NEWS: Towards an Early Warning System for Network Faults

Ankur Gupta and Purnendu Prabhat
Model Institute of Engineering and Technology - Jammu

Efficient network fault detection is a complex process especially when scale, heterogeneity of devices and interconnectivity issues are factored in. Network Management Stations rely on performing polling via ICMP and SNMP for the observed network topology while also correlating asynchronous device-level events/traps to determine the root-cause for network fault. As the size of the network increases, both approaches suffer from delays and inaccuracies. This research paper proposes a theoretical framework for an early warning system for network faults based on analysis of the past behavior of the network and creating spatial and temporal patterns of correlated events. Early warning events aid in quick detection/classification of faults and provide some headroom for the human administrators to take preventive action to reduce impact of impending faults.

Keywords: network management, early warning system, event correlation

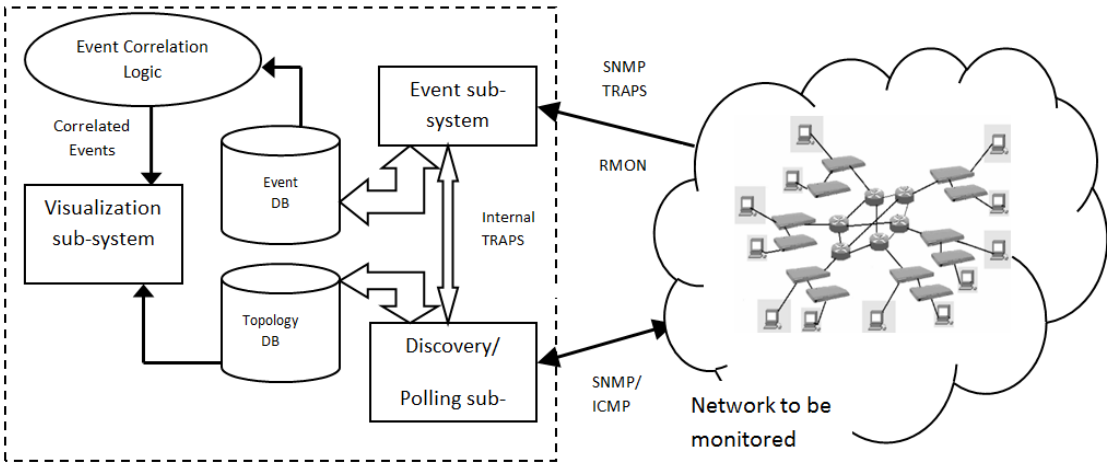
1. INTRODUCTION

Network management solutions focus principally on fault management and operate by reacting to reported network faults. The most common existing approach involves ascertaining a networks topology and then polling all objects or entities in that topology to determine whether those objects are operating normally. The polling is generally performed by means of the Internet Control Message Protocol (ICMP)[1], an extension of the Internet Protocol, and the Simple Network Management Protocol (SNMP)[2], an application layer protocol for facilitating the exchange of management information between networked objects. Existing network management systems can determine network faults once the faulty network entity or entities have been polled and their response, if any, analyzed. Figure 1 depicts the architecture of a typical Network Management Station (NMS) [Stallings 1998] with its important functional modules.

For the networks with larger topologies, however, it can take some time before the management station can complete the polling of all the entities in the network topology and hence, in many cases, until the faulty entity or entities have been polled. This constitutes a scalability problem [Gupta 2006b], fault reporting becomes more difficult or is delayed as network size increases. Network faults are also notoriously difficult to analyze since they manifest in different ways depending upon device interconnectivity and topologies and often cascade. This makes root-cause analysis extremely complex. It is common to have scenarios when the incoming events signifying network faults threaten to exceed cognitive capabilities of human administrators.

