International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Functional Requirements of Network Management System based on Simple Network Management Protocol

Sangeet Bhosure[1], Dr. Rishi Asthana[2]

[1]Ph. D. Scholar, Department of ECE, Shri Venkateshwara University, Gajraula, U. P., India

[2]Research Guide, Shri Venkateshwara University, Gajrulla, U.P., India

Abstract: ***A Network Management System (NMS) is a critical component in modern information technology infrastructures, enabling efficient monitoring, control, and maintenance of network resources and services. As organizations increasingly rely on interconnected systems to deliver services, the importance of a robust NMS becomes paramount. This abstract outline the fundamental requirements of an effective Network Management System, emphasizing its role in ensuring network availability, performance optimization, security enforcement, and scalability.***

Keywords: Network, Monitoring, Servers, Communities, SNMP, MIB, OID, NMS

1. Introduction

Network management is the intricate orchestration of ensuring that networks and systems consistently deliver their intended services at the prescribed quality of service standards to both users and interconnected systems. In most enterprise management frameworks, the agent-manager relationship plays a pivotal role. Agents, stationed within managed network/system elements, serve as the conduits for network/system management data, encompassing alerts and performance metrics, channeling them to the manager. In response, the manager takes a multifaceted approach, responding to these messages by executing actions that may include operator notification, event logging, system shutdown, or even automated attempts at system restoration. Additionally, management entities periodically poll end stations, either autonomously or upon user request, to scrutinize the values of specific variables. Agents possess detailed knowledge about the devices they oversee and proactively or reactively relay this information to management entities within one or more enterprise management systems, facilitated by a network management protocol. The term 'enterprise management' encompasses the holistic management of both networks and systems.

This paper [1] investigates the challenge of SYN flood attacks within the context of SDN (Software-Defined Networking) environments and leverages the programmability features of Open vSwitch (OVS) to combat flooding. It further introduces a novel approach to expose and mitigate attacks in SDN by employing SDN applications and Simple Network Management Protocol (SNMP) monitoring sensors, such as Paessler Router Traffic Grapher (PRTG) Enterprise Monitor. These sensors identify and respond to anomalous patterns in malicious traffic. The proposed application demonstrates its efficacy against SYN flooding attacks through a systematic process, from detection to alarm activation to application execution, ultimately restoring traffic to its normal state.

In another vein, paper [2] presents meticulously designed system architecture for Internet of Things (IoT) applications, focusing on temperature and relative humidity measurements using the DHT11 temperature and humidity sensor. This system effectively utilizes Simple Network Management Protocol (SNMP) to manage diverse network devices and facilitate data transfer. The ESP32 Wi-Fi microcontroller, connected to the sensor, communicates seamlessly with the Open Platform Communication (OPC) server. Network variables are meticulously identified using Object Identifiers (OIDs) and then aggregated into the Management Information Base (MIB). These two crucial components empower the SNMP monitoring tool, enabling users to monitor network infrastructure and perform troubleshooting tasks with ease.

Furthermore, paper [3], titled "Network Management and Monitoring System using SNMP Protocol, " delves into the pivotal role of Simple Network Management Protocol (SNMP) in the realm of network management. The authors [4] elucidate the multifaceted functionalities of SNMP and delve into various aspects of its operation. They explore the challenges and opportunities associated with SNMP-based management systems, underscoring the imperative need for scalability, security, and performance optimization. Additionally, the paper [6] thoroughly dissects the challenges associated with network discovery, topology mapping, fault detection, and configuration management. The work underscores the paramount importance of meeting these requirements to ensure the seamless execution of SNMP-based network management, aligning closely with the central theme of functional requirements.

Lastly, paper [11] introduces an analytical perspective on system requirements and proposes a data collection strategy based on data types to enhance collection efficiency. The paper provides insight into the system's architecture and its implementation. Furthermore, RFC [10] delineates standards track protocol for the Internet community under the purview of the IAB, soliciting discussion and suggestions for improvements.

Functions of Network Management System:

The Network Management System fulfils a spectrum of functions, including:

Performance Management: This encompasses the measurement of diverse metrics related to network/system performance. These metrics undergo meticulous analysis to establish baseline norms, and appropriate threshold values are determined to ensure the requisite level of performance for each service. Notable performance metrics include network/system throughput, user response times, and line utilization. Management entities continuously monitor these performance metrics, promptly generating alerts and transmitting them to the management system when thresholds are exceeded.

