International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-7, Issue-4, July-2019
DOI: 10.21276/ijircst.2019.7.4.3

A Review of Applications and Approaches of Network Monitoring

Asfiya Sultana, Dr. Bhat Geetalaxmi Jairam

Abstract - **Monitoring the network forms an important part of the Network Management, assisting in visualization of the network behaviour in real time. Networks are growing extensively and managing this huge network is utterly challenging. Traffic engineering, quality of service, and anomaly detection also depend on network monitoring for decision making (1). In spite of the ever-increasing complicated networks there are a number of approaches proposed for network monitoring which help to reduce the extra overhead on the network, along with monitoring the entire network as efficiently as possible. This paper lists and studies a few of these Network Monitoring Approaches and also various applications of Network Monitoring.**

Keywords – **Network Traffic, Network Monitoring, Anomaly Detection, Software Defined Networks, Monitoring Agents**

I. INTRODUCTION

Networks are dynamic domains. Network Admins are ceaselessly approached to include new clients, advances and applications to their networks. These progressions can affect their capacity to convey steady, unsurprising system execution. At the point when network issues emerge, Network Admins are constrained to distinguish the underlying driver before it impacts clients, applications and the business. This is increasingly tricky with discontinuous execution issues which are difficult to repeat and analyze. Network Monitoring Systems continuously interact with the network devices to collect data, using standard protocols such as

- SNMP, Simple Network Management Protocol
- WMI, Windows Machine Interface
- SSH, Secure Shell for Unix and Linux server

In this review paper, we walk through various applications and methodologies of network monitoring

II. APPLICATIONS OF NETWORK MONITORING

A. *Detection of Strategic Network Attacks*

Authors Mathieu Dahan, LinaSela, Saurabh Amin studied the generic problem of strategic network inspection, in which a defender (inspection agency) is tasked with detecting the presence of multiple attacks in the network. The defender hasaccess to a limited number of detectors that he/she can randomly position in the network to monitor its components. Their aim was to have minimum number of detectors which can ensure target detection rate. They developed a novel approach to construct an approximate equilibrium strategy profile of the game. This construction could be viewed as a generalization of some of the previously known results in security games, and was scalable to large-scale networks (2).

Detecting and solving coordinated attacks on Networks require a distributed network monitoring infrastructure. Such an infrastructure will have two logically distinct elements: distributed monitors that continuously collect packet and flow-level information, and a distributed query system that allows network operators to efficiently and rapidly access this information (3).

Authors, F. Fischer, F. Mansmann, D. A. Keim, S. Pietzko, and M. Waldvogel, in their paper, presented the NFlowVis system to analyze intrusion detection and flow data. The user interface of the system follows a drill-down metaphor and guiding the analyst from an abstract overview of the overall network activity to aggregated views of IDS data and thorough analysis of attackers, their network traffic, and the victim hosts. In particular, this paper focused on a flow visualization technique combining a TreeMap visualization, a clustering algorithm, and Hierarchical Edge Bundles to group flows in a meaningful way. Three small cases study demonstrated the tool's applicability for exploring potentially successful attacks, for detection of slow and low-volume distributed attacks and for analysis of service usage within our network. (4).

B. *Network Traffic Monitoring & Anomaly Detection*

One of the first tasks of network administrators is monitoring routers and switches for abnormal traffic behaviour like outages, configuration changes, flash crowds and abuse (5).

Manuscript received June 22, 2019

Asfiya Sultana, Information Science & Engineering, The National Institute of Engineering, Mysuru, Karnataka, India,9945301126(e-mail: asfiya.sultana1504@gmail.com)
Dr. Bhat Geetalaxmi Jairam Information Science & Engineering, The National Institute of Engineering, Mysuru, Karnataka, India, 9448297150.,

In this context, an algorithm is proposed based on pattern recognition to help mobile operators to detect anomalies in real time (6).

