Anomaly Detection In Community Networks

David Kheri

Department of Computer Science
University of Cape Town
South Africa

April 2019

Abstract

In the quest to provide a sustainable solution to address connectivity gaps in rural and remote areas of the world, community networks have been proposed by many as the key to bridge these connectivity gaps. In this literature review, we discuss the research done on community networks, different approaches used in the obtaining of network measurements as well as how we can use different machine learning algorithms on the collected data so as to accurately and efficiently detect anomalies in the network.

CCS Concepts • **Networks** → *Network performance analysis*

Keywords Community Networks,Anomaly Detection, Network Measurements

1. Introduction

Community networks can be referred to as large-scale, self-organized and decentralized networks built with the aim of meeting the communities' communication needs[11].Community networks are usually found in very underserved and remote areas, where network access from commercial network operators is limited to non-existent[11].Considering the fact that technology is advancing at a very rapid rate, there still remains big connectivity gap in urban, rural, remote areas of many developing countries which leaves them at a great disadvantage[10].

In communities where network access is present, network operators usually lack the tools required to accurately give an information of what is happening in the network thus making it very difficult to isolate points of failure in the network and troubleshoot easily[7]. This has prompted research in study of different methodologies for network measurements. For example MONROE project focused on performing measurements in Mobile Brodband networks[5], LiveLab focused on measuring wireless networks using smartphones as an apparatus for network measurements[24].

Despite the different challenges experienced when performing network measurements,the data collected plays a crucial part in the improvement of security in the network[9].

2. Background

Community networks are decentralized communication networks which are large scale and self organized, built by the people for the people [22].

Community networks have taken different shapes and forms from when they originally emerged in the late 90s[19]. Rise of commercial high speed broadband networks has rendered some of the community networks obsolete in the areas they operated while others have prospered especially in the rural areas where connectivity to high speed internet is limited to non existent[19] [19].

2.1 Community Networks

Technically, community networks are built in a decentralized manner [11] implying that the nodes in the network are not dependent on a single server point, which in turn makes the network highly scalable and prevents bandwidth issues as no operational bottlenecks can be caused due to no single server point[19]. At the heart of Community networks are network nodes(also known as routers), these devices either relay network data or provide network access[19]. The links between the network nodes can be wired(DSL,fiber), wireless(WIFI,cellular), both wired and wireless where they complement each other so as to ultimately provide network access to the end user[19]

Currently there are many community networks but considering how informal and unpopular some of them are its impossible to list them all but the following are some of the community networks in the world

- South Africa:Inethi community network that is deployed in Ocean view and Masiphumelele regions in Cape Town[15] and Zenzeleni community network also found in Cape town[29]

- Spain:Guifi.net is a very large network comprising of greater than 20,000 Nodes and more than 24,000 links[6]
- Greece:Athens Wireless Metropolitan Network comprises of more than 2500 nodes[19]

The Networks above are fully operational but still experience some challenges in their operation, preventing further expansion of community networks. For example community networks usually use wireless connectivity, as it is very cost efficient when trying to establish large scale networks but these provide a great challenge since absence of cables will require extensive planning especially in dense suburban areas as channel allocation among competing users in the shared network becomes difficult to achieve correctly[11]. Also Standardization of community networks is also a major challenge as it greatly hinders further growth and sustainability of the present community networks[19].

3. Network Monitoring System

In the world of increasing connectivity its simply not sufficient to create a network[26]. Having a holistic view of the network is essential in the pursuit of optimal performance and reliability within the network[5]. Monitoring of the networks entails observation of the network with the aim of detecting and recovering from failures in the network, which is very crucial for service providers and network operators whenever the need to determine specifically which link or router within the providers network is the cause of poor application performance or total loss of service[13]. Surveillance of the network is not only critical in the provision of a smooth user experience to the end users, but also influence, decisions on the design of future network infrastructures through the collection and analysis of the data collected[5].

Experience from the real world can attest that no single method to monitoring that can highlight every problem in the network, as well as no single factor that can explain all failures and shortcomings in the network. This makes it very difficult to decide what metrics to be used in the monitoring of the network[5].