When designing a Network Management System using SNMP, it's important to consider factors such as scalability, performance, security, and compatibility with different SNMP versions and devices. Properly configuring SNMP settings, securing communication, and defining efficient polling intervals are essential for a reliable and effective NMS.

SNMP SNMP Agent: Software running on managed devices that responds to SNMP requests from the NMS.

SNMP Manager: Software on the NMS responsible for sending SNMP requests and processing responses.

SNMP Libraries: Programming interfaces and libraries that allow developers to implement SNMP functionality in custom applications.

A Network Management System (NMS) is a crucial tool for monitoring and managing network devices, resources, and performance. The Simple Network Management Protocol (SNMP) is a widely used protocol for managing and monitoring network devices. Here are the specifications and key components of a Network Management System using SNMP:

1) Architecture:

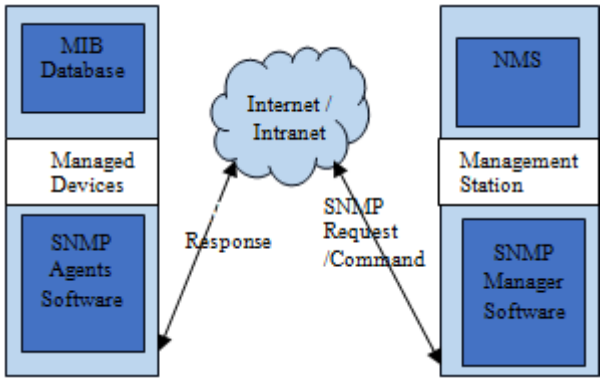


Figure 1: Architecture of NMS system

- The NMS typically consists of two main components: the Management Station and the Managed Devices.
- Management Station: This is the central control point where network administrators monitor and manage network devices. It includes software applications for data collection, analysis, and reporting.
- Managed Devices: These are the network elements being monitored and managed, such as routers, switches, servers, printers, and more.

2) SNMP Protocol Versions:

Within the realm of Simple Network Management Protocol (SNMP), three prominent versions exist, each catering to distinct requirements:

SNMPv1: SNMPv1 stands as the pioneering iteration of SNMP. While it successfully achieved the status of an open and standardized protocol, it became apparent that certain crucial aspects were lacking for specific applications. Subsequent iterations sought to rectify these deficiencies. SNMPv1 is often the choice for smaller Remote Telemetry Units (RTUs) due to its simplicity and compatibility.

SNMPv2c: SNMPv2c, a derivative of SNMPv2, introduces a noteworthy enhancement in the form of the "Inform" command. Distinguishing itself from earlier versions, SNMPv2c replaces the one-way "Trap" communication with "Informs" that solicit a response from the manager. Should a manager fail to acknowledge an Inform, the SNMP agent exhibits persistence by resending the message until confirmation is received.

SNMPv3: The latest evolution of SNMP, SNMPv3, introduces several advancements in security and authentication. A critical element within SNMPv3 is the "EngineID" identifier, which assigns a unique identity to each SNMP entity. Conflicts arise if two SNMP entities inadvertently share identical EngineIDs. This identifier plays a pivotal role in generating keys for authenticating SNMP messages, reinforcing security in the SNMP ecosystem.

SNMP Components:

SNMP's functionality revolves around a few key components:

Management Information Base (MIB): MIB serves as a structured repository, organizing definitions for managed objects hierarchically. Within its framework, MIB delineates the data structure accessible and modifiable through SNMP. Essentially, it outlines what information can be retrieved or controlled via SNMP.

Managed Objects: These represent the discrete attributes of network devices that SNMP can oversee. Each object carries a distinct identity assigned through an Object Identifier (OID). These OIDs are the linchpins that enable SNMP to navigate and interact with individual elements in the network, providing a means to monitor and manage the diverse facets of networked systems.

The Simple Network Management Protocol (SNMP) is composed of several key components that work together to facilitate the management and monitoring of network devices. These components play specific roles in SNMP operations and communication between a Network Management System (NMS) and managed devices. Here are the main SNMP components:

a) Managed Devices:
- Managed devices are the network elements being monitored and managed using SNMP.
- These devices can include UPS, routers, switches, servers, printers, access points, and more.
- Managed devices host an SNMP agent responsible for handling SNMP operations and maintaining the Management Information Base (MIB).

b) SNMP Agent:
- The SNMP agent is a software module residing on managed devices.
- It communicates with the NMS by processing SNMP requests and generating responses.
- The agent provides access to managed objects (variables) in the device's MIB.
- It can also send unsolicited notifications (traps or informs) to the NMS to report specific events.

c) Management Information Base (MIB):
- The MIB is a hierarchical database that organizes and defines the structure of managed objects in a device.
- Each managed object is identified by a unique Object Identifier (OID).
- The MIB contains information about device characteristics, performance metrics, configuration settings, and more.
- MIBs are defined using a structured language like SNMP's Structure of Management Information (SMI).

d) Network Management System (NMS):
- The NMS is a centralized software application used to manage and monitor network devices.
- It sends SNMP requests to managed devices' SNMP agents to retrieve information or perform actions.
- The NMS processes SNMP responses, displays data to administrators, and initiates management tasks.
- It can also receive SNMP traps or informs from managed devices to be alerted about events.

e) SNMP Manager:
- The SNMP manager is the component within the NMS responsible for generating SNMP requests and processing responses.
- It formulates and sends GET, GETNEXT, GETBULK, SET, and other SNMP operation requests to SNMP agents.
- The SNMP manager interprets the information received from SNMP agents and presents it to administrators in a meaningful way.

f) SNMP Protocol Operations:
- SNMP defines a set of operations that the NMS uses to communicate with SNMP agents. These operations include GET, GETNEXT, GETBULK, SET, and others.
- Each operation has a specific purpose, such as retrieving data (GET), modifying values (SET), or discovering the next object in the MIB (GETNEXT).

g) SNMP Trap and Inform Receiver:
- This component in the NMS listens for and processes SNMP traps and informs sent by SNMP agents.
- Traps and informs are used to notify the NMS about specific events, such as device reboots, link failures, or critical conditions.

3) SNMP Libraries and APIs:
- SNMP libraries and Application Programming Interfaces (APIs) provide programming interfaces for developers to implement SNMP functionality in custom applications.
- These libraries handle the low-level SNMP protocol details, making it easier to create SNMP-enabled applications.
- These components work together to enable network administrators to monitor network health, retrieve information, modify settings, and respond to events across a variety of managed devices.

4) Functional Requirements: SNMP Operations:

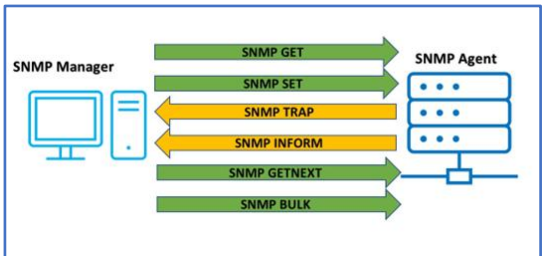


Figure 2: SNMP Basic Operation

The Application software shall support all basic operations of SNMP protocol. Simple Network Management Protocol (SNMP) defines a set of operations that allow a Network Management System (NMS) to communicate with and manage network devices. SNMP operations are used to retrieve information from managed devices, modify settings, and monitor network performance. Here are the main SNMP operations and their details:

a) GET (GetRequest):
Purpose: Retrieves the value of one or more managed objects (variables) from a target device.
Process:
- NMS sends a GET request to the SNMP agent on the managed device.
- SNMP agent retrieves the requested values from its Management Information Base (MIB) and sends the response back to the NMS.

b) GETNEXT (GetNextRequest):
- Purpose: Retrieves the value of the next managed object in the MIB hierarchy.
- Process:
- NMS sends a GETNEXT request to the SNMP agent with the OID of the desired object.
- SNMP agent finds the next object in the MIB and returns its value along with its OID.

c) GETBULK (GetBulkRequest):
- Purpose: Retrieves multiple sets of related objects in a single request to reduce network traffic and improve efficiency.
- Process:

- NMS sends a GETBULK request to the SNMP agent with parameters like starting OID and the number of variables to retrieve.
- SNMP agent returns a bulk response containing the requested variables.

d) SET (SetRequest):
- Purpose: Modifies the value of a managed object in a target device's MIB.
- Process:
- NMS sends a SET request to the SNMP agent with the OID of the object and the new value.
- SNMP agent validates the request, makes the change, and sends a response indicating success or failure.

e) TRAP and INFORM:
- Purpose: Send unsolicited notifications from managed devices to the NMS to inform about specific events or conditions.
- Process:
- SNMP agent on the managed device sends a TRAP (SNMPv1) or INFORM (SNMPv2c and SNMPv3) message to the NMS.
- The NMS processes the notification and can take appropriate actions based on the event reported.

f) Response Codes:
- SNMP operations return response codes to indicate the outcome of the operation:
- NoError: The operation completed successfully.
- NoSuchName: The specified OID does not exist in the MIB.
- BadValue: The value provided in a SET request is not valid.
- ReadOnly: The requested variable cannot be modified (applicable to SET operations).
- GenError: A general error occurred.

SNMP operations are based on the client-server model, where the NMS acts as the client and the managed device's SNMP agent acts as the server. The SNMP agent maintains the MIB, which is a hierarchical database of managed objects with unique OIDs. The NMS uses SNMP operations to query or modify these objects for monitoring and management purposes.
It's important to note that SNMPv3 introduced enhanced security features, including authentication and encryption, to protect the confidentiality and integrity of SNMP communication. This is particularly important when performing SET operations or retrieving sensitive information from network devices.

5) Security Features (SNMPv3):
- Authentication: Ensures that the message is from a valid source.
- Encryption: Protects the confidentiality of data exchanged between the NMS and managed devices.
- Authorization: Specifies what actions an authenticated user is allowed to perform.
- Access Control: Restricts access to certain managed objects based on user roles.

6) NMS Functionalities:

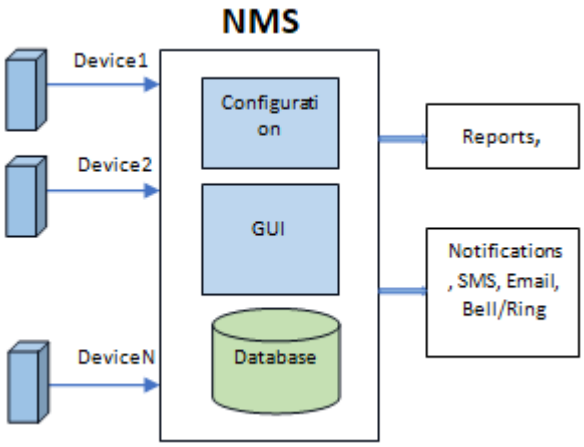


Figure 3: NMS Functionality Block Diagram:

The Application software shall include the following functionalities:

a) User Access Control and Authentication:
- Manages user accounts, roles, and permissions for NMS access.
- Controls user actions based on assigned privileges.
- Enhances security by preventing unauthorized access to critical network resources.

b) Device Add/Discovery and Inventory Management:
- Automatically discovers device/system or user access to add the new device
- by IP address and maintains an inventory
- Collects information such as device type, MAC address, firmware version, and hardware details.
- Enables accurate tracking of network assets and their configurations.

c) Performance Monitoring and Metrics Collection:
- Monitors alarms and parameters of devices/systems, interfaces, and services. Facility to add and edit parameter from the user MIB file.
- Collects metrics like CPU utilization, memory usage, interface traffic, latency, packet loss, and response times.
- Provides real-time and historical data to assess network health and identify performance trends.
- It shall have provision to select the parameters from the MIB for the monitoring purposes and interval setting to refresh the data (e. g. minimum 1sec). The selected parameters shall monitor with the given time interval and also logged it.

d) Fault Detection and Management:
- Detects and alerts administrators about UPS faults, network faults, errors, and anomalies.
- Generates notifications, alarms, and event logs for quick issue identification and resolution.
- Facilitates root cause analysis and reduces mean time to repair (MTTR).

e) Configuration Management:
- Centralizes and manages device configurations to ensure consistency and compliance.

- Allows administrators to deploy, modify, and update device settings across the network.
- Tracks configuration changes and maintains version control for auditing and rollbacks.

f) Security Management:
- Monitors network security by analysing logs and detecting unauthorized access attempts, breaches, and security policy violations.
- Enforces access controls, user authentication, and encryption to protect sensitive data and ensure compliance.
- Assists in implementing security patches and updates.

g) Network Topology Mapping and Visualization:
- Creates visual representations of network topology, including devices, links, and relationships.
- Aids in understanding network architecture, identifying potential bottlenecks, and planning expansions.
- Supports efficient troubleshooting by providing a clear view of network structure.

h) Bandwidth and Traffic Analysis:
- Monitors and analyzes network traffic patterns, usage, and congestion points.
- Identifies bandwidth-intensive applications, protocols, and users.
- Helps optimize bandwidth allocation and ensures smooth network operation.

i) Event Logging and Reporting:
- Records and stores events, alarms, and parameters for historical reference and compliance.
- Generates detailed reports and dashboards for alarms logs, parameters logs, network performance, availability, and utilization.
- Generates reports of selected parameters of a device and selected time zone.
- Facility to export generated reports in CSV or PDF format.

j) Policy Enforcement and Compliance Management:
- Enforces network policies, quality of service (QoS) settings, and regulatory requirements.
- Monitors adherence to security policies, ensuring data integrity and confidentiality.
- Conducts compliance audits and generates reports for regulatory purposes.

k) Proactive Maintenance and Predictive Analytics:
- Uses historical data and predictive analytics to identify potential network issues before they impact operations.
- Enables proactive maintenance, upgrades, and resource optimization.
- Minimizes downtime and improves network reliability.

l) Vendor-Agnostic Support and Interoperability:
- Supports a wide range of network devices/systems and equipment from various vendors, support different MIBs, facilities to add user MIBs.
- Utilizes standardized protocols (e. g., SNMP, ICMP, SSH) for seamless communication and management.
- Ensures compatibility and ease of integration in heterogeneous network environments.

These functionalities collectively empower network administrators to effectively manage and optimize network performance, troubleshoot issues, enforce security measures, and plan for future expansions or improvements. A well-implemented NMS contributes to enhanced network efficiency, reduced operational costs, and improved user experiences.

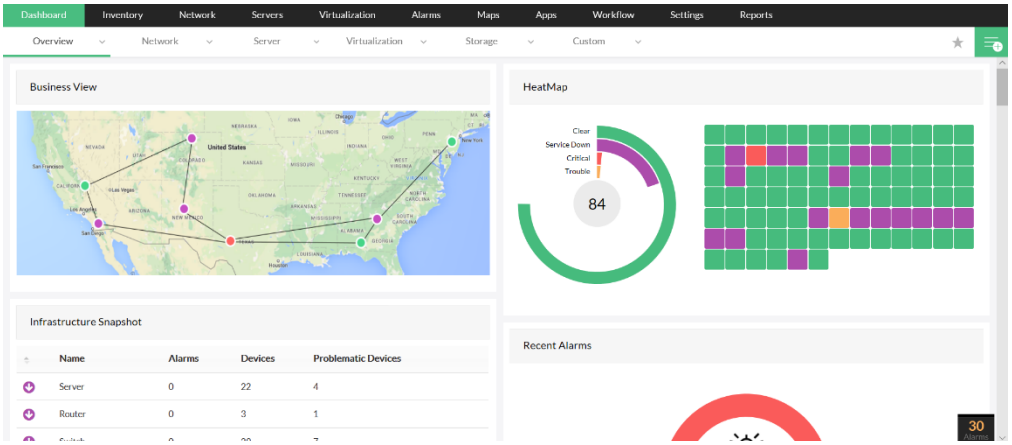
7) Graphical Capabilities:

Designing a Network Management System (NMS) with graphical capabilities using Simple Network Management Protocol (SNMP) involves creating a user-friendly interface that allows administrators to visualize and interact with network data. Here are some graphical requirements to consider when developing an SNMP-based NMS.

- Graphical User Interface (GUI):
- Topology Mapping and Visualization:
- Graphing and Charting:
- Event Logging and Notifications:
- Configuration Management:
- Security Visualization:
- Performance Heatmaps:
- Customization and Personalization:
- Responsive Design:
- Data Filtering and Drill-Down:
- Contextual Menus and Tooltips:
- User Authentication and Access Control:

When designing the graphical requirements for an SNMP-based NMS, it's essential to prioritize usability, performance visualization, and effective communication of network status and events to network administrators and operators.

NMS Tool Example: ManageEngine OpManager is a comprehensive network monitoring tool that supports multi-vendor devices, offers performance monitoring, fault management, and network mapping.



2. Conclusion

This study has explored the critical functional requirements of a Network Management System (NMS) that relies on the Simple Network Management Protocol (SNMP). Through a comprehensive analysis of SNMP-based NMS functionality, we have identified several key considerations that are vital for effective network monitoring and management.

Firstly, we highlighted the importance of robust device discovery mechanisms, which enable NMS to automatically detect and add network devices. This ensures an up-to-date inventory of network assets, facilitating efficient resource management.

Secondly, we emphasized the significance of SNMP data collection and monitoring capabilities. SNMP provides valuable insights into device performance, network traffic, and device health. An effective NMS must be capable of collecting, processing, and presenting this data in a user-friendly manner.

Thirdly, we discussed the necessity of alarm and event handling functionalities. SNMP-based NMS should be able to generate alerts and notifications for network anomalies, enabling administrators to take timely corrective actions.

Additionally, security emerged as a paramount concern. SNMP-based NMS must implement robust authentication and encryption mechanisms to protect sensitive network data and configurations.

The functional requirements of an SNMP-based Network Management System are multifaceted, encompassing device discovery, data collection, alarm handling, scalability, and security. Meeting these requirements is crucial for maintaining the integrity, performance, and security of modern networks. As technology continues to advance, NMS solutions must evolve to address new challenges and opportunities in network management.

References

[1] Ammar Dawod; Huda S. Abdulkarem, (2022). Software-defined Network with SNMP Monitoring Sensor Against SYN Flooding. IEEE 3rd International Informatics and Software Engineering Conference (IISEC)

[2] Nurvita Aji; Nazuwatussya'diyah; Endra Joelianto. (2021). IoT-Based Temperature and Relative Humidity Monitoring System Using Simple Network Management Protocol. International Conference on Instrumentation, Control, and Automation (ICA) , IEEE.

[3] Sadasivam, S., & Othman, M. (2017). Network management and monitoring system using SNMP protocol. Journal of Computer Science, 13 (12), 625-632.

[4] Molka, D., &Puliafito, A. (2019). A survey on SNMP network management. IEEE Transactions on Network and Service Management, 16 (1), 220-235.

[5] Xu, Y., & Muppala, J. K. (2017). Software-Defined Networking-Based Network Management: A Survey. IEEE Communications Surveys & Tutorials, 19 (1), 472-493.

[6] Hegde, R., & Niranjan, S. (2017). SNMP based network management. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp.926-929). IEEE.

[7] Subekti, R., Arif, A., & Prayudi, Y. (2017). Development of network monitoring system using SNMP protocol. In 2017 International Seminar on Application for Technology of Information and Communication (ISemantic) (pp.85-90). IEEE. Mauro, D., & Schmidt, K. (2013). Essential SNMP (2nd ed.). O'Reilly Media.

[8] Wijekoon, A., & Karunaratne, N. D. (2015). SNMP-Based Network Monitoring System for Small and Medium Enterprises. In 2015 Moratuwa Engineering Research Conference (MERCon) (pp.82-87). IEEE.

[9] Neto, A. C., Rothenberg, C. E., & Salvador, M. R. (2014). Fast and efficient SNMP polling using OpenFlow. In Proceedings of the 2014 ACM conference on SIGCOMM (pp.21-32)

[10] McCloghrie, K., & Rose, M. (1991). Management information base for network management of TCP/IP-based Internets. RFC 1213.

[11] Zhen-qi Wang; Yue Wang (2009) Research and Design of Network Servers Monitoring System Based on SNMP, First International Workshop on Education Technology and Computer Science, IEEE.

[12] Zeng Xiyang; Cheng Chuanqing. (2009). TT-ERCR: A Flexible SNMP Management Method. 2009

International Symposium on Intelligent Ubiquitous Computing and Education, IEEE.
[13] P. Collela, "5G and IoT: Ushering in a new era", 2017, [online] Available: https: //www.ericsson. com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/5g-and-iot-ushering-in-a-new-era.
[14] W. T. Hartman, A. Hansen, E. Vasquez, S. El-Tawab and K. Altaii, "Energy monitoring and control using Internet of Things (IoT) system", 2018 Syst. Inf. Eng. Des. Symp. SIEDS 2018, pp.13-18, 2018.
[15] Taryudi, D. B. Adriano and W. A. Ciptoning Budi, "Iot-based Integrated Home Security and Monitoring System", *J. Phys. Conf. Ser*, vol.1140, no.1, 2018.
[16] H. Hui-Ping, X. Shi-De and M. Xiang-Yin, "Applying SNMP technology to manage the sensors in internet of things", *Open Cybern. Syst. J*, vol.9, pp.1019-1024, 2015.
[17] K. Grover and V. Naik, "Monitoring of Android devices using SNMP", 2016 8th Int. Conf. Commun. Syst. Networks COMSNETS 2016, pp.3-4, 2016.