Tracking Network behaviour and detecting abnormalities in the network traffic has emerged as a vital topic in network monitoring field to detect network attacks. As there is enormous network data flowing at any instant of time, detecting abnormalities in a user's behaviour is difficult and the existing methods face problems such as high processing, high delay and low detection rate. A study proposed a new method to increase the detection rate and efficiency. It proposed to develop a user's traffic behaviour analysis system based on a model of network traffic monitoring. It aims at developing a feature set based on characteristics of the network traffic. This feature set is optimised and used to locate the abnormalities in the network and the user creating the abnormal traffic. The experimental results show that the proposed method has a higher detection rate and lower delay in the analysis of abnormal user's traffic behaviour than that of the existing approaches (7).

A research proposes NOMAD, a scalable network monitoring framework that uses dynamic statistical properties of network traffic for anomaly detection in networks. NOMAD relies on high resolution measurements and on-line analysis of network traffic to provide real-time alarms in the elementary phase of network anomalies (8).

It uses algorithms for anomaly identification based on criteria such as source/destination addresses, packet length etc. Another similar research developed a Network Monitoring system for high-speed network traffic. They developed a general purpose platform for network monitoring for high speed networks. The developed platform formed the basis for performing complex real-time analysis such as application usage behaviour, security analysis, infrastructure planning, etc. (9).

Online network monitoring is challenging because large amount of network data cannot be captured in a finite period of time and in a limited picture. Authors J. Kim and A. Sim in their paper "A New Approach to Online, Multivariate Network Traffic Analysis", propose a new approach that offers an eminent summary of the network traffic with the multivariate analysis. With this approach, the current state of the network will display an abstract pattern compiled from a set of traffic variables, and the detection problems in traffic analysis (e.g., change detection and anomaly detection) can be reduced to a straightforward pattern identification problem (10).

C. *Overlay Network Monitoring*

Monitoring and diagnosis of network conditions is a central problem in any network. As such It has received a lot of attention in the Internet association in general and in the context of overlay networks in particular. Independently, recent advances in network coding have shown that it is possible to increase network capacity and better share the available resources by allowing intermediate nodes to perform processing operations, in addition to just forwarding packets. Network coding techniques can be used to improve several aspects of network monitoring in overlay networks. As a specific application, Fragouli, Christina & Markopoulou, use an approach for the well-known problem of network tomography, and in particular for inferring link loss rates from end-to-end measurements. They demonstrate that their approach will decrease the information measure utilized by probes, improve the accuracy of estimation, and reduce the complexness of choosing methods or trees to send probes (11).

In a separate research, a tomography-based overlay network monitoring system is presented. For an overlay of n end hosts, the space of O(n2) paths can be characterized by a basis of O(n log n)paths. They selectively monitor these basis paths, and then use the measurements to infer the loss rates of all other 220 paths. Both simulation and real implementation on the Internet show that their techniques achieve accurate loss rate estimation (12).

As an improvement to this work, the authors implement and evaluate an algebraic approach for adaptive scalable overlay network monitoring. The approach works in real time, offers fast adaptation to topology changes, distributes balanced load to end hosts, and handles topology measurement errors. Both simulation and real Internet implementation yield promising results (13).

D. *Network Monitoring and Software Defined Networks (SDN)*

Software Defined Networking guarantees to change network management tasks by separating the management plane (a central controller) from the data plane (switches).

Software-defined Networking (SDN) provides a flexible platform for the network monitoring and relies on a central controller to ask switches for traffic statistic to get a global traffic view for security (14).

Network applications use high level interface to monitor network status without being concerned about the low level details. In order to keep the switch design simple, the statistics collection mechanism is implemented as a pull based service. The frequency of polling the switches determines monitoring accuracy and network overhead (15).

New research initiatives, such as virtualization**,** software-defined radios**,** and software-defined networks; allow more flexibility for networks (16).

Programmable networks are now used extensively for the convenience they offer. Installation, Configuration and Upgrade of network elements is done programmatically. OpenNetMon, is an approach and open-supply software implementation to reveal according to-glide metrics, mainly throughput, delay and packet loss, in Open Flow networks. Usually, ISPs over-provision capability a good way to meet QoS needs from customers. Software-Defined Networking and Open Flow allow for higher network control and flexibility inside the pursuit of running networks as correctly as feasible. Where Open Flow presents interfaces to put in force exceptional-grained Traffic Engineering (TE), Open NetMon affords the monitoring vital to determine whether or not cease-to-give up QoS parameters are certainly met and provides the input for TE techniques to compute suitable paths. OpenNetMon polls area switches, i.e. Switches with go with the flow stop-points connected, at an adaptive fee that will increase whilst flow charges range among samples and reduces when flows stabilize to minimize the wide variety of queries. The adaptive rate reduces network and switch CPU overhead while optimizing measurement accuracy (17).

E. Monitoring a virtual network infrastructure

Network monitoring is not an option for a production infrastructure: its administration must keep under control the utilization and the performance of the network, and applications take advantage of input from traffic sensors. One of the basic features of network monitoring in a networking-enabled IaaS is that the output should be adherent to the VLAN abstraction, and that the interface should allow access from the network administrator as well as from network-aware applications. To investigate the issues that are found in the design of a network monitoring infrastructure offered as part of an IaaS, we need to identify the activities that take advantage of its outcomes, starting from the most popular: load balancing (18).

F. Network Monitoring in Multicast Networks

Information contained in robust distributed network codes can be used to deduce possible locations of link failures or losses in a network, without the overhead of additional probes. The system provides worst-case bounds regarding the relationship between failure ambiguity and the coding field size, and we characterize this relationship in more benign networks with experimental simulations. It can bind the required field size and complexity for designing a robust network code that distinguishes among a given set of failure events (19).

G. Monitoring Service for Wireless Sensor Networks

Given the constrained assets of remote sensor arrange framework, information of the traffic created by every hub and administration can be of extraordinary worth. However, bookkeeping and passing on this checking data in this low-asset foundation is testing. Current observing answers for remote sensor organizes either utilize detached checking, requiring a different system, or spotlight just on identifying and investigating disappointments in the sensor arrange. A study presents FAMoS: a flexible active monitoring service to collect wireless sensor network traffic volume and distribution data. The services are provided with limited overhead and is applicable in many contexts. Each node locally collects data about network traffic and then periodically transmits the data to a back-end for further analysis and processing (20).

H. Social Network Monitoring

The basic idea in social network monitoring is to detect sudden changes in the behaviour of a subset of the individuals in the network. Some of the recent methods proposed for monitoring social networks are:

1. Control chart and hypothesis testing methods
2. Bayesian methods
3. Scan methods
4. Time series models (21).

III. APPROACHES TO NETWORK MONITORING

A. Smartphone-based crowd sourcing for network monitoring

Fine-grained monitoring is still an elusive goal because of the always growing size and complexity of today’s networks. Moreover, the increased pervasively of networked applications acts as a centrifugal force that pushes monitoring to the periphery of the network. In this scenario, crowdsourcing is a possible answer to the raw power needs, whereas the smartphone platform helps to incorporate ubiquity and mobility into the mix. The term crowdsourcing has been introduced to denote the process of solving problems with the help of the masses. Differently from outsourcing, where the people hired for performing a service are external to the hiring company but their identity is still relevant, in crowdsourcing the call is open and directed to an undefined audience. Most of crowdsourcing systems are based on the Web, as it provides efficient and inexpensive collaboration tools (22).

B. Use of Automata theory and Under provisioned Query Processor for Network Monitoring

Computer networking protocols have always been appealing candidates for applications of automata theory. Not only are protocols commonly specified as finite-state automata, much of the current technology of implementing and verifying protocols relies on application of automata theory. We can consider the problem of monitoring the execution of network protocols. Suppose a given piece of computer equipment claims to implement a certain network protocol through one of its communication interfaces. A passive monitor can be introduced outside this interface that can watch all the bits travelling to and from the device under test, and check them for some properties. Such a monitor could give important information about the proper running of the protocol (23). In passive network monitoring, the statistics quotes usually show off a large top-to-average ratio. Provisioning a stream query processor to address height rates in this kind of putting may be prohibitively high priced. It is located that there are significant capacity price financial savings to provisioning a network screen for regular statistics prices rather than the most load. A look at observed that controlling the trade-off between provisioning and latency is key to enabling those cost savings (24).

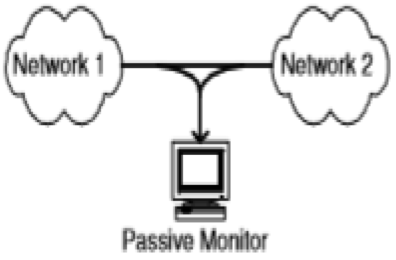

Fig. 1: A Typical Passive Network Monitoring Setup

C. Compressed Network Monitoring

The idea is to accurately monitor performance metrics (e.g., end-to-end delays in an IP network or bit-error rates in an all-optical network) on a collection of n_p end-to-end paths using measurements on a subset of these paths. The size of the subset, $n_s<n_p$, is (ideally) much smaller than the total number of paths (25).

Monitoring end-to-end network properties is often useful to visualize the overall performance of the network. Since, the networks are vast; the measurement of end-to-end properties is not feasible. A study shows that end-to-end network properties may be accurately predicted in many cases using a significantly smaller set of carefully chosen paths than needed for exact recovery (26).

In applications such as routing, each node needs to have information about the current status of the entire network. This itself generates a lot of overhead in the network. A model is proposed in which nodes pick up information from measurements generated by other nodes, an upper bound is derived for the number of measurements that each node must generate, such that the expected number of measurements observed by each node is sufficient to provide a global view of the entire networked data (27).

D. Immersive Network Monitoring

An immersive network monitoring system is used for real-time and retrospective analysis of network traffic. The 3-D representations are designed from the perspective of monitoring traffic at an administrative boundary between the Internet and an internal network. The user is provided with multiple ways of exploring the environment and interrogating visual objects for additional information and synchronizing the environment with external analysis tools. The system has been used on complete data from multiple sites for purposes of situational awareness and detecting and analyzing traffic patterns for anomalous behaviour. The system can present traffic in near real-time or can move back and forth in archived data at any time scale. The use of an animated, immersive, 3dimensional environment with physical metaphors allows us to display large volumes of data from disparate sources as well as data with high degrees of dimensionality. The system provides visual representations that allow analysts, operators, and researchers to explore and discuss network issues in a rich and intuitive environment (28).

E. Network Traffic Monitoring using Graphs

Monitoring network traffic and detecting undesirable applications has come to be a tough hassle, considering the fact that many programs obfuscate their traffic using unregistered port numbers or payload encryption. Apart from some notable exceptions, maximum traffic monitoring tools use two varieties of techniques: (a) preserving traffic records such as packet sizes and inter-arrivals, flow counts, byte volumes, and so on., or (b) reading packet content. Two essential features in network monitoring tools dealing with vast amounts of network data are aggregation and the ability to spot patterns. TDGs represent a natural extension of previous approaches that have aggregated at the packet, flow, and host levels by aggregating across nodes. The aggregation across nodes also reveals patterns of social interaction across nodes that are specific to applications. These interaction patterns or graph structures can then be used to visually and quantitatively monitor existing applications and potentially detect concealed applications and malcode. Assuming that not many diverse applications use the same port number, port-based TDGs can be used to identify the type of application utilizing a given port (29).

Monitoring network traffic and classifying applications are essential functions for network administrators. These tasks are becoming increasingly challenging: (i) many applications obfuscate their traffic using nonstandard ports, and (ii) new applications constantly appear. It suggest the needs for behavioral-based approach, where the detector look for basic behavior of the applications that are both intrinsic to the application and distinct from normal traffic. Identifying intrinsic behaviors makes, it is difficult for application writers to disguise such behaviors without defeating the very purpose of the application. A graph-based representation of network traffic which captures the network wide interactions of applications is proposed. In these graphs, nodes are individual IP address and edges between nodes represent particular communications (30).

Most of the Network Monitoring Solutions include direct measurements of parameters or work on inference, which are usually affected by low precision data or high network overhead. Different from those approaches, we are able to mix the direct measurements offered by software defined network (SDN) and logical thinking techniques supported network pictorial representation to derive a hybrid network monitoring scheme; it can strike a balance between measurement overhead and accuracy (31).

F. Using Agent Mobility for Large-scale and Dynamic Network Monitoring

As networks are becoming pervasive, there is great importance of collecting efficient information for monitoring, maintenance, fault handling, performance evaluation and so on. Distributed monitoring systems manage to deal with scalability issues only to a limited extent, but cannot deal with highly dynamic networks. A study presents an active distributed monitoring system based on mobile agents. Agents are used as area monitors, which are not bound to any particular network node that can “sense” the network, and move around to get better location accuracy. Simulations demonstrate the capability of this approach to cope with large-scale systems and dynamic network conditions (32).

Network Monitoring approaches need to be flexible enough to scale up, as the networks are growing on a rapid pace. One such network monitoring framework is called VISUM. It relies on a distributed set of agents within the network to monitor network devices and store the collected information at data repositories. VISUM's key features are its extensibility for new functionality and its seamless support for new devices and agents in the monitoring framework (33).

G. Remote Network Monitoring Using SDN technologies

The communication networks are constantly changing these days by becoming bigger and more complex (34). As the complexity of the networks grows, the necessities for a better monitoring grow. The conventional methods for network monitoring cannot meet these new demanding situations. Better network monitoring solutions can be put in force by using Software Defined Networking technologies. The efficiency of the proposed solutions can be determined by comparing its performance with any traditional network monitoring method.

H. Network Monitoring using System-level Diagnosis

System-level Diagnosis includes testing a given system to identify which units of the system are faulty and which are fault-free. This diagnosis is applied to LAN, WAN and wireless network monitoring. Most of the diagnosis models assume that, a fault-free tester is used to test if the given unit is fault-free or not. As most real systems are not synchronous, this assumption is actually hard to implement in practice, and thus results in a probabilistic solution (35).

A study proposes that a fault-free tester may not correctly determine the state of the tested unit. It proposes that network monitoring can be done using imperfect tests.

I. Network Monitoring using Real-time Dynamic Information

Networks have been growing ever since they were created. As the size of the networks is massively increasing, monitoring and management of these networks is no longer possible with human effort. Automated network monitoring and management is used to do the job. To keep track of the network traffic, polling is generally used, to poll the network agents for information. This approach increases the load on the network with request-response messages. An efficient way to get real-time information dynamically would be for the agents to send the network information to management entities without the need of request messages. In this approach, each agent decides its monitoring period and sends the same the management station. Thenthe manager collects them and approves every agent's amount while not modification or adjusts it supported the full traffic generated by observation messages (36).

The agents receive a response from the management station about their monitoring period, according to which they send the network information to the latter. A system is proposed to serve as an experimental testbed for determining the efficacy of different human factors and machine learning initiatives on operator performance in network monitoring (37).

This helps to create an adaptive and automated user-interface for network monitoring systems. A study proposed a Computer and Network Asset Manager (CNAM), a network management application, which helps enterprises to have overall updated information about their IT infrastructure at any instant of time. CANM collects information on all hardware components of the network instruments that are on the network (38) and the user is able to view the real-time data via the interface and also can give relevant input to the system.

J. Network Monitoring using M2M sensor systems

An approach was proposed for a network management and monitoring system that will use Machine-to-Machine (M2M) sensor systems, reducing costs through fast isolation of a subpart of the network that is not functional (39). The system consists of a low-cost sensor, with an integrated M2M interface and a web server for management and monitoring of the network. The system aims at integration of data from various network elements and sensors together with the existing systems for managing and monitoring the network, for a better utilization of the collected data.

K. Identifying disruptive routers

Attackers usually target routers in a network to misroute or drop packets passing through those routers. A protocol named WATCHERS is proposed which detects routers that misroute or drop packets passing through them. A WATCHER relies on the principle of conservation of flow in an exceedingly network: all information bytes sent into a node, and not destined for that node, are expected to exit the node WATCHERS tracks this flow and detect routers that violate the conservation principle. (40).

L. Network Monitoring and Scalability

Monitoring the network is a vital component of network operation, but as the networks grow in size, monitoring systems tend to create a significant overhead in the network. A research shows that measurement correlation often exhibited in real networks can be successfully exploited to reduce the network monitoring overhead, it proposes an online adaptive measurements technique with which a subset of nodes are dynamically chosen as monitors while the measurements of the remaining nodes are estimated using the computed correlations (41).

InfiniBand (IB) is communication standard used in high-level computing. As the size of the InfiniBand network grows, predicting the network behavior becomes difficult. Also, there are no efficient approaches that enable the visualization of the network operation and performance in a dynamic way. One of the researches proposed a Monitoring tool – INAM. The tool monitors and analyses InfiniBand clusters and collects information specified by the InfiniBand (42). The system provides a web interface to view the performance of various network components as well as the whole network in real time.

IV. SUMMARY AND CONCLUSION

In this paper, we have summarized a few of the Network Monitoring applications to show the variety of areas wherein Monitoring is involved ,the review includes fields like Social networks, Overlay Networks, InfiniBand etc. It also focuses on the review of numerous approaches, proposals, tools and the systems that try to accomplish the monitoring of the entire network in an efficient way, reducing the overhead, latency, maximizing the precision rate, minimizing the error rate and thereby delivering the service in a cost-effective manner and competent way.

REFERENCES

[1] P.-W. Tsai, C.-W.Tsai, C.-W.Hsu, and C.-S. Yang, “Network Monitoring in Software-Defined Networking: A Review,” IEEE Systems Journal, vol. 12, no. 4, pp. 3958–3969, Dec. 2018.

[2] Mathieu Dahan, LinaSela, Saurabh Amin, “Network Inspection for Detecting Strategic Attacks”. Published on Oct 14, 2018in arXiv: Computer Science and Game Theory

[3] Xin Li, Fang Bian, Hui Zhang, C. Diot, R. Govindan, Wei Hong Hong, and G. Lannaccone, “Advanced Indexing Techniques for Wide-Area Network Monitoring,” 21st International Conference on Data Engineering Workshops (ICDEW’05), 2005.

[4] F. Fischer, F. Mansmann, D. A. Keim, S. Pietzko, and M. Waldvogel, “Large-Scale Network Monitoring for Visual Analysis of Attacks,” Lecture Notes in Computer Science, pp. 111–118.

[5] P. Barford and D. Plonka, “Characteristics of network traffic flow anomalies,” Proceedings of the First ACM SIGCOMM Workshop on Internet Measurement - IMW ’01, 2001.

[6] M. Mdini, A. Blanc, G. Simon, J. Barotin, and J. Lecoeuvre, “Monitoring the network monitoring system: Anomaly Detection using pattern recognition,” 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), May 2017.

[7]Y. Lai, Y. Chen, Z. Liu, Z. Yang, and X. Li, “On monitoring and predicting mobile network traffic abnormality,” Simulation Modelling Practice and Theory, vol. 50, pp. 176–188, Jan. 2015.

[8] R. Talpade, G. Kim, and S. Khurana, “NOMAD: traffic-based network monitoring framework for anomaly detection,” Proceedings IEEE International Symposium on Computers and Communications (Cat. No.PR00250).

[9] B. Kurt, E. Zeydan, U. Yabas, I. A. Karatepe, G. K. Kurt, and A. T. Cemgil, “A Network Monitoring System for High Speed Network Traffic,” 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Jun. 2016.

[10] J. Kim and A. Sim, “A New Approach to Online, Multivariate Network Traffic Analysis,” 2017 26th International Conference on Computer Communication and Networks (ICCCN), Jul. 2017.

[11] Fragouli, Christina &Markopoulou, A. (2005) “A network coding approach to overlay network monitoring”.

[12] Y. Chen, D. Bindel, and R. H. Katz, “Tomography-based overlay network monitoring,” Proceedings of the 2003 ACM SIGCOMM conference on Internet measurement - IMC ’03, 2003.

[13] Y. Chen, D. Bindel, H. Song, and R. H. Katz, “An algebraic approach to practical and scalable overlay network monitoring,” ACM SIGCOMM Computer Communication Review, vol. 34, no. 4, p. 55, Oct. 2004.

[14] S.-H. Shen, “An Efficient Network Monitor for SDN Networks,” ACM SIGMETRICS Performance Evaluation Review, vol. 46, no. 2, pp. 95–96, Jan. 2019.

[15] S. R. Chowdhury, M. F. Bari, R. Ahmed and R. Boutaba, "PayLess: A low cost network monitoring framework for Software Defined Networks," 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, 2014, pp. 1-9.\

[16] D. F. Macedo, D. Guedes, L. F. M. Vieira, M. A. M. Vieira, and M. Nogueira, “Programmable Networks—From Software-Defined Radio to Software-Defined Networking,” IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1102–1125, 2015

[17] N. L. M. van Adrichem, C. Doerr, and F. A. Kuipers, “OpenNetMon: Network monitoring in OpenFlow Software-Defined Networks,” 2014 IEEE Network Operations and Management Symposium (NOMS), May 2014.

[18] A. Ciuffoletti, “Monitoring a virtual network infrastructure,” ACM SIGCOMM Computer Communication Review, vol. 40, no. 5, p. 47, Oct. 2010.

[19]T. Ho, B. Leong, Yu-Han Chang, Yonggang Wen, and R. Koetter, “Network monitoring in multicast networks using network coding,” Proceedings. International Symposium on Information Theory, 2005.ISIT 2005.

[20] J. Maerien, P. Agten, C. Huygens, and W. Joosen, “FAMoS: A Flexible Active Monitoring Service for Wireless Sensor Networks,” Lecture Notes in Computer Science, pp. 104–117, 2012.

[21] Woodall, William & Zhao, Meng&Paynabar, Kamran & Wilson, James. (2016). An Overview and Perspective on Social Network Monitoring. IISE Transactions.49. 10.1080/0740817X.2016.1213468.

[22] A. Faggiani, E. Gregori, L. Lenzini, V. Luconi, and A. Vecchio, “Smartphone-based crowdsourcing for network monitoring: Opportunities, challenges, and a

case study," IEEE Communications Magazine, vol. 52, no. 1, pp. 106–113, Jan. 2014

[23] Bhargavan, Karthikeyan& Chandra, Satish& J. Mccann, Peter & A. Gunter, Carl. (2001). "What Packets May Come: Automata for Network Monitoring". SIGPLAN Notices (ACM Special Interest Group on Programming Languages). 36. 10.1145/373243.360221.

[24] F. Reiss and J. M. Hellerstein, "Declarative Network Monitoring with an Underprovisioned Query Processor," 22nd International Conference on Data Engineering (ICDE'06), 2006

[25] M. Coates, Y. Pointurier, and M. Rabbat, "Compressed network monitoring for ip and all-optical networks," Proceedings of the 7th ACM SIGCOMM conference on Internet measurement - IMC '07, 2007.

[26] D. B. Chua, E. D. Kolaczyk, and M. Crovella, "Efficient monitoring of end-to-end network properties," Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.

[27]A. Fattaholmanan, H. R. Rabiee, P. Siyari, A. Soltani-Farani, and A. Khodadadi, "Peer-to-Peer Compressive Sensing for Network Monitoring," IEEE Communications Letters, vol. 19, no. 1, pp. 38–41, Jan. 2015

[28] Fisk, Mike, Steven A. Smith, Paul M. Weber, Satyam Kothapally and Thomas P. Caudell. "Immersive Network Monitoring." (2003).

[29] Iliofotou, Marios&Pappu, Prashanth&Faloutsos, Michalis&Mitzenmacher, Michael & Singh, Sumeet& Varghese, George. (2007). Network monitoring using traffic dispersion graphs (TDGs). 315-320. 10.1145/1298306.1298349.

[30] M. Iliofotou, "Exploring Graph-Based Network Traffic Monitoring," IEEE INFOCOM Workshops 2009, Apr. 2009.

[31] Z. Hu and J. Luo, "Cracking network monitoring in DCNs with SDN," 2015 IEEE Conference on Computer Communications (INFOCOM), Apr. 2015.

[32] A. Liotta, G. Pavlou and G. Knight, "Exploiting agent mobility for large-scale network monitoring," in IEEE Network, vol. 16, no. 3, pp. 7-15, May-June 2002. doi: 10.1109/MNET.2002.1002994

[33] C. C. Ho, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer, "A scalable framework for wireless network monitoring," Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots - WMASH '04, 2004.

[34]A. I. Frunza, C. I. Rincu, and A. Jitaru, "Remote Network Monitoring Using SDN Based Solutions," 2018 International Conference on Communications (COMM), Jun. 2018

[35] E. T. de Camargo and E. P. Duarte, "Network Monitoring with Imperfect Tests," Proceedings of the 2016 workshop on Fostering Latin-American Research in Data Communication Networks - LANCOMM '16, 2016.

[36] K. S. Shin, J. H. Jung, J. Y. Cheon, and S. B. Choi, "Real-time network monitoring scheme based on SNMP for dynamic information," Journal of Network and Computer Applications, vol. 30, no. 1, pp. 331–353, Jan. 2007.

[37] S. W. Kortschot, D. Sovilj, H. Soh, G. A. Jamieson, S. Sanner, C. Carrasco, S. Ralph, and S. Langevin, "An open source adaptive user interface for network monitoring," 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Oct. 2017.

[38] A. Roohi, K. Raeisifard, and S. Ibrahim, "An application for management and monitoring the data centers based on SNMP," 2014 IEEE Student Conference on Research and Development, Dec. 2014.

[39] G. Suciu, V. Suciu and C. Butca, "Network management and monitoring using M2M sensor systems," 2014 IEEE 20th International Symposium for Design and Technology in Electronic Packaging (SIITME), Bucharest, 2014, pp. 175-178.

[40]K. A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R. A. Olsson, "Detecting disruptive routers: a distributed network monitoring approach," Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat.No.98CB36186).

[41] S. Silvestri, R. Urgaonkar, M. Zafer, and B. J. Ko, "An Online Method for Minimizing Network Monitoring Overhead," 2015 IEEE 35th International Conference on Distributed Computing Systems, Jun. 2015.

[42] N. Dandapanthula, H. Subramoni, J. Vienne, K. Kandalla, S. Sur, D. K. Panda, and R. Brightwell, "INAM - A Scalable InfiniBand Network Analysis and Monitoring Tool," Lecture Notes in Computer Science, pp. 166–177, 2012.

ABOUT THE AUTHORS

Asfiya Sultana, M.Tech in Computer Network Engineering,Information Science and Engineering, The National Institute of Engineering, Mysuru – 08, Karnataka, India

Dr. Bhat Geetalaxmi Jairam, Associate Professor, Information Science and Engineering, The National Institute of Engineering, Mysuru – 08, Karnataka, India