Measurements have to be performed so as to efficiently and accurately monitor a network, as seen by the shift towards deployment of a number of measurement platforms in the quest of providing network operational support[7]. A number of applications have been implemented so as to provide a clear picture of the network performance eg., Speedtest by Google, Speedtest by OOKLA or running a special measurement application[16]. Drawbacks from applications such as Speedtest is that the measurements taken lack either scalability and repeatability as well as no means of providing a guarantee on the accuracy and availability of the collected metadata eg.,type of device, which operating system its running, location information[5].

Given the drawbacks of some of this applications, further research has been done on following different methodologies on network measurements

3.1 LiveLab

LiveLab is a Methodology employed in the measuring of wireless networks using smartphone users, which was mainly motivated by the fact that there is a significant increase in the number of smartphones in the world and continuing to rise rapidly[24]. It involves leveraging mobile users as a network sampling tool through the collection of data from smartphone users thus providing a more accurate picture of network on analysis of the data[24].
This methodology did experience some practical challenges:

- Mobility of the user caused a significant variation in network quality by the users, which in turn led to a diversity of user experiences in the network[24]
- Privacy as well was also a serious issue as users were afraid of some of the privacy concerns that would occur as a result of logging smartphone activity which was resolved through the anonymizing of the data collected[24].

Despite its practical challenges, LiveLab's main strength was its ability to provide in-field programmability of the logger as that provided researchers with the ability to update the loggger and schedule a new measurement like you would do with a lab computer[24]. This feature is quite useful as it makes measuring of the network very dynamic and in turn adaptable to different scenarios.

3.2 MONROE

MONROE is a tool used to measure and assess mobile brodband networks[21]. Availability of 4G and 4G+ technologies coupled with the increase in number of mobile phones, has led to the explosion of mobile brodband networks[5]. This advancement has prompted the importance of monitoring these networks, with the aim of properly assessing their performance and reliability[5].

Considering the applications used to perform network tests mentioned earlier lacked repeatability and scalability, MONROE is a unique platform built for the aim of conducting repeatable, independent, multihomed, large-scale measurements and experiments in operational mobile broadband networks[21]. MONROE platform comprises of hundreds of nodes scattered over four European countries(Norway, Sweden, Spain, Italy) and a backend system that collects the measurement results[20].

Through the collection of data from operational mobile broadband networks, it enhances fundamental characteristics of mobile brodband networks and the relationship between popular applications and performance of the network[5]. This has proved to be quite beneficial in the provision of feedback on the design of the upcoming 5G technologies as well as improving user experience for mobile users currently still using 3G/4G technologies[5].

4. Anomaly Detection

Anomalies mean differently depending on the applied domain and the problem in question[3]. For example unusual traffic activity in the network could mean a node has been compromised and transmitting data to unauthorized locations, or payments done in a different country for the first time can be a sign of a fraudulent activity[3]. In this context an anomaly can be referred to as unusual behaviour in the network, that does not conform to the expected network activity[2]. Anomalies are very important as they are very rare but significant events and prompt immediate action to be taken as a way to handle such events[2].

Current techniques used in anomaly detection, model the system behaviour and normal network activity and identify anomalies as deviations from the normal network behaviour [12]. Techniques that are currently available, require a profile of normal activity which is different depending on the system, network or application[3]. This approach makes it easier to detect attackers as they are not aware of the system profile thus harder to carry out their activities undetected[9].

Figure 1 displays a generic framework employed in the detection of anomalies in the network. Network traffic data undergoes preprocessing first(which depends on anomaly detection techniques used)[3]. Then, anomaly detection techniques are applied which can be categorized into supervised and unsupervised[3]. Evaluation of the output is done with the use of a label or score[3].

4.1 Challenges of Anomaly Detection

Despite the many techniques available on anomaly detection, difficulties in accurately detecting anomalies include:

- Noisy data can be an anomaly in itself and thus difficult to distinguish between noise and anomaly[9].
- Absence of labelled data to be used in the detection of anomalies[3].
- Since normal examples far outnumber anomalies, it is not feasible to use supervised learning techniques as they require a big data set of labelled data for classification[14].

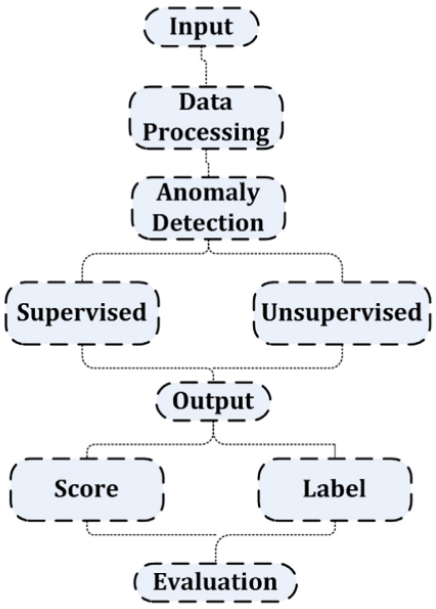

Figure 1. Generic framework for network anomaly detection

- Continuous change of what is considered normal behaviour in the network systems might render some of these technique useless[3].

4.2 Types of Anomalies

To be able appropriately detect an anomaly, it needs to be known from the outset what kind of anomaly is being listened for as there are different types of anomalies and they differ in the nature as explained below,

- Contextual anomaly:this is when an anomaly occurs with respect to a particular context. For example,network usage usually higher than usual during night time as most people are in their homes but if the same behaviour is exhibited during day time that can be flagged as a contextual anomaly[9].
- Collective anomaly:when a group of data points behave anomalous to the rest of the data,that is what is considered a collective anomaly [3].
- Point anomaly:these are anomalies that occur when a particular data point deviates from the normal data pattern for example if a users network usage is less than 500megabytes per day if but if it becomes 10gigabytes on a random day that is a point anomaly[9].

4.3 Output of Anomaly Detection Techniques

As indicated from Figure 1, outputs of common anomaly detection techniques can be represented in two forms which are as described below[3]

- Label:According to many anomaly detection techniques currently present, results are returned in the

form of a label example anomalous for suspicious network activity or normal if the network exhibits normal behaviour[3]

- Score:In this output form anomalies are assigned a value based on a scale usually 0-1 of how anomalous it is and assessed based on a custom threshold set by the network operator or analyst[3] as demonstrated on Table 1 where a threshold of 0.7 was set

Table 1. Table Showing Scores with their Labels

Data Instance	Score	Label
1	0.4	Normal
2	0.2	Normal
3	0.9	Anomalous
4	0.6	Normal

4.4 Type of Network Attacks

With the widespread of network access across the world, more and more users are increasingly vulnerable to network attacks making their digital information and their whole machine as a whole at risk[3].

- Denial of Service:This is the kind of attack that intends to disrupts a machine or network resource from fulfilling its intended purpose and in the process denying the intended users from gaining access to said resource [18]
- Probing:This is an attempt of gathering information about a system, that is looking for weaknesses with the intention of attacking when its least expected and with a bigger probability of escaping undetected[3].
- Remote to User(R2U):In this attack, an attacker tries to gain remote access to a user machine in the network through brute force approaches such as guessing passwords or sniffing user passwords with the purpose of attaining the privilege of sending packets over its network. Also known as Remote to Local Attack[18].
- User to Root(U2R):This attacks aims to gain illegal access to administrative account with the intention of manipulating important resources[18]

4.5 Mapping of Anomaly Types with Network Attacks

Networks attacks discussed can be mapped to different types of anomalies based on the nature of how they manifest themselves in the network as shown in the Figure 2. Denial of Service is mapped to Collective anomaly for example for the case of numerous connections to a web server is a collective anomaly but a single connection is legitimate[3]. Probe attacks which perform a surveillance of the system with a malicious intent can be mapped to contextual anomaly[3]. R2L and U2R can be mapped to point anomaly as these attacks are very sophisticated and not easy compared to perform as compared to others.

