Strategic Planning and Monitoring of Network Design

Yiqiao Yin
Ph.D. Student

Abstract

This paper discusses and explores the model architecture of network types. The premise assumes that the role is to create a training document to explore some network types and topology with the interns at a large company. To achieve this task, this paper investigates and provides in-depth overview of the different network types and topologies.

1 Network Operations Center

This assignment investigates the network operations strategy to develop proactive plan to monitor the network performance. The content of the work is designed and built upon the foundation of the previous assignment. The work builds on a variety of understanding including network design, network topology, and network reliability. The plan is to design a real-time monitoring system to measure the network performance and availability. The security of the network is part of the equation as well and will be proactively monitored. In tThe his assignment, we list out comprehensive plans for how to shift strategic plan to focus on Network Operations Center (NOC for short).

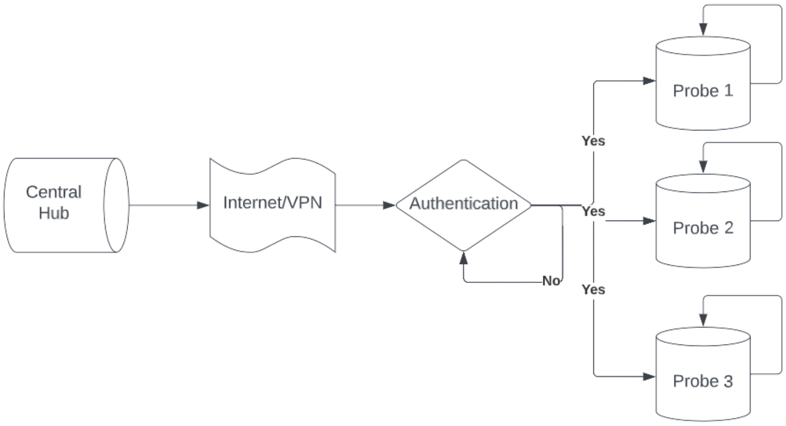
2 Network Performance Monitoring Tools and Probes

Network monitoring is extremely import especially at the scale indicated from previous assignments, i.e. a company operating 150 branches across multiple states in the northeastern region of the United States. The environment is the first thing to discuss and all applications distributed need to be delivered to each station and branch with timely manner. The overall goal is to measure the performance issue as well as a set of other different metrics by supervising the capabilities of network probes. Many scholars have been investigating the systems that adapt large-scale network mapping and the capacity to handle different variety of resources Lowekamp et al. (2003); Matthews and Cottrell (2000); Wolski (1997).

Zangrilli and Lowekamp (2003) proposed a novel solution to measure the network performance by capturing its traffic. When the network probes are available and there is no online traffic required to be measured, the active probes are then recommended to provide a variety of different measures Lowekamp (2003); Zangrilli and Lowekamp (2003). In our case, this solution is recommended to be put to test case. This is because the solution can be an ideal candidate for the scalability of network that is desired to be measured. With over 150 sites traveling all at once, the information hub can really deliver some surprising impact and hence affect the network performance issues. A solid monitoring system needs to be put to place and Lowekamp (2003) proposed a solution especially for this case, because their work targets on the flexibility of the network architecture. The network needs to modify the strategy to adapt to different runtime issues and the potential roadblocks of unavailable bandwidth. Second, the reporting cannot be neglected either, because it is an important step leading to critical performance issues.

One additional concept to discuss in regarding to network performance monitoring tools and probes is the user-level information. This is referring to the specific bandwidth and data transferring efficiency at a level that is benchmark to each user. This can be an important benchmark and metrics to evaluate when it comes measuring large-scale performance issues. Not only do we want to ensure the WAN operates globally without interruption we also want to ensure at a user level contingency plans are at place when any malfunction occurs. MAGNeT allows the network signal to passes through the web traffic and then it measures and categorize the signal. Hence, it is pruned to understand the issues between each layer of stacked internet protocols. LTT, alternatively, is widely used for debugging purposes and it is popular for collecting information on a global level instead of trivial information from each connection.

Figure 1: **Network Operating System (NOS)**. The central hub initiates the signals. The signals goes through the cloud for authentication. When successfully approved, the information is then released to each probe.



