Technical Disclosure Commons

Defensive Publications Series

October 30, 2018

Method To Estimate Network Availability

Vijayaraghavan Bashyam

Nachiappan Valliappan

Method to Estimate Network Availability

Abstract:

A distributed network makes network services available to end users at various nodes or connection points throughout the distributed network's geographic area. A network administrator monitors the performance, capability, and availability of the distributed network to provide the network services. However, the network administrator may be limited to network traffic or other network-side parameters that may not provide an accurate or a conclusive representation of the state of the distributed network. For example, diminished or decreased network traffic could indicate a malfunction in the distributed network or be a natural consequence of a decreased number of end users. Cost, infrastructure requirements, and other limitations prevent installation and operation of a secondary network, which could be used to conclusively determine the conditions of the area within the distributed network. Instead, machine-learning algorithms may monitor and model some features of the distributed network, which may supplement service availability composite metrics, and allow the network administrator to better evaluate the condition of the distributed network without the need of the secondary network.

Keywords:

Network, distributed network, wireless, smart device, WiFi, Bluetooth, Internet-of-Things, IoT, traffic, hotspot, node, access point, machine-learning.

Background:

As the world grows ever more connected, people, machines, cities, and nations increasingly rely on networks that link each to one another. Network administrators tend these networks and make every effort to assure they are consistently available to end users and consistently running at peak performance. However, network administrators can neither know nor

control the circumstances or conditions of the areas in which the networks are located with absolute certainty. The network administrators have many tools at their disposal, but increased information collected about the network, or the conditions of the area in which a network operates, comes at an increased cost in resources and infrastructure and may have implications in matters of privacy. Thus, the network administrators must make educated judgments based on incomplete information when evaluating the performance of a network or making repairs, adjustments, or upgrades to the network.

Description:

A distributed network makes network services available to end users at various nodes or connection points throughout the distributed network's geographic area. A network administrator monitors the performance, capability, and availability of the distributed network to provide the network services. However, the network administrator may be limited to network traffic or other network-side parameters that may not provide an accurate or a conclusive representation of the state of the distributed network. For example, diminished or decreased network traffic could indicate a malfunction in the distributed network or be a natural consequence of a decreased number of end users. Cost, infrastructure requirements, and other limitations prevent installation and operation of a secondary network, which could be used to conclusively determine the conditions of the area within the distributed network. Instead, machine-learning algorithms may monitor and model some features of the distributed network, which may supplement service availability composite metrics, and allow the network administrator to better evaluate the condition of the distributed network without the need of the secondary network.

A distributed network may include something as simple as a device-to-device wireless connection, something as complex as a traffic-control system throughout a metropolitan area or a

large geographic area, or a cellular network that covers entire geographic regions. The distributed network may feature wired connections, wireless connections, or combinations of wired and wireless connections. The distributed network may integrate or coordinate with other networks or systems. For example, the distributed network of traffic control devices throughout a city may also be integrated or coordinated with emergency response systems.

For simplicity purposes, this document focuses on wireless systems, but the principles disclosed herein are equally applicable to other distributed networks, including distributed networks spanning a large geographic area. A generic wireless network includes a series of access nodes or connection points. A hotspot includes a number of access points in a common area or part of a common network scheme. For example, consider the train station hotspot of Figure 1. The train station includes six different wireless access points (labeled as AP1-AP6), including those near a storage closet, the restrooms, a book shop, the ticket counter, and two others within the general indoor waiting area. An end user may connect his or her electronic device to the wireless network at the train station hotspot, which may or may not require specific credentials like a login or a password.

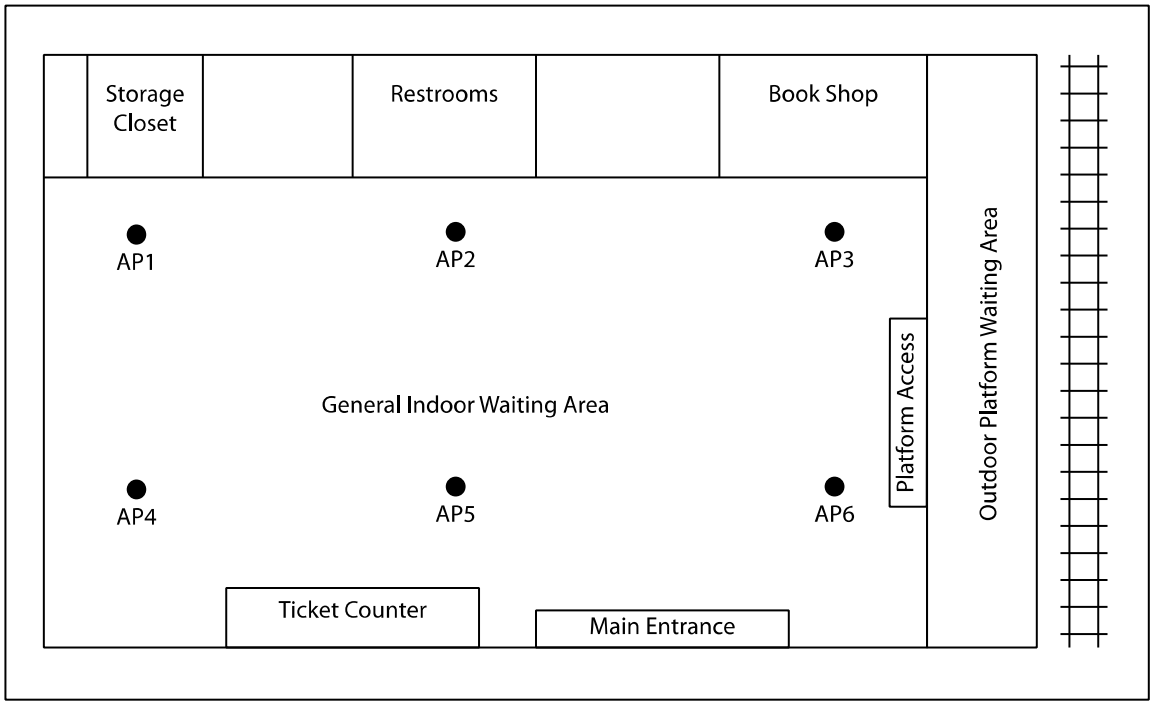

Figure 1

A network administrator monitors the six access points of the train station hotspot. The network administrator could receive telemetry data or other check-in data regarding each individual access point. The telemetry data could include a record of the number of bytes downloaded, a number of bytes uploaded, a number of connected user devices, or other such traffic-related data. Although the telemetry data may provide insight into the operation of the access point (or could be aggregated over the entire hotspot), the telemetry data may not reflect an objective state of the access point. For example, a decrease in bytes uploaded or downloaded could be interpreted as a potential problem or malfunction at the access point. However, the access point may be functioning correctly, and another explanation may account for the change in data traffic at the access point. Consider the book shop at the train station, which also sells snacks and drinks. A spilled drink could redirect wireless device users to a different location within the train station, which may decrease the traffic at the wireless access point near the book shop and inaccurately

imply the wireless access point is not functioning correctly. In a hotspot the size of the train station, a network administrator could visually determine the alternate cause for a change in the traffic at the access point. However, in a distributed network spanning a large geographic area like the traffic control or lighting systems of New York City, manual visual inspection or investigation into changes in traffic patterns at individual streetlight access points would overwhelm any manual investigation or confirmation system.

In a distributed network like the train station, the distributed network serves as more than just a conduit for providing a strong internet connection to end users to accomplish end-user-initiated tasks. A distributed network can also provide information or services not specifically requested by end users. For example, in the event of a missing child, distributed networks spanning a large geographic area send amber alerts or other notifications to all users within the distributed network. Distributed networks can also provide additional information regarding inclement weather, traffic congestion, planned disruption of network services because of routine maintenance, special time-dependent deals, or the like. However, if a network administrator is unable to confirm that the distributed network is available to end users, the additional information may never make it to the end users within the distributed network while the additional information remains relevant.

The current disclosure describes ways to use machine-learning algorithms to reduce false positives by quantitatively evaluating the availability of a node within a network to connect services provided by the network to end users. For example, the system can determine a fraction of time an access point is powered up (e.g., using a scale or rating between 0 and 1). Next, the system could also determine how much time the access point can connect to the services of the network, such as connecting to the Internet at the train station of Figure 1. Multiplying the time

powered up and the time the system can connect to system services would produce a quantitative measure of the availability of the network services at the access point or node. Combining quantitative measures of several access points could produce a quantitative measure of the availability of the network services at the hotspot.

A straightforward determination of availability, however, does not completely account for the nuances of reality. For example, the train station of Figure 1 shows an access point near the ticket counter by the main entrance and an access point near a storage closet. In normal operations, the access point near the ticket counter will engage with significantly more wireless devices because many patrons of the train station are likely to pass by it. The access point near the storage closet could enter a sleep or low power mode for much of the day because fewer devices attempt to connect through it. Conventional systems could misinterpret the "low" traffic or "low" power at the storage closet access point as low network availability based on the normal operations and movement patterns of patrons at the train station. Further, conventional systems could also magnify the problem by artificially lowering or skewing an availability rating of the train station hot spot by incorporating the "low" availability rating of the storage closet access point in an evaluation of the train station hotspot as a whole.

Consider another example. In a lighting network of a city, a streetlight could be disconnected for certain periods, perhaps due to periodic maintenance of other utilities sharing the same pole, structure, or other factors. A conventional network administration system could lower the availability rating of the streetlight. However, if the periodic maintenance or other factors occurred during daylight hours, the streetlight was never actually unavailable for providing the network service for which it was intended: light at night. In a city of a just a few lights, manual adjustment or conscious human override of the false-positive decrease in availability is possible.

But, in a metropolitan area with thousands or tens of thousands of streetlights, human interpretation of the system availability data is not feasible.

Here, machine-learning algorithms can overcome a need for a manual override or human interpretation. In the two examples above, the system could include an importance criterion for individual nodes or for collections of nodes. The train station nodes could be analyzed and weighted by assigning an importance to each node. Thus, the node nearest the ticket counter could be weighted heavier than the node nearer the storage closet. Or, the system could account for lower-power sleep or hibernation times of the node nearer the storage closet or the book store, even during the day when the nodes should be active, knowing that such times may coincide with rush hour, where patrons are moving directly to and from the train platform. Additionally, the system can set an importance rating based on the time of day, the day of the week, or account for holidays. A node of the train station performing admirably at lower-traffic times, such as very early morning, but struggling during higher-traffic times, such as rush hour, could be obscured in an overall rating of the train station if not analyzed individually and in light of the conditions at the node. Likewise, daylight hours could be assigned a lower importance level than dusk and night hours when evaluating the availability of a streetlight.

Machine-learning models and algorithms can also learn to identify a disruption in availability at a node based on a deviation from normal operations. For example, a network administrator can identify a particular time when he or she is certain the network services are available at the node, such as by manual tests or inspection of the area of the node in the geographic network. The system may monitor parameters, counters, or other characteristics on the network side and use these characteristics as a proxy for the network services being available to end users. Thus, the system can monitor proxies for the network services at the node and identify times at

which the services change in availability, such as providing an increased or a decreased amount of service. Here, the machine-learning algorithms can identify anomalies in network service availability. For example, a transportation service provider could be alerted to a particular service vehicle departing from normal operational conditions, such as a taxicab unexpectedly providing a diminished amount of service, which could indicate a driver turning off the meter and providing discounted or undocumented services. In some cases, the system is not monitoring whether the node is entirely up or entirely down, but rather calculates a probability that end users have access to the network services.

Not only can a machine-learning system assist in intelligently combining or averaging access points into an overall rating for a hotspot, which may supplement service availability composite metrics constructed by other analytical means, the system can also parse out interactions among the access points themselves and allow the network administrator to better evaluate the condition of the distributed network. For example, consider the train station of Figure 2.

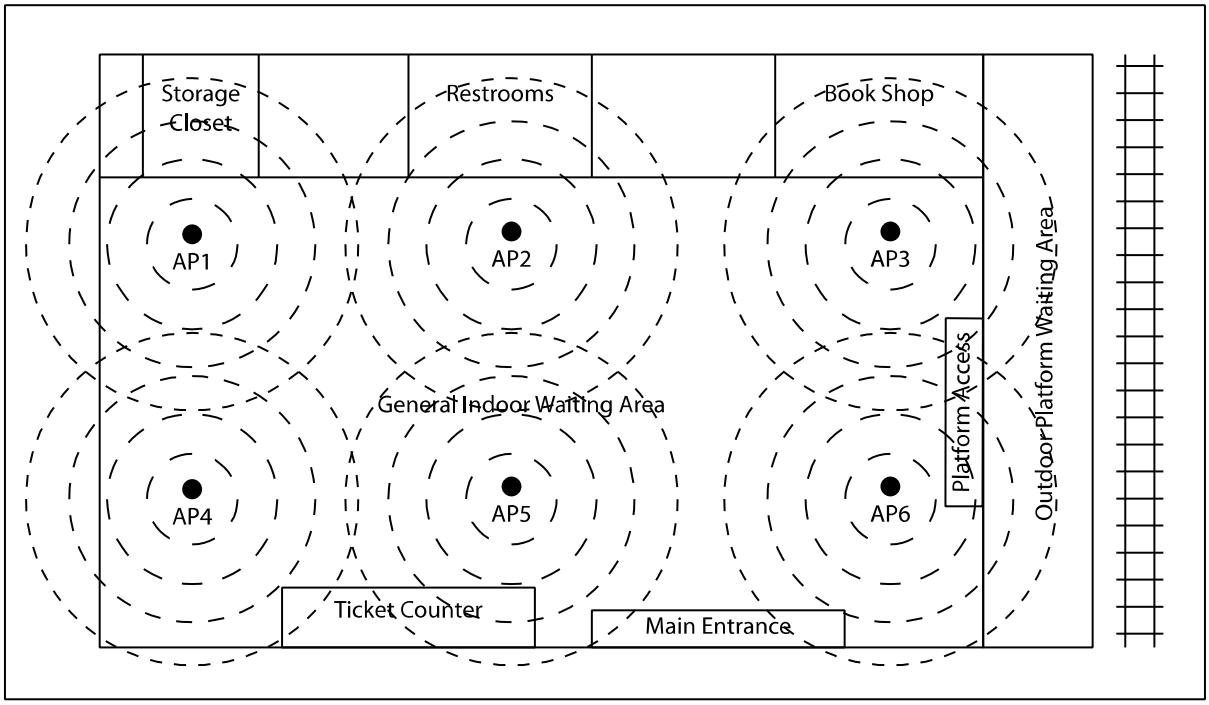

Figure 2

Although similar to Figure 1, Figure 2 includes representations of relative coverage areas of each access point or node (for clarity purposes the coverage areas are represented somewhat smaller than normal or ideal circumstances; as illustrated there would be areas within the train station not covered or poorly covered by any access point, which could be unacceptable in practical circumstances). In any given hotspot or collection of nodes, coverage provided by a single node will often overlap, at least in part, with other adjacent nodes. In some cases, an underperforming node can be masked by its neighbors because end users can still obtain access to the network services by borrowing from an adjacent node. An adjacent, overlapping node could cover a fractional portion of an underperforming node's service area. Although useful for end users, who may not be affected by non-ideal network availability, underperforming nodes can place additional strain on adjacent nodes and on the entire network. When analyzed as a whole, conventional network-side parameters may not reveal if or which nodes are underperforming because overall

aggregate traffic may not have changed enough. Here, the system takes into account the performance of individual nodes in light of information describing the overlap of the nodes in space and time. Thus, having monitored the individual nodes over time, the system can identify parameters outside normal operational conditions, such as parameters indicating overperformance or underperformance by a particular node. In some circumstances, an overperforming node could be used to reveal a malfunctioning or underperforming neighbor node.

Additionally, the system can assign a reliability rating to individual nodes or collections of nodes, hotspots, cities, metropolitan areas, or other networks, networks combinations, or network conglomerates. For example, in the example of the spilled drink near the book store at the train station, a network administrator could receive a notification that the node nearest the book store is suddenly performing far beneath normal standards. In some circumstances, this could trigger additional notifications that result in a manual, physical inspection of the train station, which could be costly in both time, resources, and human capital. However, knowing the propensity for spills or other disruptions near the book store, the system could assign a lower reliability rating at the book store node than at the ticket counter node, which could be assigned a higher reliability rating. The system could rely more on the ticket counter node when aggregating the state of the train station hotspot, which could reduce the number of false positive notifications or alarms.

As networks grow larger and larger, the machine-learning system described here could be used to intelligently monitor the availability of network service to end users when manual or human-conducted monitoring of network availability is less feasible. Machine-learning algorithms may monitor and model the distributed network, which may supplement service availability composite metrics constructed by other analytical means, and allow the network

administrator to better evaluate the condition of the distributed network without the need of additional infrastructure.