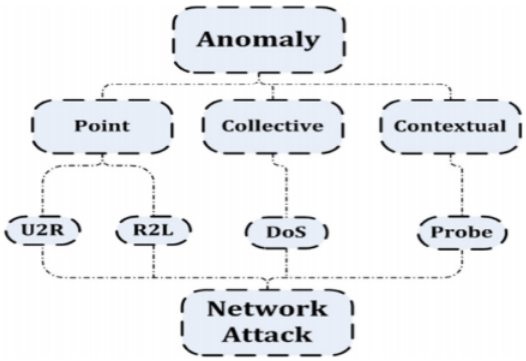

Figure 2. Mapping of Anomaly Types with Network Attacks

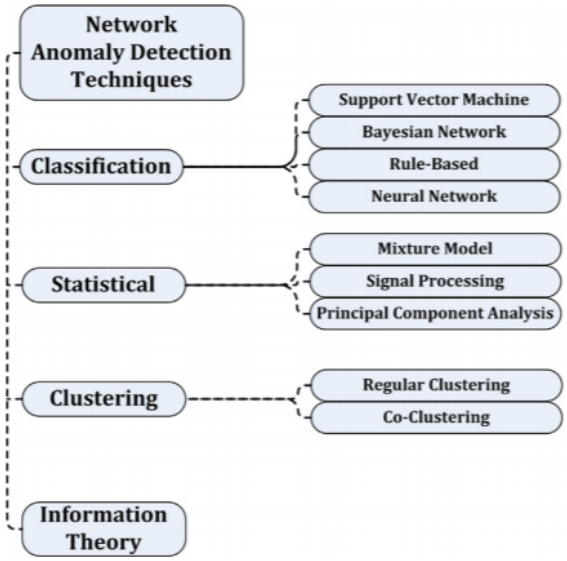

Figure 3. Taxonomy of Anomaly Detection Methods

5. Anomaly Detection Techniques

Network anomaly detection is a broad research topic which contains a number of surveys done on the subject matter. An in-depth survey of anomaly detecting techniques that were created using different machine learning techniques and statistical theories have been discussed[9].

Some work has been done in the context of wireless networks by Sun et al [25]. They present a survey of different intrusion detection techniques that they used for mobile ad-hoc networks(MANET) and wireless

sensor networks(WSN)[25]. They discuss two domain independent online anomaly detection schemes using the location history obtained through the traversal of a mobile user. Sun et al constructed a feature based vector on several parameters such as call duration, call inactivity period, call destination to identify a users calling activity which would be analysed by the use of classification techniques[25].

5.1 Classification Based System

This method mainly relies on experts' knowledge on network attacks, network attacks with a known signature can be quickly and easily detected[3]. This methodology only detects networks attacks that are defined before hand and not easily adaptable to new network attacks which are constantly appearing in different versions and stealthier than ever[3].

This technique relies on a profile of normal traffic activity to be used to establish a baseline and any activity that deviates from what is considered normal is treated as an anomaly[18]. Considering this approach any activity that is considered normal but not within the profile of normal network activity will be considered an anomaly and raise a false alarm which is one of its key weakness[3]. For this method to be used in practice a large enough dataset of what is considered normal traffic data has to be used so as to accurately train the system and reduce the rate of false alarms[3]. The idea of a normal network activity is constantly changing as network environments are always evolving implying what is considered normal today might not be in the near future [3].

An example of classification based Intrusion Detection System is Automated Data Analysis and Mining(ADAM) that provides a testbed for detecting anomalous activity[8]. ADAM couples classification techniques and association rule mining to discover attacks in the tcp-dump audit trail. First, ADAM builds a repository what is considered "normal" frequent data instances from attack free periods[8]. Second, ADAM runs a sliding window based online algorithm that finds frequent data instances in the connections and compares them with those stored in the normal dataset repository, discarding data items that are deemed normal[8]. ADAM uses a classifier that has been trained to be able to classify known and unknown attacks as well as false alarms[8].