Many other tools Mathis et al. (2003); Lowekamp (2003); Gardner et al. (2002); Yaghmour and Dagenais (2000); Callaghan et al. (1994) that are available for us are the following. The Web100 tool provides a variety of different instruments to measure network connectivity issues Mathis et al. (2003). For kernel based tools, MAGNeT and the Linux Trace Toolkit (LTT) can be potential contenders Lowekamp (2003); Gardner et al. (2002).

3 Events to Monitor and Detect Security Issues

Mohanta et al. (2020) provided a list of potential threats and events that are worth monitoring and these events posed danger to security safety.

Table 1: **Summary Table of List of Events**.

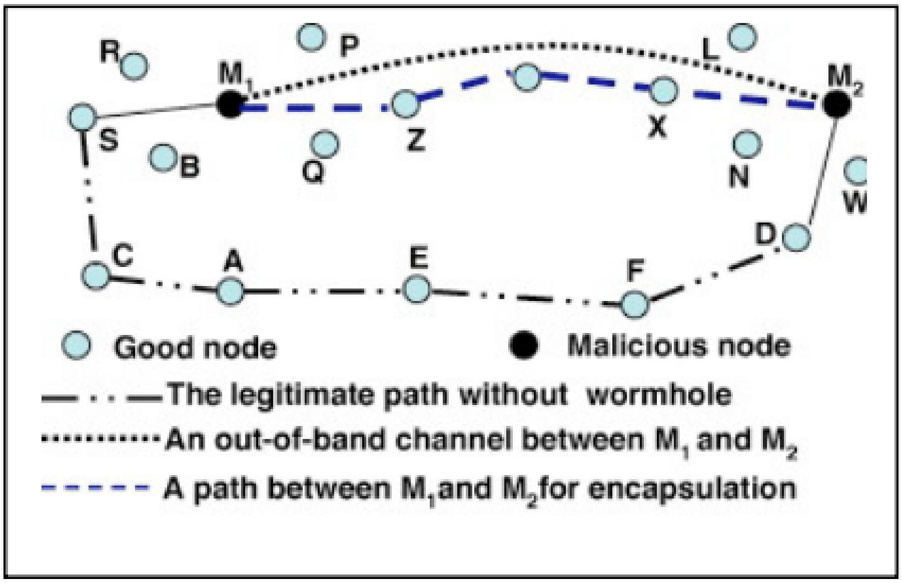
Type	Cite
Jamming	López et al. (2019)
DoS	Baig et al. (2020)
Intrusion Detection System (IDS)	Almiani et al. (2020)
Internal	Tariq et al. (2019)
Access control	Yan et al. (2019)
Wormhole	Deshmukh-Bhosale and Sonavane (2019)

Jamming attack is the first type of event on the list and it is originally introduced by López et al. (2019). It is a type of DoS attacks where the strategy of such attack focus on sending a large volume of signals to affect the reliability of the communication channel. DoS attack, as the most common attack in Internet of Things, is another type of event because it often attacks user at low-end device which usually can be neglected by users Baig et al. (2020). One interesting attack that arise is called Intrusion Detection System (IDS) Almiani et al. (2020). In regarding to this type of attacks, machine learning tools such as anomaly detection can be used to tackle this type of problems. This problem is magnified at today's world because modern day computing technology including networking, data storage, management, and so Almiani et al. (2020) proposed a sequential model to investigate and evaluate the data security. Their work showed improved stability and robustness in regards of performance measure metrics of the dataset on the end-users IoT devices Almiani et al. (2020). Malicious node can be another form of attacks and this type of events focus on the heterogeneous nature of the smart phone or other similar devices that users use. This can be crucial when employees of the companies have their accounts logged into using their remote devices such as iPhone or iPad and they are accessing the internet using public Wifi and so on. Events like this can be an area where malicious attack can take place. Hence, this report proposes to have monitoring system in place. Internal and access attack are orchestrated together simultaneously which then could potentially create this parallel process called a Wormhole attack Tariq et al. (2019); Yan et al. (2019); Deshmukh-Bhosale and Sonavane (2019). Wormhole attack can cause severe damage to the IoT routing Deshmukh-Bhosale and Sonavane (2019). It constructs a tunnel between two users or two machines in the internet topology to design an information passage. The wormhole attack relies on this type of passage to transfer malware across different locations of the system. The diagram of this type of attack is drawn in Figure 2 which is cited from Figure 2 of Deshmukh-Bhosale and Sonavane (2019).

4 Alerts and Notification Responses

In emergency situation where there is a shut down or some malfunction in the network system, the responsive personnel will be notified. This calls for a contingent plan in place. Disregard the channel, some form of notification is needed and the role responsible needs to be checked and put in place. As naive as this may sound, the entire alert and notification responses system essentially refer to the system where a message, an email, or call will be triggered to send to the employee who is in charge of a malfunction situation. Hence, the system is required to be precise and on-time. This is to avoid the scenarios where the person is notified but there is not a malfunction or the person is not notified when there is one. To describe the scenarios thoroughly, denote the scenarios for the signal to be either malfunction or normal and assume the person is either notified or

Figure 2: **Generalized diagram for wormhole attack**. Deshmukh-Bhosale and Sonavane (2019)


R
P
L
M_1
M_2
S
B
Q
Z
X
N
W
D
C
A
E
F
Good node
Malicious node
The legitimate path without wormhole
An out-of-band channel between M_1 and M_2
A path between M_1 and M_2 for encapsulation

not. Hence, we have a two-way table and this gives us $2^2 = 4$ scenarios. This is shown in Table 2. The notification can be passed or not, and hence the situation can either be "yes" or "no". The malfunction can also be positive or negative because there is either an alert or not. This gives 4 unique scenarios. They are true positive, true negative, false negative, and false positive. The two true scenarios are easy to interpret. They refer to the situations where the notification is correct. The incorrect situations can be false negative and false positive. The false negative is when there is not a notification when there is a malfunction. The false positive is when there is a notification but there is no malfunction. The false positive is the classic "crying wolf" situation and the high occurrences of false positives can lead to a potential unvisit when there is a "yes" for notification.

Table 2: **Confusion matrix of alert system correctness**.

		Notified	
		Yes	No
Malfunction	Yes	True Pos.	False Neg.
	No	False Pos.	True Neg.

Hence, based on the above reasoning, there also needs to be a learning procedure in place to improve the notification and alert accuracy when responses are triggered. The end of the channel is the human response. Since it is a human response, psychology and behavioral instinct plays into the equation so that we the designer of this entire strategic monitoring system needs to take this into consideration. This is because it is not just our responsibility to design a complete system. We also need to think in the positions of our employees who are waking up 2AM in the morning to check the system if there is ever a malfunction. They better not be waking up at 2AM and arrive to the factory at

3AM only realizing it is a false positive. This event creates discouragement for these employees to do their job correctly.

The alert and notification system can be quite substantial when we are at the beginning stage designing the network system for a company that has 150 branches operating in the northeastern region of the United States. By setting quick and efficient notification system, the first responders are able to arrive at the scene to tackle the malfunction and any other internet connectivity issues. In addition, a learning system is also recommended to be set up so that the precision and accuracy of the notification/alert can improve.

5 Key Performance Indicators (KPIs)

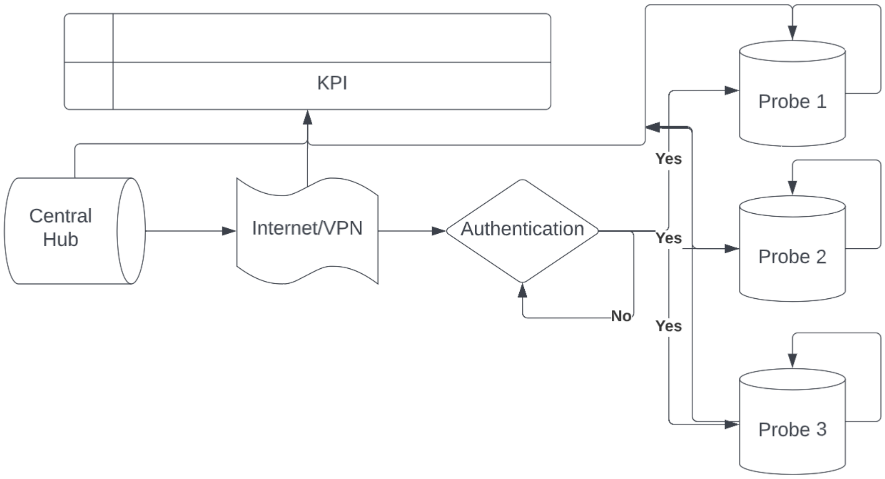
A Key Performance Indicators (KPIs) is a performance measure metric that evaluates the network management. There are several perspectives to be aware of. Here we list them in the following.

First, the KPI needs to efficiently conform the definition of the performance measure. IF there is not a direct link between KPI and the network connectivity status, then the KPI would be not be meaningful. Second, the KPI needs to be understood easily. The description needs to state the issues inside out and every building block needs to be well understood by not just technicians but also management team. The KPI also requires a protocol for action. For various reasons, it is important that the document and the evaluation metrics calls for action. This avoids unnecessary costs in the operation process and the negligible behavior in the corporate management workflow.

6 Visualization and Reporting

The visualization of the proposed reporting system is drawn in Figure 3. The central hub starts with the initiation of the data transfer on a secure network system. The internet and VPN remains in tact and will be required to transfer the data towards each probe. The authentication is set in place to verify the access or request from each probe. The probes serve as branches to ask for data from the central hub upon approval of the internet access.

Figure 3: **Diagram of KPI Reporting System**.



References

Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., and Razaque, A. (2020). Deep recurrent neural network for iot intrusion detection system. *Simulation Modelling Practice and Theory*, 101:102031.

Baig, Z. A., Sanguanpong, S., Firdous, S. N., Nguyen, T. G., So-In, C., et al. (2020). Averaged dependence estimators for dos attack detection in iot networks. *Future Generation Computer Systems*, 102:198–209.

Callaghan, B. P. M. M. D., Hollingsworth, J. M. C. J. K., Karavanic, R. B. I. K. L., and Newhall, K. K. T. (1994). The paradyn parallel performance measurement tools. .

Deshmukh-Bhosale, S. and Sonavane, S. S. (2019). A real-time intrusion detection system for wormhole attack in the rpl based internet of things. *Procedia Manufacturing*, 32:840–847. 12th International Conference Interdisciplinarity in Engineering, INTER-ENG 2018, 4–5 October 2018, Tirgu Mures, Romania.

Gardner, M. K., Feng, W.-c., and Hay, J. R. (2002). Monitoring protocol traffic with a magnet. In *Passive & Active Measurement Workshop*.

López, M., Peinado, A., and Ortiz, A. (2019). An extensive validation of a sir epidemic model to study the propagation of jamming attacks against iot wireless networks. *Computer Networks*, 165:106945.

Lowekamp, B., Miller, N., Karrer, R., Gross, T., and Steenkiste, P. (2003). Design, implementation, and evaluation of the remos network monitoring system. *Journal of Grid Computing*, 1(1):75–93.

Lowekamp, B. B. (2003). Combining active and passive network measurements to build scalable monitoring systems on the grid. *ACM SIGMETRICS Performance Evaluation Review*, 30(4):19–26.

Mathis, M., Heffner, J., and Reddy, R. (2003). Web100: extended tcp instrumentation for research, education and diagnosis. *ACM SIGCOMM Computer Communication Review*, 33(3):69–79.

Matthews, W. and Cottrell, L. (2000). The pinger project: active internet performance monitoring for the henp community. *IEEE Communications Magazine*, 38(5):130–136.

Mohanta, B. K., Jena, D., Satapathy, U., and Patnaik, S. (2020). Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, 11:100227.

Tariq, N., Asim, M., Maamar, Z., Farooqi, M. Z., Faci, N., and Baker, T. (2019). A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered iot. *Journal of Parallel and Distributed Computing*, 134:198–206.

Wolski, R. (1997). Forecasting network performance to support dynamic scheduling using the network weather service. In *Proceedings. The Sixth IEEE International Symposium on High Performance Distributed Computing (Cat. No. 97TB100183)*, pages 316–325. IEEE.

Yaghmour, K. and Dagenais, M. R. (2000). Measuring and characterizing system behavior using {Kernel-Level} event logging. In *2000 USENIX Annual Technical Conference (USENIX ATC 00)*.

Yan, H., Wang, Y., Jia, C., Li, J., Xiang, Y., and Pedrycz, W. (2019). Iot-fbac: Function-based access control scheme using identity-based encryption in iot. *Future Generation Computer Systems*, 95:344–353.

Zangrilli, M. and Lowekamp, B. B. (2003). Comparing passive network monitoring of grid application traffic with active probes. In *Proceedings. First Latin American Web Congress*, pages 84–91. IEEE.