iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XI **Month of publication:** November 2022

DOI: https://doi.org/10.22214/ijraset.2022.47293

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

Analysis of SNMP Based Protocols in IoT and Real-World Scenarios

Gautam R[1], Suyog P[2], G S Nagaraja[3]
[1, 2, 3]*Department of Computer Science and Engineering, RV College of Engineering*

Abstract: ***In the scenario of large organizations device management and maintenance plays an important role in proper functioning of network connected devices. SNMP (Simple NetworkManagement Protocol) is an internet Protocol running in the application layer of the OSI modelthat governs the functioning of the network devices such as routers, switches and access points. The implementation of SNMP is done mainly using UDP (User Datagram Protocol) which is best effort protocol leaving the responsibility of error correction to the application layer. Whatcan be gathered from the local device and what may be modified and set are specified by SNMPManagement Information Bases, or MIBs for short.***
Index Terms: SNMP v1, SNMP v2c, SNMP v3

I. INTRODUCTION

Any network must have management since it gives users the ability to, among other things, detect defects, change operating parameters, gather data on network performance, and govern how the network is used. The usage of management protocols that provide all types of management data transfers between the manager and managed systems is generally required for network administration. A network of heterogeneous devices known as "things" or "nodes" that typically interact using data link (L2) technology such as ZigBee, Z-Wave, Bluetooth, Wi-Fi, or Low-Rate wireless personal area network with an IoT gateway (hub, controller) connected to the Internet is known as the Internet of Things (IoT) network. It is currently difficult to predict how the many IoT devices will be coordinated given the wide range of machine capabilities and connections. Due to their limited software and hardware capabilities, the majority of Internet of Things (IoT) devices do not support TCP/IP communication, making it challenging to incorporate IoT device monitoring into the primary network monitoring and management system. An SNMP proxy agent can convert IoT monitoring data into Management Information Base (MIB) objects after acquiring the data through the CoAP and MQTT protocols (also called SNMP objects). We can use MIB objects for a variety of reasons because they contain IoT monitoring data.

A. SNMPv1

It is one of the older monitoring protocols and is relatively easier to set up as it takes raw text input. It implements simple procedures for requests and responses such as Get, GetNext, Set and Trap protocoloperations. It outlines a simple, limited MIB that uses scalar variables and two-dimensional tables. Security issues wereone of its limitations and the need for a newer version was strong. For instance, a company can believe that the security of itsinternal network is high enough that SNMPcommunications do not require encryption.In spite of the initial specification, the "community name," which is sent in cleartext, is frequently thought of in these situations as a password.

B. SNMPv2

This was a revision over the previous addressing the security foot falls. It was thesecond generation of the protocol. The protocol included variants as follows (i) SNMPv2c – Community-based. (ii) SNMPv2u – User-Based (iii) SNMPv2* - Commercial Consortium defined protocol. The v2c implementation added support for 64 – bit systems

C. SNMPv3

SNMPv3 overcame the various security constraints that were prevalent in v1 and thesuite of v2. The version 3 was highly modular and was built from the original SNMPv1 and SNMPv2c frameworks. The product is pretty fundamental with the previous versions but also improved upon the following characteristics, (i) Security –Authentication and Privacy. (ii)Administration – Mainly of the Authorization and the access control of thepeople and the policies running on the various network devices that are being maintained by the network management protocol.

SNMPv3 maintains the Usernameand the access keys for secure login and wasable to extend its functionality with Remotemonitoring and Network management using standard SNMP operations. Theadditional features and threat protection functionalities addressed by SNMPv3 are (i) Masquerade avoidance system verifyingthe data integrity and source. (ii) Information modification avoidance byimplementing time stamps. (iii) Uses anaccess control table to confirm operator authorization and safeguard crucial data from malicious and/or unintentional corruption.

II. REAL-WORLDSCENARIOS

A. IoT Monitoring

The general architecture of the SNMP Proxy Agent is shown in fig 1. A smart home environment that makes use of MQTT communication and Home Assistant as an IoT gateway—the source ofIoT events that are recorded in the log file—can be used to illustrate the concept of a unified SNMP interface. The purpose of establishing SNMP proxy agents for IoT devices and gateways is to offer data feeds for the current network monitoring systems.

The SNMP proxy agent's design includes an IoT data extractor that (i) receives IoT monitoring data from various local sources,such as locally captured communication and log files, (ii) extracts values of interest,and (iii) stores them in the IoT monitoring database. The proxy agent's second building piece is an SNMP agent process, which is a TCP server application that handles SNMP requests. When the agent process receives the request, (i) fetches thedefinition of the desired MIB object from alist of supported IoT MIB objects, (ii) searches the database to find the most recent value, and (iii) responds with a MIBobject and its value.

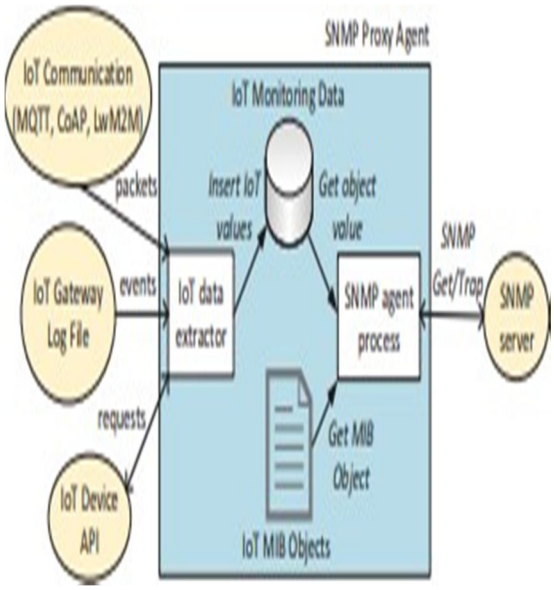


Figure 1 SNMP Proxy agent Architecture

The SNMP proxy agent gathers informationabout IoT monitoring from various sources,converts it into MIB objects, and then makes it available via a typical SNMP interface. The main advantage of thetechnique is that it provides a single view ofall linked IoT and non-IoT devices, regardless of communication protocol. Systems for monitoring specialised applications, software for managing smart buildings, and security and diagnosticapparatus, or just visualising the data on thenetwork monitoring system's dashboard, are all possible ways to process the data further.

B. IoT Control API

A manager device (Android or Windows) that may register numerous client devices with it makes up the Control API. Once the client device is registered with the manager,it uses SNMP get requests to monitor the state of various client properties and buildsa MIB tree for each client. In addition to monitoring, the manager device can also setother client values, including Bluetooth. Figure 1 explains the general approach andmakes it evident that the manager can change both MIBs and that MIBs are maintained on both sides. In addition torequesting the client to make changes to itsMIB via the network, the manager modifiesthe values of parameters in its local MIB. Following the manager's instructions, the client modifies its own MIB and in the client device as well. The continued synchronisation of the two MIBs is ensured.

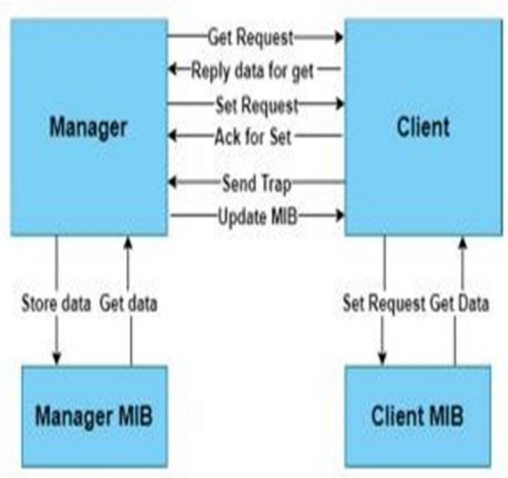


Figure 2 Block Diagram of Control API

1) Client Design

Every client device has a MIB tree that contains all of its many attributes. When a client registers with a manager, the managersends SNMP get requests to the client on aregular basis. While the client responds to the get request by reading data from its MIBtree, a current copy of the client's MIB treeis stored on both the client's and the manager's side.

2) Manager Design

The manager may be running on a Windows or an Android device. Multiple client devices (android devices) can be registered with the manager device for management. The manager issues an SNMP get request after the client device has been registered in order to keep track ofall the various client properties in a MIB tree. The tree is continually refreshed to ensure that it is always consistent with the clients. Using SNMP set commands, the manager can also change a number of client attributes, such as turning on the client's NFC.

3) MIB Tree and OID

An organised text file within the SNMP manager called a management information base is used to gather information and arrange it hierarchically. A MIB tree of each client's attributes is kept up to date. Each Android smartphone keeps track of about 22-50 properties in total. Each attribute's unique OID is used to save the attributes.

4) Client-Manager Interaction

Manager requests an android device's MIB and sends a register request to the client using the client's IP address. The manager receives the MIB from the client, from which it extracts the data it requires to manage, such as Bluetooth and networkstatus, and from which it also creates a local copy of the MIB for every registered client. When a value needs to be changed or toggled, the management sends a signal to the client, who then changes the value and sends a confirmation back to the manager that the change has been implemented in thedevice. When a manager wants to deregistera client, the manager sends the client afinish signal, which deregisters the client.

When a device or client undergoes a change, such as turning on Bluetooth, the mobile phone immediately sends a trap, or message in the form of a form, informing the management that Bluetooth haschanged. When the manager receives the trap, it updates its own MIB.

Because of the widespread use of Windows and Android, these operating systems are required to operate and configure SNMP-based IoT devices. SNMP may be used to provide IoT control APIs for both the Android and Windows platforms.

C. Temperature And RelativeHumidity Monitoring System BasedOn Iot Using A Simple Network Management Protocol

Using a DHT 11 temperature and humidity sensor, the Internet of Things (IoT) may beused to measure temperature and relative humidity. In order for the ESP32 Wi-Fi microcontroller attached to the sensor to communicate with the Open Platform Communication (OPC) server, Simple Network Management Protocol (SNMP) can be used as shown in fig 3.

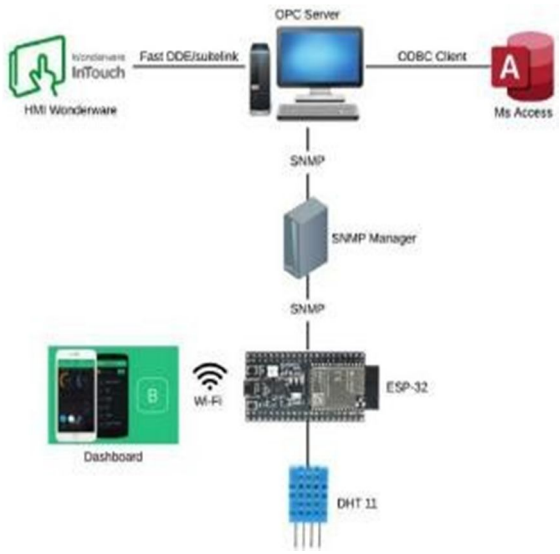


Figure 3 System architecture of IoT

Additionally, Object Identifiers (OIDs) are used to identify the network variables, which are subsequently gathered into a Management Information Base (MIB). TheSNMP monitoring tool needs these two components in order to allow the user to keep track of network infrastructure andconduct troubleshooting. Using SNMP,data collected from the ESP32 Wi-Fimicrocontroller is gathered on the OPC server before being sent to OPC Clientssuch Human Machine Interfaces (HMI) andOPC data loggers for analysis. The ESP32 microcontroller can be linked to a mobile application through Wi-Fi to show real-time data alongside the HMI.

III. RESULTS AND ANALYSIS

The SNMP can be used to combine real- time data collection and IoT device monitoring. To do this, SNMP proxy agentsare installed on IoT gateway devices or in an appropriate network location with accessto IoT traffic. The IoT applications that wehave seen in the paper is shown to be usingMQTT protocol, and we can notice that the usage of SNMP protocol goes hand-in-handwith a wide range of protocols. Theimplementation of interfacing with IoT APIs can further enhance interoperability with other platforms such as Android or Windows. It also provides the manager device with the control plane functionality to be able to control multiple devices.

The latest SNMP proxy agent gathers IoT monitoring information from various sources, converts information into MIB objects, and makes it available via a conventional SNMP interface**.**

SNMP Proxy agents along with cost- effective, large-scale SNMP network managers is used for effective large-scale polling like in real world data centres.

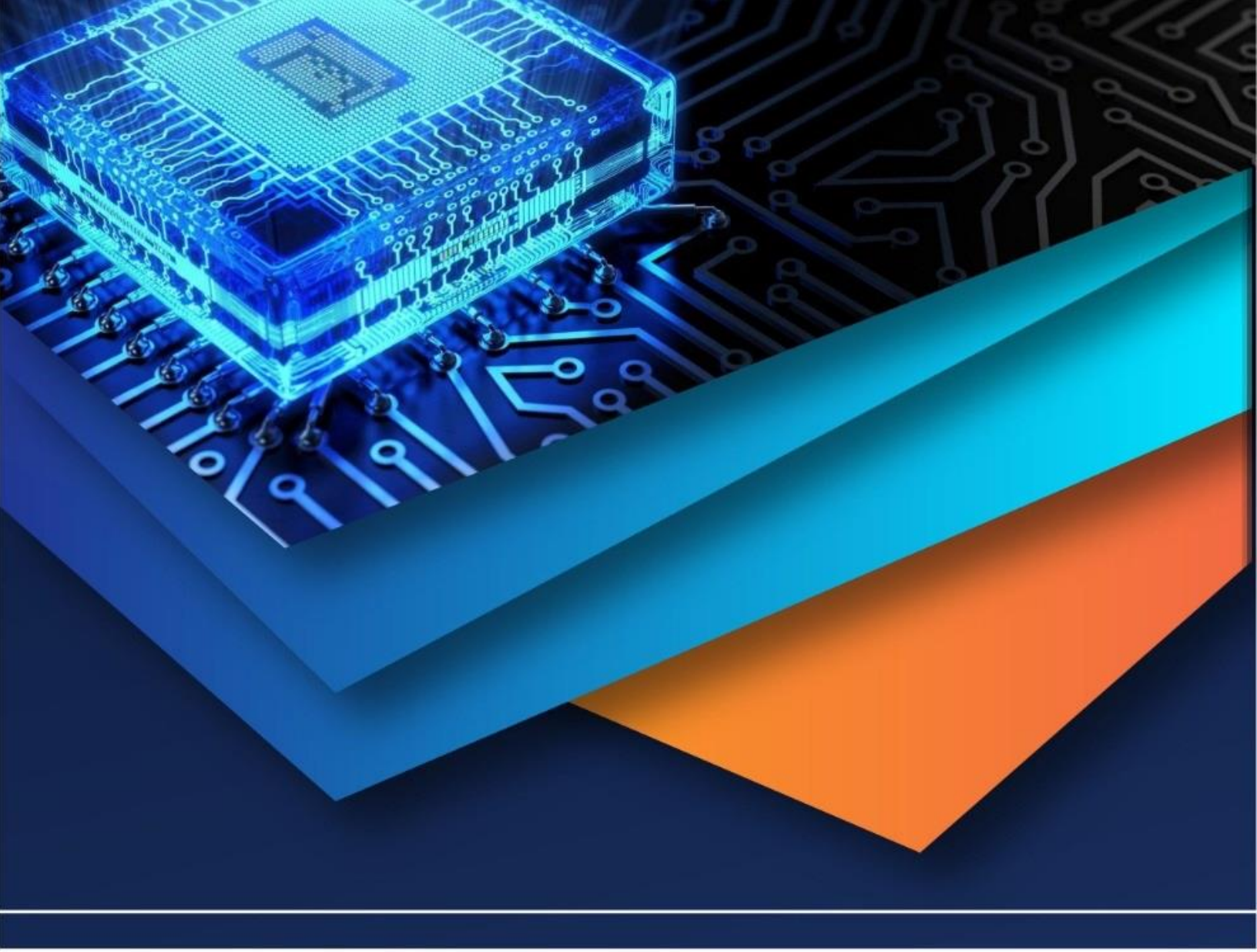
IV. CONCLUSION

SNMP can be used as a protocol for IoT data exchange due to its advantages in being extensively adopted, having a large variety of standard MIBs available,reporting and monitoring network device performance. The client-side monitoring system complies with the security constraint by using SNMPv3 with appropriate security methods, providing nocomprehensive information on the real infrastructure in use, and avoiding information leakage risks.

REFERENCES

[1] M. Savić, M. Ljubojević and S. Gajin,"A Novel Approach to Client-Side Monitoring of SharedInfrastructures," in IEEE Access, vol.8, pp. 44175-44189, 2020.
[2] Z. Hu, Y. Qiao and J. Luo, "ATME: Accurate Traffic Matrix Estimation inBoth Public and Private DatacentreNetworks," in IEEE Transactions on Cloud Computing, vol. 6, no. 1, pp. 60-73, 1 Jan.-March 2018.
[3] P. Roquero and J. Aracil, "On Performance and Scalability of Cost- Effective SNMP Managers for Large-Scale Polling," in IEEE Access, vol. 9, pp. 7374-7383.
[4] S. Sinche et al., "A Survey of IoT Management Protocols andFrameworks," in IEEECommunications Surveys & Tutorials, vol. 22, no. 2, pp. 1168-1190, Secondquarter 2020.
[5] W. Zhang, M. Dong, K. Ota, J. Li, W.Yang and J. Wu, "A Big DataManagement Architecture for Standardized IoT Based on Smart Scalable SNMP," ICC 2020 – 2020 IEEE International Conference on Communications (ICC), 2020, pp.1-7.

[6] M. Zeeshan, M. Z. Siddiqui and F. B.Rashid, "Design and Testing of SNMP/MIB based IoT Control API,"2019 IEEE 16th International Conference on Smart Cities:Improving Quality of Life Using ICT& IoT and AI (HONET-ICT), 2019, pp. 054-058.
[7] O. Boyar, M. E. Özen and B. Metin, "Detection of Denial-of-Service Attacks with SNMP/RMON," 2018IEEE 22nd International Conference on Intelligent Engineering Systems (INES), 2018, pp. 000437-000440.
[8] F. A. Hambali, R. Fitriana and E. Joelianto, "Integration System of IoT Gas Sensor using Simple Network Management Protocol and Open Platform Communication," 2021 IEEE 7th Information Technology International Seminar (ITIS), 2021,pp. 1-6.
[9] M. Malboubi, "Optimal-CoherentNetwork Inference (OCNI): Principles and Applications," in IEEETransactions on Network and Service Management, vol. 15, no. 2, pp. 811-824, June 2018.
[10] N. Aji, Nazuwatussya'diyah and E. Joelianto, "IoT-Based Temperature and Relative Humidity Monitoring System Using Simple Network Management Protocol," 2021 International Conference on Instrumentation, Control, and Automation (ICA), 2021, pp. 174-179.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY