governance, upholding, and stipulating of networked systems. Network management is vital to rule and manage practices and is normally conceded out of a network operations axis. Governance deals with observing the path of resources in the network and how they are allocated. It includes all the maintenance that is needed to keep the network under control. This paper presents a survey of various techniques used in network management and Hidden Markov Model (HMM) that is utilized for IT service management in detail.

Keywords – Hidden Markov Model (HMM); IT service Management; Network Management

I. INTRODUCTION

IT service management (ITSM) refers to the realization and administration of value information technology services. IT service management is executed by IT service contributors through group of people, procedure and information technology. Service management is attracting more and more important within the area of IT management, and functional service provisioning has conveyed a new clash of how to pact with these services so that elevated convenience is assured [1],[2]. How to capably manage and systematize services in convoluted IT service environment with repeated changes is a difficult issue. Furthermore, services and the associated information approaching from diverse sources are characterized as different, partial, assorted, and geologically distributed. Numerals of authors have applied Hidden Markov Models (HMMs) to the task [3], [4], [5].

A Markov model is an easy stochastic procedure based on arbitrary, memory less transition through various sequence of states. In HMMs, we assume that the states themselves are not directly recognizable, but we can formulate some indirect observations, and from these we can estimate the underlying process. HMM is one of the majority popular approaches for modeling time series data [6]. They have extensive applications in areas such as speech identification, bio-informatics, and Internet traffic modeling [7], [8], and more appropriate for finding problems in networks [3], [4], [5]. Once we have trained such a model, we can then look for unlikely order of observations, and use these to network management.

II. LITERATURE REVIEW ON NETWORK MANAGEMENT

Fei Zhang and Wenjun Wu [9] have introduced a novel network traffic classifier PL-CHMM based on Coupled Hidden Markov Models (CHMM) using the Packet- Level features in network traffic gush. Outcome illustrate that PLCHMM based traffic classifier can attain more than 90% accuracy, in classifying each test dataset.

Kave Samalation and Sandrine Vaton [10] have made analysis on performance of real-time appliances on end-to-end packet channels which are powerfully associated to fatalities and temporal delays. Numerous readings demonstrate that these network features may be interconnected and present a definite measure of memory such as bursty fatalities and delays. The memory and the arithmetical reliance among fatalities and temporal delays propose that the channel may be well modeled by a Hidden Markov Model with suitable hidden variables that confine the present state of the network. For this they projected an Input/output Hidden Markov

Model that, skilled with a customized edition of the Expectation- Maximization algorithm, which demonstrates outstanding performance in modeling distinctive channel activities in a set of real packet links. Their work expands to case of variable inter-departure time, the prior proposed Hidden Markov Model that well characterizes fatalities and delays of packets from a intermittent source.

Cesar D. Guerrero1 and Miguel A. Labrador [11] have proposed a Hidden Markov Model-based procedure to end-to-end available bandwidth estimation and supervising that develops the performance metrics and therefore assures to develop the use of these practices in other circumstances. Available bandwidth estimation procedures are being utilized in network supervising and administration tools to afford information concerning the utilization of the network and makes sure the compliance of service level agreements. However, the exercise of these procedures in other functions and network environments is limited by the convergence time, correctness, and total of transparency that they introduce. So they initiated the estimator, which has been put into operation in a new tool called Traceband, is as precise as Spruce and Pathload but significantly quicker, and initiate far less overhead. In adding up, when compared by means of bursty cross-traffic, Traceband is the solitary tool that correctly responds to zero-traffic periods, which may be predominantly useful for those purposes the necessitate to make resolutions in real time.

Alberto Dainotti, Walter de Donato, Antonio Pescap`e and Pierluigi Salvo Rossi [12] have proposed a Hidden Markov Model (HMM) based packet-level traffic classification approach. Traffic classification and recognition is a productive investigates part. Further than Quality of Service, service isolation, and billing, one of the most significant functions of traffic classification is in the meadow of network security. In their proposed approach the classification is carried out by using actual network traffic and estimating - in a collective manner - Packet Size (PS) and Inter Packet Time (IPT) uniqueness, thus enduring appropriate to encrypted traffic too. The usefulness of their proposed approach is estimated by allowing for numerous traffic typologies such as actual traffic sketches of Age of Mythology and Counter Strike (Multi Player Network Games), HTTP, SMTP, Edonkey, PPlive (a peer-to-peer IPTV application), and MSN Messenger. They have specified the systematic basis and the mathematical particulars concerning the model. Outcomes of the projected approach illustrate that are able to classify network traffic by means of packet-level arithmetical properties and therefore it is a good candidate as a module for a multi-classification framework.

Hung X. Nguyen and Matthew Roughan [13] suggest a method, letting multiple parties to together infer a Hidden Markov Model (HMM) for traffic and/or consumer behavior in order to notice anomalies. Finding of malicious traffic and network strength troubles would be much easier if ISPs shared their data. Unluckily, they are disinclined to share because doing so would either go against privacy legislation or render business secrets. On the other hand, secure distributed calculation allows computations to be made using confidential data, without revealing this data. They extended the previous work on HMMs in network security to take account of interpretations from multiple ISPs and extend secure protocols to gather the model parameters without illuminating the confidential data. They implemented a prototype of the protocols, and their testing's with the prototype show a sensible computational and communications overhead, building it realistic for acceptance by ISPs.

III. APPLICATION OF HMM FOR NETWORK MANAGEMENT

A Hidden Markov Model is a finite set of states; each state is related with a probability distribution. Transitions between these states are administered by a set of probabilities called transition probability. In a particular state a possible outcome or observation can be formed, which is related representation of observation of probability distribution. It is only the result, not the state that is marked to a peripheral viewer and consequently states are ``hidden" to the exterior; resulting the name Hidden Markov Model [14].

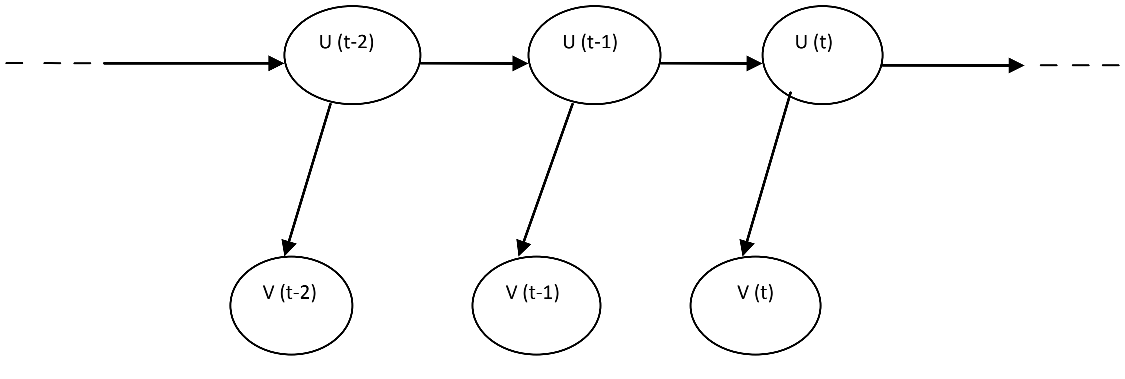

Figure 1. The general architecture of an instantiated HMM.

Figure 1 shows the general architecture of an instantiated HMM. Every elliptical shape signifies an indiscriminate variable that can take on several amounts of values. The arbitrary variable U (t) is the hidden state at time t (U (t) $\in \{U1, U_2, U_3\}$). The random variable V (t) is the scrutiny at time t (with V (t) $\in \{V1, V_2, V_3, V_4\}$). The arrows in the diagram denote conditional dependencies.

From the figure 1, it is obvious that the conditional probability distribution of the hidden variable U(t) at time t, given the values of the hidden variable U at all times, depends only on the significance of the hidden variable U(t − 1): the values at time t − 2 and previous to have no influence. This is called the Markov property. Likewise, the value of the observed variable V(t) only depends on the value of the hidden variable U(t) (both at time t).

In the typical kind of hidden Markov model measured here, the state space of the hidden variables is distinct, while the observations themselves can either be distinct (normally produced from a categorical distribution) or incessant (normally from a Gaussian distribution). The parameters of a hidden Markov model are of two types, transition probabilities and emission probabilities (also known as output probabilities). The transition probabilities organize the approach the hidden state at time t is chosen specified the hidden state at time $t - 1$.

Generally worn administrator servers are based on conventional technique and do not get used to real time. To resolve this difficulty, we suggest a manager server that facilitates supports on Hidden Markov Model and make use of the Modified Censored Production Rules (MCPR) that was given by Hewahi [15] for the following causes such as that allows the arrangement to react over time within the demand of time limitation and also the MCPR arrangement can robust well to assist in construction of the manager server acclimatize with the novel happening and transforms over time.

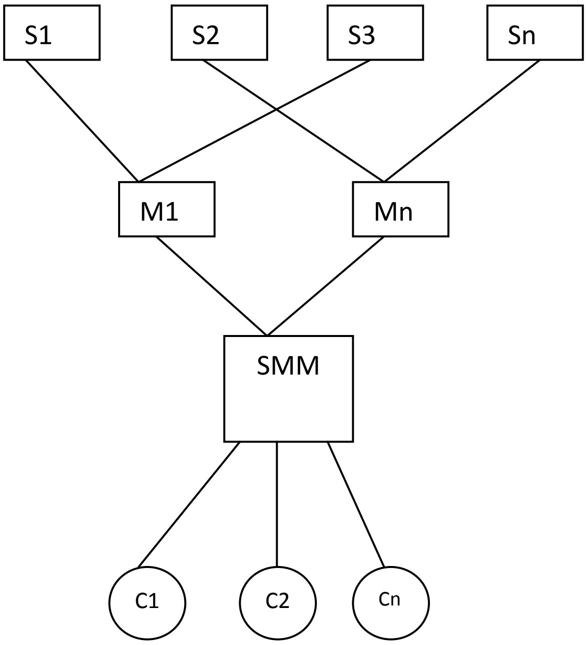

Figure 2. The architecture of the proposed system.

The thought at the back of using Modified Censored Production rules (MCPR) for administrating servers is the capability to settle in them over time based on the varying of the environment such as a crowded server (serving many requests at the same time), failure of other servers, and occasion of some unexpected events. The major plus of using MCPRs is its capability to pact with the events in a real time system style. The advancement which we tag along is anxious for the management from local management server up to the service servers.

In Figure 2, S-n is the nth function server, C-n is the nth client, M-n is the nth manager and SMM is the server main manager. The process would be as follows: The client solicits for a service by sending a request to Server Main Manager which verifies the kind of the request and transfers the request to suitable Manager (M). M assists as a manager for servers on provision that the service for the agreed request. The preferred M will allocate the request to one of its connected servers.

IV. CONCLUSION

In this survey a range of approaches towards network management is been overviewed and a brief discussion of Hidden Markov Model is given which reflects the benefits and ease of HMM. The study shows that Hidden Markov Model can be used for network management. This will be a base for further enhancement of the technique, and resulting into a better management of network. The future work on this can be to make HMM more effective and covering other aspects also.

REFERENCES

[1] A. Keller, “Managing Application Services over Service Provider Networks: Architecture and Dependency Analysis,” Proc. IEEE/ IFIP Network Operations and Management Symp. (NOMS ’00), 2000.

[2] A. Ganek and K. Loeckner, “An Overview of IBM Service Management”. IBM Systems J., vol. 46, no. 3, pp. 375-385, 2007.

[3] D. Ariu, G. Giacinto, and R. Perdisci. “Sensing attacks in computers networks with Hidden Markov Models”. In Proceedings of the Machine Learning and Data Mining in Pattern Recognition - MLDM, pages 449– 463, 2007.

[4] C. Bartolini, L. Gaspary, A. Sperotto, R. Sadre, P.-T. de Boer, and A. Pras. “Hidden Markov Model modeling of SSH brute-force attacks”. In Integrated Management of Systems, Services, Processes and People in IT, pages 164–176. Springer Berlin / Heidelberg, 2009.

[5] Y. Song, S. Stolfo, and T. Jebara. . “Markov models for network-behavior modeling and anonymization”. In Technical reports-Columbia University, http://hdl.handle.net/10022/AC:P:10682, 2011.

[6] L. R. Rabiner. A tutorial on Hidden Markov Models and selected applications in speech recognition. Proc. of the IEEE, 77(2):257–286, February 1989.

[7] H. X. Nguyen and M. Roughan. “SAIL: Statistically Accurate Internet Loss Measurement”. In Proceedings of ACM Sigmetrics 2010 Conference, New York, NY, June, 2010.

[8] C. V. Wright, F. Monrose, and G. M. Masson. “On inferring application protocol behaviors in encrypted network traffic”. J. Mach. Learn. Res., 7:2745–2769, December 2006.

[9] Fei Zhang, Wenjun Wu. “A Network Traffic Classification based on Coupled Hidden Markov Models”. State Key Laboratory of Software Development School of Computer Science, Beihang University

[10] Pierluigi Salvo Rossi, Francesco Palmieri. “Internet Loss-Delay Modeling by Use of Input/Output Hidden Markov Models”. Dipartimento di Informaticae Sistemistica Universit´a di Napoli “Federico II”

[11] Cesar D. Guerrero1 and Miguel A. Labrador . “A Hidden Markov Model Approach to Available Bandwidth Estimation and Monitoring”. University of South Florida Department of Computer Science and Engineering Tampa, Florida 33620

[12] Alberto Dainotti, Walter de Donato, Antonio Pescap`e and Pierluigi Salvo Rossi. “Classification of Network Traffic via Packet-Level Hidden Markov Models”. Department of Computer Science and Systems University of Naples “Federico II”.

[13] Hung X. Nguyen and Matthew Roughan. “Multi-Observer Privacy-Preserving Hidden Markov Models”. School of Mathematical Sciences,The University of Adelaide, Australia.

[14] “HMM-based Integration of Multiple Models for Intrusion Detection”. Chen Xiuqing, Zhang Y ongping, Tang Jiutao. 2010.

[15] Hewahi N., “Hidden markov model for censored production rules”, Proceedings of ICIT’2009, Jordan,2009.