One existing Root Cause Analysis (RCA) and event correlation software package is provided by EMC Corp. under the trademark SMARTS [EMC]. This package employs a codebook approach in which a codebook that embodies vendor specific knowledge regarding events and their relationships is created, however, the codebook must be manually created so the correlation and RCA remain fundamentally reactive in nature, and only act after a fault has occurred. IBM Netcool [IBM] also provides proactive fault management through advanced correlation. Data mining techniques that generate knowledge of the past network behavior are used to train machine learning systems to predict alarms have been discussed in [Caravela et al.]. A system for predictive network fault detection is proposed by the authors in [Wang et al. 2010]. The proposed scheme relies on mining network signatures which is a pattern of network faults and their associated symptoms. As real-time events are received, signature matching is employed to predict

[1]https://tools.ietf.org/html/rfc792
[2]https://tools.ietf.org/html/rfc1157



. Figure 1:A typical Network Management Station.

impending faults. One shortcoming of this method, as mentioned by the authors themselves, is that the system is unable to fully exploit the temporal relationships between the nodes. The Active Problem Analyzer [HP] in the HP OpenView Network Node Manager bases its network fault analysis on the spatial relationship between nodes and computes the impact of a fault on related nodes by auto-discovering their relationship and dependencies.

In this paper, we describe an early-warning mechanism for network faults which relies on analyzing past behavior of the network to build spatial and temporal-based patterns of correlated events., It examines both spatial as well as temporal patterns of events based on a final network condition. The past behavior of the network thus forms the basis for future predictions. The steps involved in the process are:

(1) Monitoring events in the network;
(2) Discovering relationships between events;
(3) Responding to an adverse network condition by examining event patterns preceding said adverse network condition;
(4) Correlation of event patterns with adverse network conditions;
(5) Real-time checking for matches or partial matches between stored event patterns and current events
(6) Responding to a match by issuing an early warning indicating the adverse network condition or conditions associated with a matched event pattern.

The events comprise network alarms generated by the Network Management Station (NMS) through polling and also asynchronous traps generated by individual devices to signal abnormal conditions or performance degradation.

Section 2 of the paper discusses the system model for the Network Early Warning System (NEWS) and section 3 provides different use-case scenarios to illustrate the operation of NEWS.

2. SYSTEM MODEL

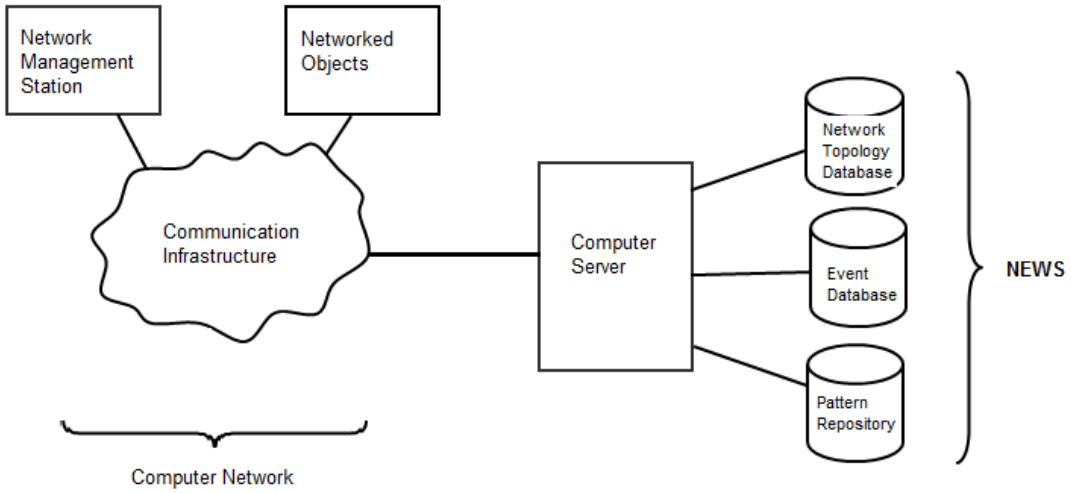
The early-warning mechanism described in this paper relies on mining the event database of an existing NMS looking for patterns that manifest as adverse network conditions or faults. Thus, historical events are analyzed to build associations between various network entities or events; these associations may be based on the object (or entity) that generated those events, any temporal/spatial relationships between those events, and any relationship between the entities

that generated those events. These associations are built as patterns of occurrences, which are constantly evaluated against incoming events. As incoming events start matching stored patterns, early-warning events are issued indicating potential network problems.

The system is envisaged as comprising:

(1) An input for receiving data indicative of network events - the event sub-system in an NMS;
(2) A network event database for storing said data indicative of network events the event database;
(3) A pattern database with identified patterns indicative of potential network faults or adverse network condition;
(4) A pattern analyzer for searching and correlating network events preceding an adverse network condition to identify event patterns, for storing patterns so identified in said pattern database in association with data indicative of the respective adverse network condition, and for real-time matching of said patterns with current network events;

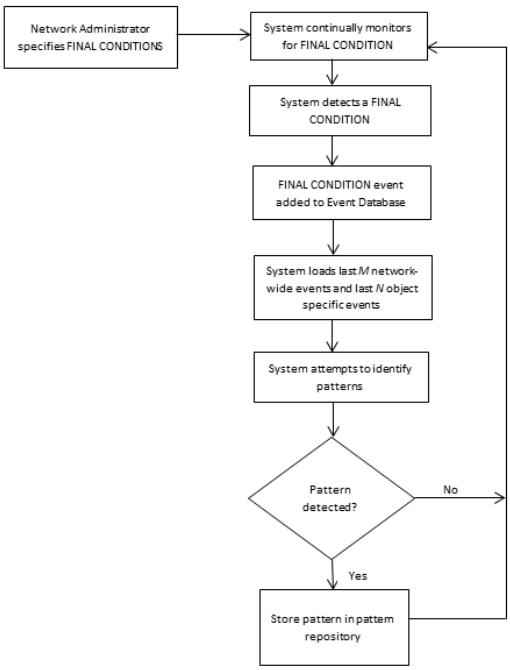
The pattern analyzer is configured to respond to a match (full or partial) by issuing a warning indication the adverse network condition or conditions associated with a matched pattern. Figure 2 illustrates schematically the proposed Network Early Warning System (NEWS).



. Figure 2: Schematic diagram of NEWS.

The network management ecosystem comprises of the computer network composed of various networked objects or nodes (including servers, printers, end computers, routers, switches and the like), a Network Management Station (NMS) and the communication infrastructure. The networked objects and NMS are in electronic communication via the communication infrastructure, which may be in the form of an intranet, the internet or a like telecommunication mechanism. Individual nodes communicate, in some cases, via the communication infrastructure but in other cases directly with each other. It would also be appreciated that in some arrangements, the communication infrastructure will form or at least be regarded as a part of the computer network. This is typically the case when the computer network comprises a local area network. However, when the communication infrastructure comprises the internet, it may not be regarded as a part of the computer network.

Figure 3 shows a flow diagram of the steps performed by the NEWS for preparing to predict network faults. Let this phase be called Preparation Phase.



. Figure 3: Preparation Phase of NEWS.

At first the network administrator specifies a list of network faults which are generally of a critical nature. These fault conditions or performance degradation conditions are termed *final conditions*.

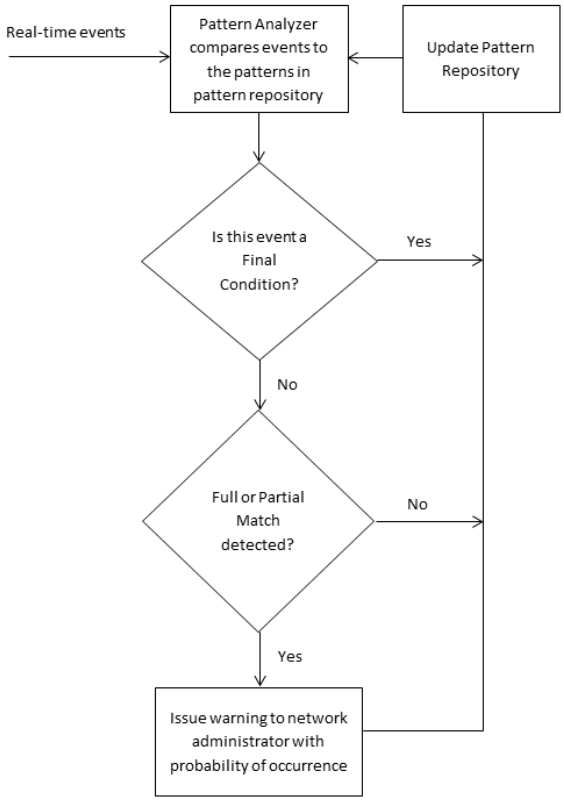
NEWS then continually monitors for *final condition*s and one is detected when such an event is received from one of the networked objects or from the NMS. Whenever a *final condition* is detected, NEWS loads from the event database the last M network-wide events, i.e. events relating to the entire network, and the last N object-specific events preceding the *final condition* event to create a set of related events. NEWS also loads from the event database N object-neighborhood specific events rather than N object-specific events, i.e. N events from the neighborhood of an object, rather than from strictly objects themselves. The values of M and N are derived from heuristics and are configured by the network administrator.

Once the NEWS has built the complete set of related events to mine, it attempts to detect patterns within the set before the *final condition* event was observed. For example, these patterns can comprise repeated sequences of events, events with systematically varying time intervals between them or events with spatial relationships between the entities that generated them (such as that one is connected to other, one is upstream of the other, or both are in a single standby routing protocol group or in the same VLAN). In searching for such patterns, the NEWS draws on the network topology information stored in the network topology database. Thus, the NEWS attempts to evaluate the temporal and spatial relationships between events in the event database and the objects that generate those events to determine if any earlier events had a bearing on the *final condition* event.

When the pattern is discovered, NEWS stores that pattern in the pattern repository which

associates with each pattern of events a *final condition* which the pattern has leads to. The data in this repository, which collectively resembles a grammar with a set of rules, is built over time.

By this sequence of steps, the NEWS populates the pattern repository, for use in the monitoring for future network faults. This monitoring phase is illustrated by means of flow diagram of Figure 4.



. Figure 4: Monitoring Phase of NEWS.

The pattern analyzer within NEWS compares real-time events and with the patterns in the pattern repository. If a match or a partial match is found, NEWS issues an early-warning message to the network administrator, indicating that the *final condition* associated with the matched pattern may soon occur, assigning a probability and expected time of occurrence based on its historical analysis.

The assigned probability indicates the likelihood that the predicted *final condition* will occur. This is determined from the number of current events matched to an already stored pattern. Successive early warning events with increasing probability are therefore issued as more events match a pattern. It is possible that the same current message may lead to the issuance of multiple early warning messages indicating multiple *final condition*s with varying probabilities.

NEWS also monitors whether the *final condition* event actually occurs or not following the early warning events issued. The probabilities are therefore adjusted dynamically. A set of patterns, events and likelihoods that the former will lead to the latter is built in the pattern database. Subsequent warning issued in previous step can therefore include further adjustment to the probabilities assigned to each predicted event on this basis. As a result, the message sent to the network administrator will not necessarily predict with absolute certainty what faults will

occur, but they will provide useful predictions of likely faults that can be provide troubleshooting hints or extra time to initiate corrective interventions.

NEWS thus provides a proactive approach to network fault management rather than, a reactive approach, by analyzing past patterns of events resulting in critical network faults. It can take into account events generated by other network entities in the vicinity of a network entity being analyzed for better impact analysis, automatically determine spatial and temporal relations between events, dynamically update correlation rules for better correlation of events and hence provide early-warning information on the impending network faults.

The patterns identified by NEWS to be associated with a *final condition* event can also be used to provide information about the causes of faults, since the events forming the pattern will in many cases indicate the underlying problem or problems that cause the fault and not merely circumstances coincident with the fault. Analysis of the pattern of events found to coincide with the *final condition* can thereby be used to correct a faults root cause rather than merely anticipate that fault.

As mentioned above, the network topology database is updated as the topology of the network is altered. Consequently, the NEWS will respond to changing network topology and events dynamically, discarding updating or discovering new event patterns accordingly.

3. NEWS SCENARIOS ANALYSIS

3.1 Scenario 1: A Switch goes down.

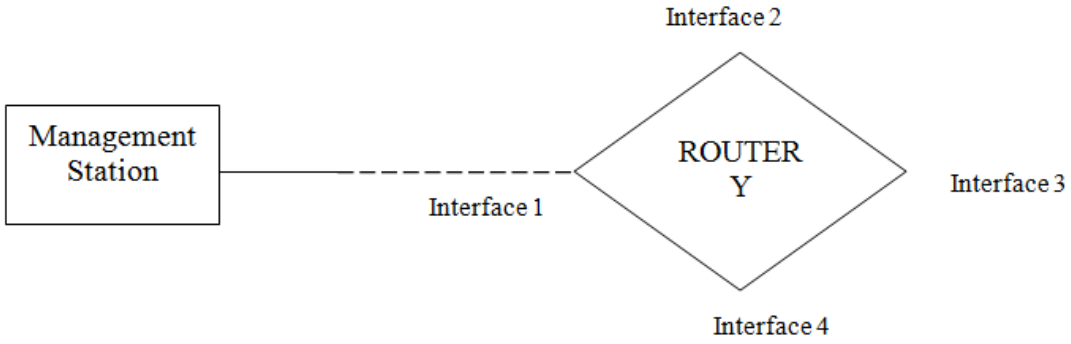
Consider a *final condition* event NODE DOWN configured by the network administrator. The NODE DOWN event is typically generated by a management station whenever an individual node does not respond to SNMP/ICMP. Say, a Cisco switch goes down and the management station has emitted a NODE DOWN event for that switch, say X. NEWS will therefore, search the event database for all events with the event source as switch X. Say, it comes across two occurrences of the Cisco chassisAlarmOn [Cisco] trap one chassisMajorAlarm and one chassisMinorAlarm. If the chassisMajorAlarm has occurred later than the chassisMinorAlarm, there is a high probability that the malfunction condition indicated in the chassisMajorAlarm could have caused the node to fail (it could be due to overheating failure of the cooling fan or the power supply). The chassisMajorAlarm followed by the NODE DOWN is identified as a pattern. As a rule, alarms with the status major are indicative of serious malfunction conditions and the NEWS gives them the required weightage during analysis. On the other hand, if the chassisMinorAlarm has occurred after the chassisMajorAlarm, it indicates a normalization of the operational state of the switch chassis and would be less likely to cause the entire switch to be unresponsive. In this case, the NEWS will attempt to look towards other potential causes of node failure. However, if none are found, it will assign a low probability to the occurrence of a NODE DOWN event after the occurrence of a chassisMinorAlarm.

3.2 Scenario 2: A routers interface is not responding.

Consider a router Y, with multiple interfaces and the network topology indicated in Figure 5. Again the NODE DOWN event is the *final condition* event configured by the network administrator. Consider that interface 1 on the router has the SNMP management address. The other three interfaces (2 through 4) are connected to different networks. For the sake of simplicity let us consider that the management station connectivity to the router is only through interface 1, which means that there exists no other network path between the management station and the router in question.

Suppose that the NODE DOWN event occurs for router Y. NEWS searches the event database for events with the source as router Y. Suppose it finds the following sequence of events (presented in a notional format) in increasing order of time:

—interface 2 DOWN, router Y
—interface 3 DOWN, router Y



. Figure 5: Routers interfaces

—router Y, statusMinor
—interface 1 not responding, router Y
—NODE DOWN, router Y

An interface down event is normally generated when the SNMP request for ifOperStatus MIB [Presuhn 2002] variable returns the status value DOWN, given that the ifAdminStatus MIB variable has the value UP. An interface down event typically signifies that the device is still up, since it is responding to SNMP. However, in this case interface 1 is not responding to SNMP, because when it becomes non-operational, it takes down the SNMP management address with it. Given this network topology, the device will always be marked as DOWN, if it cannot be reached through any other network path. NEWS remembers not only the event, but the particular interface, which when not responding caused the device to be marked DOWN. Thus, it can prevent the wrong conclusion of NODE DOWN when only interface 1 is marked down and interface 2, interface 3 and interface 4 are not marked as down.

Another variation to this scenario is that sometimes a management station, NMS computes the status of the device based on the status of its contained entities. For instance, the NMS could enforce a policy, marking a device as CRITICAL, when 75

—interface 2 DOWN, router Y
—interface 3 DOWN, router Y
—nodeMinor, router Y
—interface 4 DOWN, router Y
—NODE CRITICAL, router Y

In this case, we have three interface DOWN events, indicating that the device is still responding to SNMP. NEWS looks up the interface list for the device in question (it is assumed that the interface list for a particular device is available from the network topology database through a well-defined interface, i.e. topology APIs) and computes the percentage of interface DOWN events to the actual number of interfaces for that device in the topology.

Finally, if the interface 1 is unreachable, NEWS can prevent the incorrect conclusion of it being marked as down leading to the NODE DOWN event. This can be done by examining neighboring topology for router Y and then examining for upstream failures which could cause interface 1 to be unreachable. Thus, the volume of events can also be reduced while improving accuracy by preventing generation of false alarms.

3.3 Scenario 3: Identification of temporal relationships between events.

Consider the occurrence of NODE DOWN (critical event) and NODE UP (normal event) events occurring within a time window of 5 minutes (a typical time window provided as a guideline

by many device vendors to perform event correlation based on temporal relationship, depending on the configured frequency of polling for various network entities). Typically, the network administrator wants to focus on events which represent a malfunction or an error condition in the network. Event patterns like a NODE UP following a NODE DOWN event within a small time window should typically be suppressed as the error condition (NODE DOWN) stands corrected (NODE UP) on its own.

NEWS actively searches the event database to look for event patterns based on temporal relationships. This is done by looking for occurrences of complementary events from the same device or network entity within the configured time window. This time window is configured by the network administrator and a good value should be a little more than the configured frequency for polling of devices. If each router or switch in the network is to be polled at an interval of 5 minutes, then the corresponding NODE UP event can only be generated when the device is next polled, i.e. after 5 minutes. Thus, a time window of, say 6 minutes should be good enough to cover for NMS processing overheads and network latency, if any.

So the NODE DOWN NODE UP event pair would be an identified temporal event pattern and placed in the event pattern repository.

As another example for this scenario, we have events such as INTERFACE DOWN INTERFACE UP event pair. This is especially useful in identifying flapping interfaces, which are a nuisance for network administrators and occur mostly because of dial-up connections being made and brought down repeatedly. NEWS can identify such occurrences and intimate the network administrator via an early-warning alarm, for necessary action (mostly disregarding the event barrage). In these cases, NEWS attaches a 50

NEWS is also perceptive about repeated occurrences of such events, especially the NODE DOWN NODE UP pair as these events could indicate a security risk as the device could be rebooted repeatedly due to a virus or denial of service attack). After X occurrences (configurable by the network administrator) of the event pair the NEWS sends out an early-warning event to the network administrator indicating the possibility of a security risk.

NEWS can thus identify temporal relationships between the specified *final condition* event and any other event which occurs before or after the *final condition* event within the configured time window. Its scope is not limited to the examples discussed above. Repeated occurrences of the same event within a specified time period can be identified and suppressed, if required. For instance, the Cisco router syslog [Cisco 2016b] messages for CPU hogging (SYS-3-CPUHOG) and configuration changes (SYS-5-CONFIG) are two such candidate events which can potentially have repeated occurrences for a router device within a short time period.

3.4 Scenario 4: Whether the device is reset or is unreachable.

Cisco Event Correlation Guidelines and [Cisco 2016a; **?**] provides the following example for a Cisco 5000 Catalyst Switch, to detect whether the device was reset from the console as opposed to it being unreachable: The SYS-5: System Reset syslog message is received when the device is reset. The SNMP-5: Cold Start trap should be received in N minutes (N=switch reboot or reload time +1) after the occurrence of the SYS-5: System Reset syslog event. If not, this signifies a critical switch software error or operation intervention.

NEWS, after analysis of these events can have two possible event patterns in the pattern repository a SYS-5: System Reset followed by a SNMP-5: Cold Start within N minutes or a SYS-5: System Reset followed by a NODE DOWN event.

3.5 Scenario 5: Spatial Analysis

3.5.1 *Upstream device DOWN.* One of the challenges before network management solution is to determine the root cause of a particular network fault. If a particular device is unreachable, is it because of an upstream device (from the perspective of the location of the NMS) being down or is it because that device itself is down? If a router goes down, the devices which are downstream from that router would not be reachable, assuming that there was no other network path to those

devices.

Let us consider an important server; say X, in a network and the network administrator has configured the NODE UNREACHABLE event for that server X as the *final condition* event for NEWS. NEWS would use the topology API to compute the set of devices which are in the neighborhood of server X based on the configured number of hops from the specified node. For instance, a hop count of 1 would result in the computation of the set of network entities which are directly connected to the server X (say a switch) and a hop count of 2 would result in the computation of the set of devices connected to the devices which are directly connected to server X.

When NEWS begins analysis of the event database and encounters the NODE UNREACHABLE event for server X, it searches for all events pertaining to devices from the computed neighborhood of the server X. Depending on the order in which devices are polled, the events from the neighborhood of the server X could occur before the NODE UNREACHABLE for server X or after its occurrence. NEWS therefore scans for related events before and after the occurrence of NODE UNREACHABLE event for server X.

Consider that the server X is directly connected to switch Y and NEWS comes across the NODE DOWN event for switch Y while analyzing the *final condition* event for server X. Since switch Y is in the immediate neighborhood of server X, the switchs failure could be related to the unreachability of server X. This is identified as a pattern by the NEWS. Next time, when the NODE DOWN event for switch Y is received, the NEWS lets out an early-warning alarm to indicate that the server X would also be unreachable as a result.

A traditional NMS would not be able to figure these scenarios out till all the devices in the neighborhood are polled, which could potentially take a longer time depending on the polling frequency and how the internal polled object lists are maintained by the NMS. Also neighborhood analysis at run-time is an overhead and would result in delayed reporting of root-cause failures, much after the actual failure occurred.

3.5.2 *Impact analysis of related objects.* Consider a switched network, with various VLANs and an active Spanning Tree Protocol (STP) [Cisco 2016d] for ensuring a loop-free switched topology. Let the *final condition* event be a STP reconfiguration event indicated by the SPANTREE-6 series of syslog messages. The STP reconfiguration could be because a device in the spanning tree failed, was removed from service, was added to the network or a link between two switches participating in the spanning tree was added or removed.

NEWS computes the set of all devices participating in the VLAN and the spanning tree, by using the interface to the topology database and then searches for any prior events from those devices. For instance, if two switches are connected to each other, an INTERFACE DOWN event on switch 1 will take the corresponding connecting interface on switch 2 down with it (the connecting link will go down). If both these switches were participating in the spanning tree, it could lead to the spanning tree reconfiguration. In this case, the following event pattern is identified by the NEWS:

—INTERFACE DOWN, switch 1

—LINK DOWN, switch 1 and switch 2

—STP RECONFIGURATION event

Another possible scenario for a switch X participating in VLAN Y and the corresponding spanning tree could be:

—INTERFACE DOWN, switch X

—NODE DOWN, switch X

—VLAN TOPOLOGY CHANGE event, VLAN Y

—STP RECONFIGURATION event, VLAN Y

Thus, NEWS takes into account the participative relationships within a network, enabling it to perform an effective impact analysis. A switch participates in a VLAN and a spanning tree. Similarly, a router could participate in a HSRP [Cisco 2016c] or multicast group. NEWS is able to process these relationships which is an improvement over existing predictive frameworks.

3.6 Scenario 6: Generic Analysis

For all *final condition* events, NEWS attempts to answer the following questions:

—How does it impact the network in general?

—Does it cause congestion?

—Does it cause performance degradation?

—How does it impact the higher order services, built on top of various network elements?

Because NEWS does not work on hard-coded correlation rules, it is flexible enough in recognizing events and figuring out conditions in the network which occurred or existed prior to certain events. For instance, a service impact event for the Microsoft Exchange Server [Microsoft 2016] could be generated by any service management solution. Given this NEWS would look up all occurrences of this event in the event database and for each occurrence, attempt to figure out if there existed a network event which could be correlated to the service impact event. This could be due to an interface on the server running the Microsoft Exchange Service being down or the server itself being down.

Each pattern stored in the pattern repository represents a likely sequence of events, which could occur before the occurrence of the *final condition* event. One of the biggest advantages here is that the event correlation rules need not be specified. Each network device vendor provides proprietary events and event correlation scenarios. So, a comprehensive event correlation solution which is vendor agnostic is not a possibility as of now as these correlation rules need to be built into the NMS for specific correlation scenarios. NEWS thus alleviates this problem.

4. CONCLUSIONS AND FUTURE WORK

We have presented a novel strategy for dynamically building patterns of events preceding observed network faults, which helps in generating early-warning events indicative of impending faults. Such events can greatly help the network administrators in quick classification and detection of network faults and possibly create some lead time to initiate preventive or corrective action to reduce the impact of the network fault. Suggestions of corrective actions can be generated for the reference of the network administrator and subsequently, the actions initiated by the human administrator can be codified in an expert system leading to completely autonomous mechanism to deal effectively with impending network faults. The inputs from early-warning events can also be used to initiate smart network management through dynamic optimization of polling strategies, allowing faster mean-time-to-detect and faster root cause analysis of network faults. We intend to validate the effectiveness of NEWS on real data sets in the future.

Note: The framework described in this research paper was first disclosed in US patent application US 20070174449 A1 [Gupta 2006a].

REFERENCES

Caravela, I., Arsenio, A., and Borges, N. A closed-loop automatic data-mining approach for preventive network monitoring. *Journal of Network and Systems Management*, 1–30.

Cisco. Support information for cisco traps. https://goo.gl/O25EWG.

Cisco. 2016a. Best practices for catalyst 4500/4000, 5500/5000, and 6500/6000 series switches running catos configuration and management. https://goo.gl/NbAwpD.

Cisco. 2016b. Cisco syslog. http://www.cisco.com/c/en/us/tech/ip/syslog/index.html.

Cisco. 2016c. Hot standby router protocol (hsrp): Frequently asked questions. https://goo.gl/qNc1tD.

Cisco. 2016d. Spanning tree protocol (stp) / 802.1d. https://goo.gl/h7vawY.

EMC. Smarts software-data center management-emc. http://www.emc.com/it-management/smarts/index.htm.

Gupta, A. 2006a. Method and system for identifying potential adverse network conditions. US Patent App. 11/487,248.

Gupta, A. 2006b. Network management: Current trends and future perspectives. *Journal of Network and Systems Management 14,* 4, 483–491.

HP. Hp openview network node manager, active problem analyzer. http://h41111.www4.hp.com/nsm/uk/en/whitepapers/NSM WP Active Problem Analyzer.pdf.

IBM. Netcool network management. http://www.emc.com/it-management/smarts/index.htm.

Microsoft. 2016. Exchange server for business. https://products.office.com/en/exchange/microsoft-exchange-server-2016.

Presuhn, R. 2002. Management information base (mib) for the simple network management protocol (snmp). *Management*.

Stallings, W. 1998. *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.* Addison-Wesley Longman Publishing Co., Inc.

Wang, T., Srivatsa, M., Agrawal, D., and Liu, L. 2010. Spatio-temporal patterns in network events. In *Proceedings of the 6th International COnference*. ACM, 3.

Prof. Ankur Gupta is the Director at the Model Institute of Engineering and Tech- nology, Jammu, India, besides being a Professor in the Department of Computer Science and Engineering. Prior to joining academia, he worked as a Technical Team Lead at Hewlett Packard, developing software in the network management and e-Commerce do- mains. He obtained B.E (Hons) Computer Science and MS Software Systems degrees from BITS, Pilani and his PhD from the National Institute of Technology in India. His main ar- eas of interest include peer-to-peer networks, network management, software engineering and cloud computing. He has published over 40 peer-reviewed papers in reputed interna- tional journals and conferences and is a recipient of the AICTE's (All India Council for Technical Education) Career Award. He has filed 10 patents in diverse technical domains and is the founding managing editor of the International Journal of Next-Generation Computing (IJNGC). He is a senior member of both the IEEE and ACM and a life member of the Computer Society of India. Email-ID: ankurgupta@mietjammu.in.

Purnendu Prabhat is an Assistant Professor at Model Institute of Engineering and Technology, Jammu in the Department of Computer Science & Engineering. He received his Bachelors degree in Computer Science & Engineering from Kalasalingam University, Tamil Nadu in 2012 and Masters degree in Computer Science from Central University of South Bihar in 2014. His research interests include Network Management and Software Defined Networking. Besides research he enjoys programming and teaching. Email-ID: purnendu.cse@mietjammu.in.