Master Subagent Based Architecture to Monitor and Manage Nodes in Mobile Ad-hoc Networks

Vishalakshi Prabhu H
(Department of Computer Science & Engineering, Rashtreeya Vidyalaya College of Engineering, Bangalore, 560059, India,)

ABSTRACT

Ad-hoc wireless networks have been receiving increasing attention in the research community as well as the industry. Ad-hoc wireless networks are distributed systems formed spontaneously without relying on existing infrastructure. It's formed from wireless mobile nodes which can move around freely; dynamically self-organize into temporary network topologies. Currently there are certain tools available to the network administrators to discover the mobile network nodes automatically. However monitoring is more difficult in networks where the topology changes very frequently such as Mobile Ad hoc networks (MANET). In this paper, an SNMP based framework that is distributed and used to collect statistics from any interface is discussed. This paper outlines the experience of implementation of a Simple Network Management Protocol (SNMP) agent based framework.

Keywords- **Embedded, FCAPS, interface agent, master agent, sub agent.**

1. INTRODUCTION

Network management is a highly technical subject. FCAPS - Fault, Configuration, Accounting, Performance and Security are a common way of modularizing the network management functions. A set of fault monitoring, diagnostic and control capabilities are essential to manage any network.

Mobile Ad-hoc networks are characterized by low bandwidth, link loss and by constant topology change. It is challenging to keep the arbitrarily formed network and application work properly because MANETs present several constraints. They are characterized by a dynamic network formation, scarcity of resources and distributed nature. These features make their management a difficult task. Also, the traditional network management approaches become impractical in MANET environment. [1]

The Simple Network Management Protocol (SNMP) is the most popular network management protocol for wirednetworks. SNMP uses a Management Information Base (MIB) to store the state of the various entities in a network node. A local SNMP agent is responsible for maintaining the database on the node. The MIB database has a well-defined syntax called Abstract Syntax Notation (ASN.1) and the values of all the monitored elements are stored in the database. SNMP uses User Datagram Protocol (UDP) for communicating with the database using a set of simple primitives to query and set the state of MIB element**.** [2]

2. LITERATURE SURVEY

2.1 Simple Network Management Protocol

The heart of network management activity involves gathering information from network elements. In SNMP, management information is represented in a structured manner in the management information base (MIB). Every node in the network maintains an MIB that can have information about its current configuration, operation statistics, and parameters to control its functioning. Objects in the MIB are divided into different groups [3]. In a typical SNMP setup, any one node is assigned the responsibility to manage a sub network or a set of agents. This node is called the manager node which polls its agents by sending SNMP protocol data units (PDU's) [3], [4].

2.2 Management approaches in MANET

In a MANET environment, management is a difficult problem because the constantly changing topology induces additional overhead for network state collection over bandwidth-constrained links if one uses traditional network management techniques. To overcome the challenges, Willard [5] suggests that an ad hoc network management protocol must meet these critical requirements. Firstly, it must be able to maintain Network

Management (NM) services through dynamic networking conditions through self-configuration. Throughout the life of the network it may autonomously merge with other sub-nets or partition, and nodes may dynamically join or exit the network. The NM architecture must adapt to these changes to maintain NM services across the MANET. Secondly, the NM architecture has to be highly efficient. Maintaining the NM across a dynamic topology requires a higher degree of overhead compared to static networks.

The ANMP (Ad Hoc Network Management Protocol) is described in [6] to manage ad hoc networks. ANMP introduces the concept of cluster-based management where nodes in the network participate in the cluster construction and cluster head election process. Management is based on a hierarchical approach where cluster heads poll management information from their cluster members in a centralized manner.

In contrast, the Guerrilla management architecture provides management flexibility and continuity by making its nomadic managers adapt to dynamic network conditions. Moreover, nodes with probe processing capability facilitate management by delegation, where management functionality is not limited to information polling, which results in more efficient bandwidth utilization. [7]

Policy-driven approaches have been suggested for ad-hoc network management such as Phanse's PBNM [8], Policy-Enabled Configuration Across Networks (PECAN) [9] and Bhatia’s PENM [10], Chadha’s PBMANM [11], Chadha’s PBN [12]. In such approaches, policy servers or mobile agents are deployed in a distributed manner in the network. This distribution may be full or partial. The agents carry policies for monitoring and reporting of local events to a central reporting node.

If the agents are not fully distributed, the agents could be placed in certain locations in the network where they collect information about the hosting node as well as neighboring nodes. The strategy for locating the agents can be static or dynamic. If the network is not mobile and the topology remains fairly static, the agents can be placed based on an off-line algorithm that optimizes their location based on some metric like topology, traffic profile etc. If the topology changes quite often due to mobility or otherwise, then a dynamic placement policy is required. These approaches enable specific policies to be enforced such that the management framework only responds to certain types of events or changes in the network. This minimizes the amount of data collection but the information granularity and its accuracy depends on whether a correct policy has been devised for the situation that the node is experiencing at any given moment. This is because anticipating, defining and deploying the correct policies are not feasible for all possible situations.

3. PROPOSED SYSTEM

Since MANET is highly dynamic in nature, we need a way to control this system through mobile or wired terminals connected to the mobile node. The system needs integrated management software that supports FCAPS i.e. Fault, Configuration, Accounting, Performance and Security to all system components. This paper discusses about a software component that can be embedded into a mobile node to manage it through various interfaces. One of such interface can be Simple Network Management Protocol (SNMP). SNMP provides a management interface to the node. Limited FCAPS can be implemented. To function, this management software must be embedded in node. Also allow various levels of access based on user profile and this is supported by SNMP v3.

4. PROPOSED METHODOLOGY

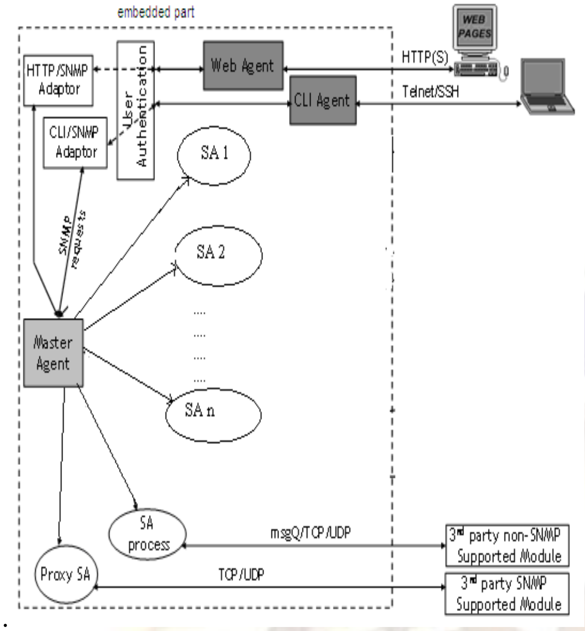
SNMP supports management of nodes using standard SNMP commands. The core of this architecture is the protocol agents supporting SNMP. Interface agents supporting user interfaces can be HyperText Transport Protocol (HTTP) or Command Line Interface (CLI).

A Master Agent (MA) supporting SNMP will be the central gateway in this architecture. MA will provide central tasks such as authentication and security. It also supports standard MIB objects.

A set of subagents (SA) will be supporting the MA in implementing module specific management functionality. Each module requiring management interface will have a corresponding subagent. (E.g. one for Domain Name System (DNS), one for routing...). Subagent is responsible for all module specific interface and implementation including module specific enterprise MIBs.

Proxy agent is a special sub agent supporting third party SNMP Agents.

If HTTP is supported, web agent will be responsible for serving all HTTP connections. This includes web authentication, translating HTTP to SNMP and translating responses back to HyperText Markup Language (HTML).



.

Figure 1: Master subagent architecture

As shown in Fig.1**,** The Master Agent is the main management gateway. If HTTP is supported, the web agents can translate the input request into SNMP and connect to Master Agent

There can be limited number of user groups that have specific access rights to the system. These will be mapped into SNMPv3 view based access, MIB object definitions and HTML display restrictions. Once an authenticated telnet session is established to a node, it should be possible to make HTTP or SNMP sessions to other nodes in the current topology. This doesn't require any special implementation on the management software module and is dependent on the security policies.

5. MASTER SUB AGENT ARCHITECTURE

5.1 Master Agent (MA)

The Master Agent present on a managed node is an entity or process. It exchanges SNMP messages with the management applications. Master agent functions as a primary interface between the Network Manager (NM) and sub-agents (SA).

In the architecture, SNMPv3 aware Master-Agent will be the central gateway for all administrative interfaces. All user requests from user interfaces like web-agent and SNMP will be processed by Master Agent.

Master Agent will be responsible for:

- Centralized services like authorization, authentication, access control and enforcing security and privacy policies.
- Standard MIBs support
- Handle all protocol specific translations (E.g. handling all versions of SNMP PDUs).
- Sub agent management (locating sub agents, list of sub agents, etc) and serves as SNMP proxy for all sub agents that are registered with it.

5.2 Sub Agent (SA)

Sub-agents are processes designed for very specific applications or components. They access the management information and provide manageability to various applications and components within a system. Such sub-agents interact with the Master Agent using SNMP. Separate Sub Agents should be implemented to support various modules in the mobile node.

The subagent instrumentation code should be embedded within the module running a separate thread. The interaction between Master-Agent and Sub-Agent will be based on Inter Process Communication (IPC) sockets. The interaction between Subagent and the module will be based on module provided Application Programming Interfaces (APIs). Product should define this API along with the MIB documentation.

On startup, the sub agent should register with the master agent with the list of MIB objects it is responsible for.

The following sequence diagram shows how the requests and traps are processed between MA and components.

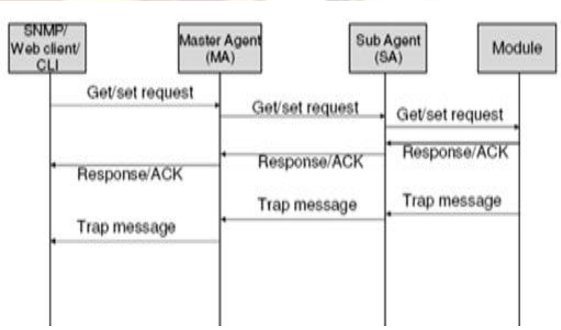


Figure 2: Sequence diagram of user requests

The following Sub-agents can be developed to interface with specific modules.

- Routing Subagent

- Core network services Subagent
- Autoconfiguration Subagent
- QoS Subagent
- Platform Subagent …..

Sub-agents are not limited to the tasks mentioned here. If any other functionality needs to be added, design the MIB and include corresponding sub-agent to support that task.

5.3 Proxy Agents

It is a special sub agent that serves as front end to other SNMP agents. This can be used in the software to integrate 3rd party SNMP agents. Proxy agent will support MA-SA protocol (SNMP in this architecture) on the northbound talking to MA and SNMP (SNMPv3, SNMPv2c or SNMP1) on the south bound talking to the external SNMP agent. Proxy agent will register all 3rd party MIB Objects with the Master Agent. When MA directs such requests to proxy, proxy should redirect them to the 3rd party SNMP agent. The proxy agents are able to support any SNMPv2c or SNMPv1 based external agents via SNMPv3.

The following diagram shows how SNMP requests for SNMP agents are handled by module using proxy agent.

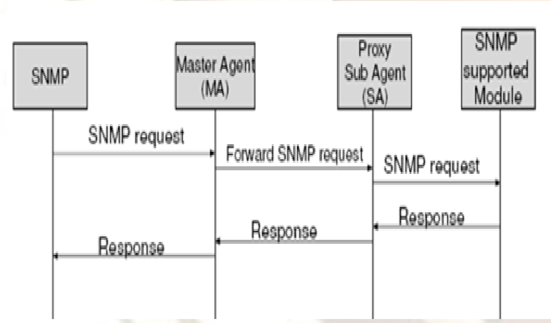


Figure 3: Sequence diagram of user requests for 3rd party SNMP supported module

5.4 Web Agent

Web Agent is optional. If supported, it could be Apache 2.2 based web server that provides HTTP access to web clients (browsers) in the front end and translates the HTTP request into SNMP request in the back end. On the south bound, design it to talk to the MA using SNMP.

Hypertext Preprocessor (PHP) scripts could be developed to access internal MIB objects from Master Agent. These scripts could be designed to generate HTML pages to be displayed on browsers. The display process should be automated with the use of style sheets. The agent could be allowed to access an Extended Markup Language (XML) file with access restrictions. This file should have the display restrictions.

5.5 Module interaction

As discussed before, software will interface through sub-agents with mobile node specific modules and through proxy agents with external (3rd party) components.

5.6 Management Interface for data objects

Module interaction for data objects could be done via module defined APIs. This could be used uniformly for read-only or read-write data and for data in any form (data in config file, /proc, in memory, in database, etc). This will avoid exposing internal access methods of module to the management software.

6. PERFORMANCE EVALUATION

6.1 Significance of Master - Sub-agent concept

In the original model of SNMP Management, single monolithic agent is used to carry out majority of the management responsibilities on a given network element. This approach is not flexible to provide an effective management of dynamic, complex and distributed systems. So the emphasis is given on a modular agent design for MANET management.

Ad-hoc wireless system is increasingly complex. Different functional components of the network will be present in different processors. So each component say routing, auto configuration, Medium Access Control (MAC) needs its own management requirement. Therefore each component will have an SNMP agent. However, there should be a single gateway for managing the entire network (distributed components).

Disadvantage of the monolithic agent concept of original SNMP model is solved using master-sub-agent concept. Original SNMP model is not capable of supporting complex and heterogeneous systems. Hence master agent should functions as a proxy for other SNMP agents.

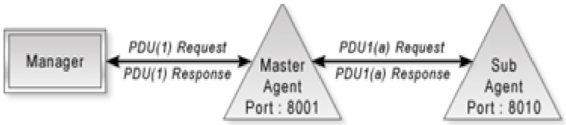


Figure 4: Master - Subagent communication

6.2 Registering Sub-Agents in the Master Agent

The Master Agent should maintain the proxy table which is used to store information about sub-agents. Each entry/row in this table can refer to one sub-agent. Each row has one sub-agent's information such as Object Identifier (OID), context name, instance value, Internet Protocol (IP) address, port number, community, version, timeout, retries, etc. Adding an entry to this table is nothing but registering one sub-agent in the master agent.

Two ways to register sub-agents in the Master Agent are

- Before Agent Startup
- During Run Time

Similar to the steps mentioned in adding entries, the entries can be deleted from the table.

6.3 Heart Beat Mechanism

Heart Beat Mechanism is used to determine the presence of a connection between master and sub-agent. This feature should be implemented to monitor the status of the sub-agent frequently and notify it to the master agent. If the status is known, the master agent need not forward the request to sub-agents, which are not alive. Instead, the master agent should be designed to throw a 'general failure' error to the manager directly.

6.4 Security Management

Standard and enterprise MIB document will detail the read and read-write objects for each module. Further, SNMP v3 view based access will be used to map these profiles to object access. Username and password are required to access the system. SNMPv3 authentication will be used for this. Further, SNMPv3's message integrity and encryption options could be used depending on the overall system security policies.

7. CONCLUSION AND FUTURE WORK

Several management solutions to manage MANET are discussed in the literature. In this paper, an architecture based on master-subagent to manage and monitor MANET is discussed. Developing the specific management software for MANET is challenging. It will provide an insight into the working of one of the rapidly deployable network system. The master subagent concept functions well for the MANET.

There is a lot of scope for further work as the software is prototyped for an Ad-hoc system that is still under research for optimization. The proposed architecture is a part of complete software needed for the establishment of Ad-hoc network.

Command line interface (CLI) can be added to the proposed software. Limited FCAPS could be implemented due to resource constraints associated with embedded nature of SNMP based software.

REFERENCES

[1] Said El brak, Mohammed Bouhorma, Anouar A. Boudhir, "Network Management Architecture Approaches Designed for MANETs", *International Journal of Computer Applications (0975 – 8887) Volume 15– No.6*, February 2011

[2] William Stallings, "SNMPv3: Security Enhancement for SNMP", *IEEE communications surveys*

[4] W. Stallings, "SNMP and SNMPv2: The infrastructure for network management", *IEEE Communication Magazine, vol. 36, pp. 37–43*, Mar. 1998

[5] Willard, Doug, "Network Management Architecture for the Objective Airborne Network," *Invited paper, MILCOM*, 2004.

[6] Chen, W. et al. "ANMP: Ad Hoc network Network Management Protocol," *IEEE JSAC*, October 1999.

[7] Shen, Chien-Chung et al., "An Adaptive Management Architecture for Ad Hoc Networks," *IEEE Comm., vol 41-2*, pp. 108-115, February 2003.

[8] Kaustubh S. Phanse, Luiz A.DaSilva, Scott F.Midkiff, "Design and demonstration of policy-based management in a multi-hop ad hoc networks," *IEEE Comm vol. 3(3)*, pp. 389-401, 2005

[9] Chadha, Ritu and Cheng et al., "PECAN: Policy-Enabled Configuration Across Networks," *Fourth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'03)*, pp. 52, 2003.

[10] R. Bhatia et al., "Policy Evaluation for Network Management", *INFOCOM* 2000

[11] R. Chadha et al., "Policy-Based Mobile Ad Hoc Network Management", *Yorktown Heights, New York*, June 2004.

[12] R. Chadha, G. Lapiotis, S. Wright, "Policy-Based Networking", *IEEE Network, March/April 2002, Vol. 16 No. 2, guest editors.*

Books :

[3] W. Stallings, *SNMP, SNMPv2, and CMIP: The Practical Guide to Network Management Standards* (1st ed. Reading, MA: Addison-Wesley, 1993).