Abbes et al introduced an approach that used decision trees with protocol analysis(which is a network sniffer used to capture packet data for further analysis[27]) for effective intrusion detection[1]. They classify data instances into benign or anomalies which included a large variety of attacks such as Dos, botnets, scans. Like any other classifier they require expensive hand labelled datasets and are unable to identify unknown attacks

Classification methods usually give more accurate results than unsupervised methods such as clustering due to the use of labelled training data[9]. Regardless of how popular classification methods are they still can not detect attacks with a signature the classifier is not trained on[9]

5.1.1 Advantages of Classification Based Systems

Classification based methods are popularly used in Intrusion system because of the following reasons

- They have a very high accuracy on detecting known attacks[3]
- They are flexible for training and testing[9]

5.1.2 Disadvantages of Classification based Systems

Classification systems although widely applicable have the following shortcomings

- They can not detect attacks whose signature is not known by the classifier[9]
- They consume more resources than other techniques[9]

5.2 Statistical Based System

Statistical theories have also been employed in anomaly detection, the established chi square theory is used in anomaly detection[28]. According to this technique a profile of normal network activity is created, but when a an event(data instance) has large deviation from normal is considered anomalous and intrusion[28].

Kruger et al proposed a statistical processing unit that could be used to detect rare network attacks such as Remote to user or user to root attacks[17]. In this system a metric would be developed which would allow the system to search automatically identical characteristics of different service request and the anomaly score would be calculated using characteristics such as length of the request, type of request and payload distribution[17].

Another example of a statistical intrusion detection system is Hierarchical Network Intrusion Detection System(HIDE), It uses statistical methods and neural network classifiers to detect intrusions in the network [30]. It is a distributed system with several tiers, with each tier containing a number of intrusion detection agents whose sole task is to monitor the activities of a host or network. HIDE's key strength is its ability to detect UDP flooding attacks even when the attack intensity is as low as 10%[30]

5.2.1 Advantages of Statistical Based Systems

On top of their inherent abilities to detect anomalies the following are other advantages to statistical based systems

- They do not require prior knowledge of normal activities of the target system implying they can learn expected behaviour of the system solely through observations[9]
- They analyse network traffic based on the theory of abrupt changes. Example they monitor a system network traffic for a long time and report when there is an abrupt change[9]

5.2.2 Shortcomings of Statistical based Systems

Statistical based systems although very powerful have the following shortcomings

- It takes a long time to report an anomaly for the first time because the building of the models requires extended time[9]
- They are susceptible to be trained by an attacker in such a way that the network traffic generated during the attack is considered normal[9]
- Setting of different parameters or metrics is very difficult as a right balance is needed unless there will be a large occurrence of either false positives or false negatives depending on the metric chosen[9]

5.3 Clustering Based System

Clustering falls under the set of unsupervised learning algorithms implying that the algorithm does not need labelled data to perform classification[3]. Clustering aims to group or cluster similar data instances together in a cluster. When detecting anomalies using clustering a set of assumptions have to be made

- Assumption1:When you create clusters of only normal data, any following data instances that do not fit well with the existing clusters of normal data are considered anomalies[3]
- Assumption 2:If a cluster contains both anomalous and normal data it has been found that the normal data lies closer to the cluster's centroid but the anomalies are farther away[2]
- Assumption 3:In a clustering with clusters of different sizes the smaller and sparser ones can be considered anomalous while the thicker clusters normal[3].

Sequira and Zaki presented an anomaly detection system known as ADMIT that detects intruders based on user profiles[23]. It does this through keeping track of sequence of commands performed by the user which in turn can be used in the creation of user profiles by clustering the sequence of commands[23]. A sequence that is not similar to the normal user's profile is considered anomalous[23].

Clustering in intrusion detection is very powerful as it does not require labelled data which is very hard to come by[3]. In addition it is very expensive to have a dataset representing every type of anomaly since they can occur in a myriad of ways[14]

5.3.1 Advantages of Clustering based Systems

- it provides a stable performance in comparison to classification and statistical methods[9].
- it does not rely on the availability of labelled data [3]

5.3.2 Disadvantage of Clustering based Systems

- Dynamic updating of profiles is time consuming[9]
- its very difficult to evaluate the technique without assuming that anomalies are usually farther from the cluster's centroid and normal data instances are closer to the cluster's centroid[3]

6. Discussion

After a discussion of the different techniques and systems that are currently used in detecting anomalies in the network, the following observations were made

- No single method can be applied to every anomaly detection problem, as every method has its weakness and strengths. A clear analysis of the nature of the problem to be addressed, is crucial in deciding which anomaly detection method is to be applied.
- Classification based anomaly detection techniques are very accurate, given that the classifier is provided with a large number of training examples which can be obtained using datasets such as NSL-KDD . Although accurate, it fails to identify attacks with signatures the classifier is not trained on and thus can not adapt to new attacks on the fly.
- Anomaly detection techniques that operate in unsupervised mode such as clustering, adapt very well to new attacks as these methods do not rely on labelled data. This implies that they are not bound to what is learnt from the training dataset instead, detect anomalies based on how a data instance is dissimilar from what the algorithm clusters as normal.

7. Conclusion

In this literature review, we have examined what community networks are and briefly discussed also how they are constructed with a few of examples of some of the community networks present. We have also discussed

different techniques, that are presently used in network anomaly detection along with their strength and weaknesses.

If we proceed to implement an intrusion detection system for community networks, the evidence is not clear on which method to use to detect anomalies in community networks as there is not much literature on the anomaly detection in community networks.

Overall, we have identified that there are a few areas that require additional research. Firstly its still not quite clear which anomaly detection techniques are quite suited for community networks. Secondly its also not clear which network attacks are quite prominent in community networks as that can significantly reduce training time if methods such as classification are used.

References

[1] Abbes, T., Bouhoula, A., and Rusinowitch, M. Efficient decision tree for protocol analysis in intrusion detection. *Int. J. Secur. Netw. 5*, 4 (Dec. 2010), 220–235.

[2] Ahmed, M., and Mahmood, A. N. A novel approach for outlier detection and clustering improvement. In *2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA)* (June 2013), pp. 577–582.

[3] Ahmed, M., Mahmood, A. N., and Hu, J. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications 60* (2016), 19 – 31.

[4] Ahmed, M., Mahmood, A. N., and Islam, M. R. A survey of anomaly detection techniques in financial domain. *Future Generation Computer Systems 55* (2016), 278 – 288.

[5] Alay, ., Lutu, A., García, R., Peón-Quirós, M., Mancuso, V., Hirsch, T., Dely, T., Werme, J., Evensen, K., Hansen, A., Alfredsson, S., Karlsson, J., Brunstrom, A., Khatouni, A. S., Mellia, M., Marsan, M. A., Monno, R., and Lonsethagen, H. Measuring and assessing mobile broadband networks with monroe. In *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (June 2016), pp. 1–3.

[6] Baig, R., Roca, R., Navarro, L., and Freitag, F. Guifi.net: A network infrastructure commons. In *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development* (New York, NY, USA, 2015), ICTD '15, ACM, pp. 27:1–27:4.

[7] Bajpai, V., and Schönwälder, J. A survey on internet performance measurement platforms and related standardization efforts. *IEEE Communications Surveys Tutorials 17*, 3 (thirdquarter 2015), 1313–1341.

[8] Barbará, D., Couto, J., Jajodia, S., and Wu, N. Adam: A testbed for exploring the use of data mining in intrusion detection. *SIGMOD Record 30* (2001), 15–24.

[9] Bhuyan, M. H., Bhattacharyya, D. K., and Kalita, J. K. Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys Tutorials 16*, 1 (First 2014), 303–336.

[10] Braem, B., Bergs, J., Blondia, C., Navarro, L., and Wittevrongel, S. Analysis of end-user qoe in community networks. In *Proceedings of the 2015 Annual Symposium on Computing for Development* (New York, NY, USA, 2015), DEV '15, ACM, pp. 159–166.

[11] Braem, B., Blondia, C., Barz, C., Rogge, H., Freitag, F., Navarro, L., Bonicioli, J., Papathanasiou, S., Escrich, P., Baig Viñas, R., Kaplan, A. L., Neumann, A., Vilata i Balaguer, I., Tatum, B., and Matson, M. A case for research with and on community networks. *SIGCOMM Comput. Commun. Rev. 43*, 3 (July 2013), 68–73.

[12] Buczak, A. L., and Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys Tutorials 18*, 2 (Secondquarter 2016), 1153–1176.

[13] Calyam, P., and Swany, M. Research challenges in future multi-domain network performance measurement and monitoring. *SIGCOMM Comput. Commun. Rev. 45*, 3 (July 2015), 29–34.

[14] Hussain, B., Du, Q., and Ren, P. Semi-supervised learning based big data-driven anomaly detection in mobile wireless networks. *China Communications 15*, 4 (April 2018), 41–57.

[15] Inethi. Inethi community network. `http://inethi.org.za/`. Accessed April 29, 2019.

[16] Kreibich, C., Weaver, N., Nechaev, B., and Paxson, V. Netalyzr: Illuminating the edge network. In *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement* (New York, NY, USA, 2010), IMC '10, ACM, pp. 246–259.

[17] Krügel, C., Toth, T., and Kirda, E. Service specific anomaly detection for network intrusion detection. In *Proceedings of the 2002 ACM Symposium on Applied Computing* (New York, NY, USA, 2002), SAC '02, ACM, pp. 201–208.

[18] Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., and Kim, K. J. A survey of deep learning-based network anomaly detection. *Cluster Computing* (Sep 2017).

[19] Micholia, P., Karaliopoulos, M., Koutsopoulos, I., Navarro, L., Baig Vias, R., Boucas, D., Michalis, M., and Antoniadis, P. Community networks and sustainability: A survey of perceptions, practices, and proposed solutions. *IEEE Communications Surveys Tutorials 20*, 4 (Fourthquarter 2018), 3581–3606.

[20] Schwind, A., Seufert, M., Alay, ., Casas, P., Tran-Gia, P., and Wamser, F. Monroe: Measuring mobile broadband networks in europe.

[21] Schwind, A., Seufert, M., Alay, ., Casas, P., Tran-Gia, P., and Wamser, F. Concept and implementation of video qoe measurements in a mobile

broadband testbed. In *2017 Network Traffic Measurement and Analysis Conference (TMA)* (June 2017), pp. 1–6.

[22] Selimi, M., and Freitag, F. Towards application deployment in network clouds. In *Proceedings of the 14th International Conference on Computational Science and Its Applications — ICCSA 2014 - Volume 8584* (Berlin, Heidelberg, 2014), Springer-Verlag, pp. 614–627.

[23] Sequeira, K., and Zaki, M. Admit: Anomaly-based data mining for intrusions. In *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (New York, NY, USA, 2002), KDD '02, ACM, pp. 386–395.

[24] Shepard, C., Rahmati, A., Tossell, C., Zhong, L., and Kortum, P. Livelab: Measuring wireless networks and smartphone users in the field. *SIGMETRICS Perform. Eval. Rev. 38*, 3 (Jan. 2011), 15–20.

[25] Sun, B., Xiao, Y., and Wang, R. Detection of fraudulent usage in wireless networks. *IEEE Transactions on Vehicular Technology 56*, 6 (Nov 2007), 3912–3923.

[26] traviskeshav. Survey of network performance monitoring tools.

[27] Wu, Q.-X. The network protocol analysis technique in snort. *Physics Procedia 25* (2012), 1226 – 1230. International Conference on Solid State Devices and Materials Science, April 1-2, 2012, Macao.

[28] Ye, N., and Chen, Q. An anomaly detection technique based on a chi-square statistic for detecting intrusions into information systems. *Quality and Reliability Engineering International 17*, 2, 105–112.

[29] Zenzeleni. Zenzeleni community network. `http://zenzeleni.net/`. Accessed April 29, 2019.

[30] Zhang, Z., Li, J., Manikopoulos, C. N., Jorgenson, J., and Ucles, J. L. Hide: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification.