Monitoring of Android Devices using SNMP

Karan Grover
IIIT Delhi
karan13048@iiitd.ac.in

Vinayak Naik
IIIT Delhi
naik@iiitd.ac.in

***Abstract*— Mobile technology is revolutionizing the way companies do business, by improving business processes, increasing productivity and enhancing customer experience. Hence the need to manage/monitor the mobile phones has never been higher. Simple Networking Management Protocol (SNMP), is an internet standard protocol for managing IP devices on a network. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. No doubt then, SNMP must be used to monitor smart phone devices for conditions that warrant administrative attention. In this paper we talk about 1. Building one of the very first SNMP Agents for Android Operating System implementing SNMP version I, II and III, 2. The results after performing benchmark tests on the SNMP Agent and measuring its performance on the phone and in challenging networks like 2G and 3G.**

I. INTRODUCTION

Many businesses face various mobile computing challenges when dealing with both Corporate Owned, Personally Enabled (COPE) devices and employee owned devices as part of the Bring Your Own Device (BYOD) program. These trends in the area of Mobile Device Management(MDM) have introduced significant challenges for IT administrators who want to enable enterprise mobility while ensuring that corporate resources are protected from unauthorized access. In this paper we describe how we have built one of the first apps, that allow device configuration management and health monitoring in real time using Simple Networking Management Protocol (SNMP)[1]. Using this we were able to monitor various aspects of the phone's health like: uptime, memory usage, ping latency and number of processes and watch real time updates using popular Network Management Systems (NMS) like Cacti and Nagios. We have also implemented SNMPv3 which incorporates authentication and encryption. We then tested the performance of the phone using 2 tests which we have talked about later.

II. RELATED WORK

WSO2 Enterprise Mobility Manager is an open source software that provides Mobile Device and Mobile App management, but doesn't essentially use SNMP. Android SNMP SDK is an Android version of SNMP based on open source NET-SNMP project. It currently supports only GET request. A different implementation of SNMP Agent on Android without SNMPv3 and SNMP4J.[2]

III. ARCHITECTURE

A. Simple Networking Management Protocol

A typical SNMP Network consists of a manager and many agents. A managed device is a network node that implements an SNMP interface that allows it to exchange node-specific information with the NMSs. An agent is a network-management software module on the managed device that exposes management data on the managed systems as variables which are organized in hierarchies. These hierarchies, and other metadata are described by Management Information Bases (MIBs). Another key component of SNMP-managed network is the Network Management Station (NMS). A NMS executes applications that monitor and control managed devices. The NMSs that we have used to test our agent are: Cacti and Nagios.

B. SNMP Agent for Android

To implement the SNMP Agent on Android we have used the free and open source SNMP4J library. When the app is started, it creates an intent service which runs the Agent on port 2001. After the agent starts running we use the already registered SNMPv2MIB[3] which allows us to query attributes like uptime, disk space, load average, memory usage, ping latency and number of processes.For implementing SNMPv3[4] we have to register the user with the Agent. For that we have to specify the version number, username, security level, authentication protocol, encryption protocol, authentication passphrase and encryption passphrase. For implementing Traps we created our own PDU of type - NOTIFICATION and sent it via the Snmp Class. It is worth mentioning that the rather sparse documentation of SNMP4J library makes implementing SNMP on Android a challenging task. Also, since mobile operators do not allow unsolicited incoming IP packets, we were not able to measure the performance of GET, GETNEXT and SET requests on 2G and 3G network. While measuring Trap, to get absolute latency we would require the mobile phone and the machine to synchronize time at the millisecond level. To avoid this, we have given latency w.r.t WiFi.

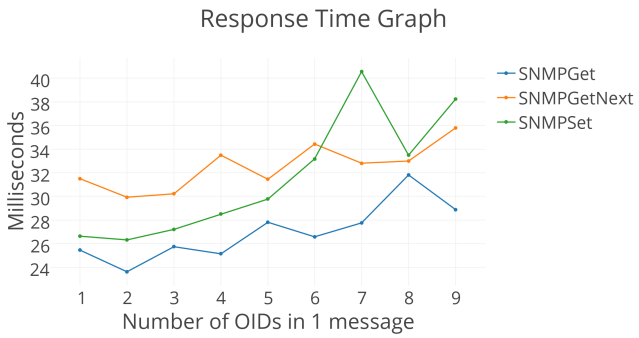
IV. BENCHMARK TESTING

A. SNMP Performance in various Networks

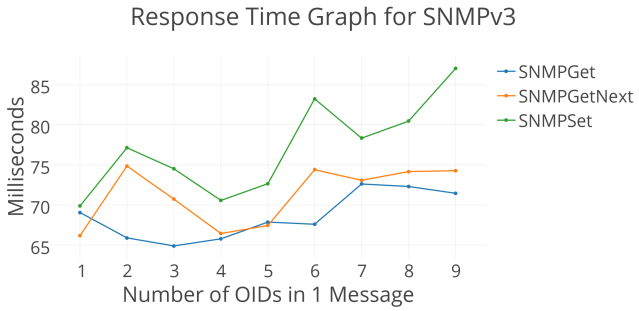
For performance evaluation we have taken 4 kinds of messages into account: snmpget, snmpgetnext, snmpset and snmp traps. Using snmpget request, the manager can request for value of a particular OID. Using snmpgetnext, the manager can ask the value next to that of the current OID. Using snmpset the manager can set the value of a particular OID. Using SNMP Traps the agent can send important information to the manager. There are 2 metrics that are important when measuring the performance of the Agent. Response Time and Response to Request Ratio. The Response time is the

978-1-4673-9622-6/16/$31.00 ©2016 IEEE

difference between the time when the response is received and when the request is sent. The following is the the graph representing the response times of different messages.



(a) Response time of SNMP requests with increasing number of OIDs in 1 message.

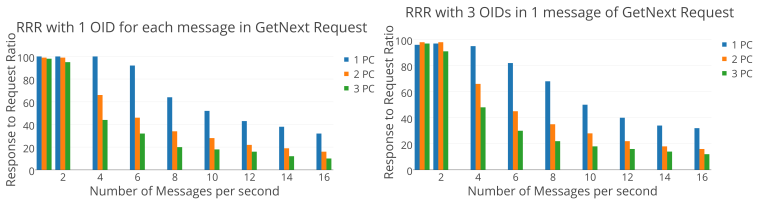


(b) Response time of SNMP v3 requests with increasing number of OIDs in 1 message.

The above graph shows snmpget, snmpgetnext and snmpset requests for SNMP v2. As we can see SNMPGet requests take the least time while SNMPGetNext and SNMPSet requests take more time than the Get Request. In the second graph we show the time taken by same requests for SNMP v3 and we see, as expected, a rise in response times. We saw snmpget values rise by 2.87 times, snmpgetnext by 2.228 times and snmpset by 2.144 times. Our second metric was Response to Request Ratio. RRR is the ratio between the number of responses received to the number of requests sent. This is a useful metric which tells us how the Agent performs under stressed conditions. To measure the performance of SNMP on challenging networks like 2G and 3G, we have used traps. We measured the relative delay as compared to WiFi when sending Traps from an android phone to a SNMP Server. The results have been shown in Figure 1. We can see that requests take about 1.43 times more time in 2G network than 3G.

(c) Response to Request Ratio of Get requests with 1 OID in each message.

(d) Response to Request Ratio of Get requests with 3 OID in each message.



(e) Response to Request Ratio of GetNext requests with 1 OID in each message.

(f) Response to Request Ratio of GetNext requests with 3 OID in each message.

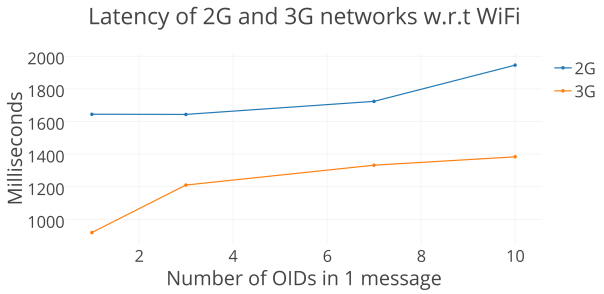


Fig. 1: Latency of Trap requests relative to WiFi. On an average 3G requests take 1200 ms more than wifi, and 2G requests take 1700ms more than wifi to reach the manager.

B. Health Monitoring of Android Device

We have shown graphs for Logged In users and number of processes among many other attributes, at a 5 minute interval and measured daily, weekly and monthly average using Cacti.

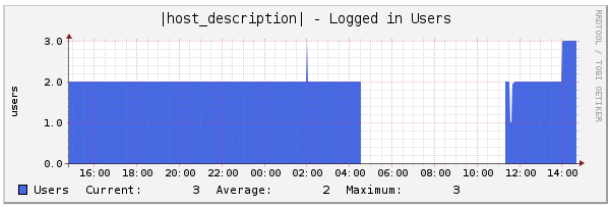


Fig. 2: Logged In Users on Android phone in Cacti

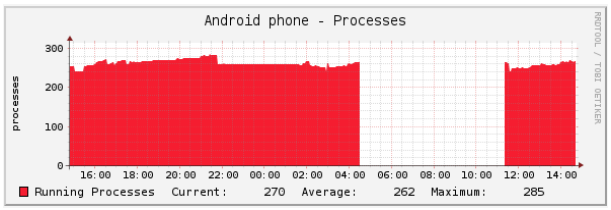


Fig. 3: Number of Processes on Android phone in Cacti

REFERENCES

[1] J. Case, M. Fedor, M. Schoffstall, and J. Davin, A Simple Network Management Protocol (SNMP), RFC 1157, May 1990.
[2] Fernando Hidalgo, Eric Gamess, Integrating Android Devices into Network Management Systems based on SNMP, 2014
[3] L. Walsh, SNMP MIB Handbook, Wyndham Press, March 2008.
[4] W. Stallings, SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, Addison-Wesley Professional, 3rd Edition, October 2013.