

Conceptualization of a Secure Agent Based Network Management System

O B. Ajayi, University of Agriculture, Abeokuta, Nigeria; E-mail: tayojayi@yahoo.co.uk

ABSTRACT

As configuration of network services is faced with wide-spread deployment problems requiring considerable human efforts and involvement, Plug-and-Play (PnP) services become a central concern. Moreover, the recent developments in the area of mobile agent based network management and ever improving Java Programming language have provided important tools for designing Secure Mobile Agent based PnP Protocol (SMA-3P). Again, a roaming agent on a network consumes significant network bandwidth which implies that their frequency and number must be regulated. In a sensitive and intelligent network where the PnP behaviour can be altered dynamically during the lifetime, the proposed system must be genuinely secure. So, it is necessary to design secure protocol using the elliptic curve based multi-signcryption for the purpose of efficiency.

Keywords: Mobile Agent, Security, Plug-and-Play, Protocol, Network, Configuration

1.0 INTRODUCTION

The current network is characterized by its increasing distribution, its dynamic nature, and the complexity of its resources, due to the increasing requirement of different services (Yang, 2003). Network management essentially involves monitoring and controlling the devices connected in a network by collecting and analyzing data from the devices (Stallings, 1999).

The current trend is to deploy mobile agents to manage large heterogeneous networks. Mobile agents are special software objects that have the unique ability

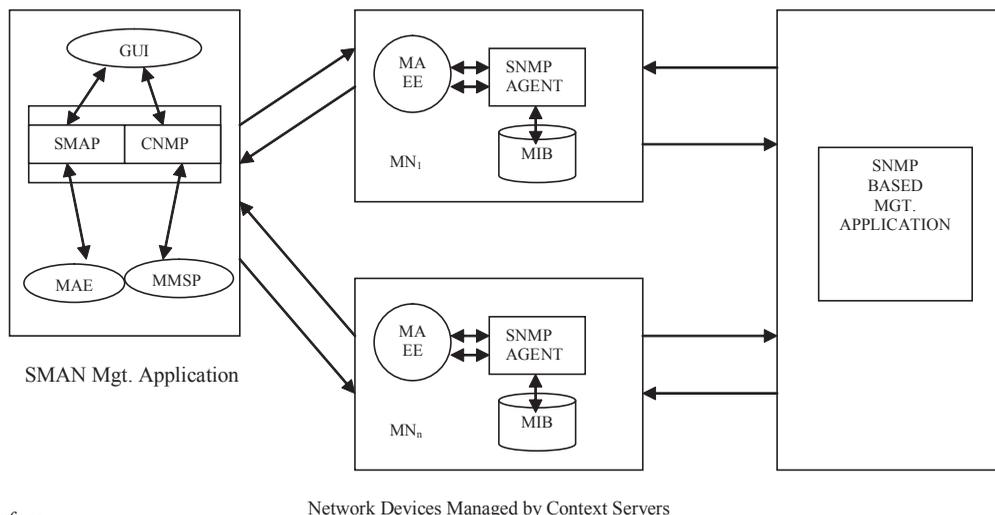
to transport itself from one system in a network to another in the same network (Feng, 2002).

One of the possible approaches is to automate the installation and configuration steps using a mobile-agent based Plug-and-Play (PnP) architecture for service configuration.

2.0 RELATED WORKS

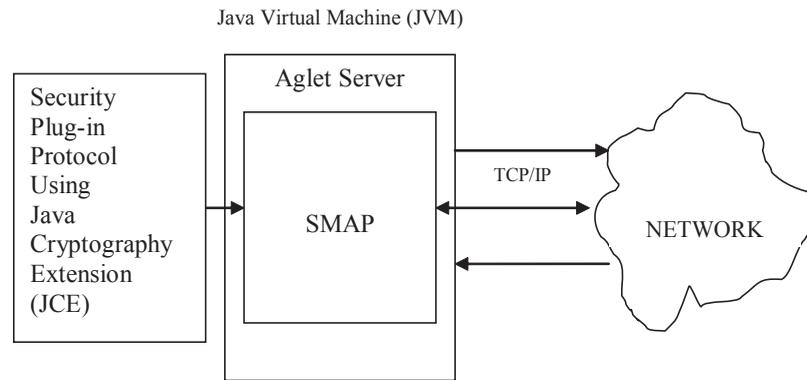
As networks are growing and becoming more distributed, the need for better management through available distributed technologies is being realized. According to Kona (2002), mobile agent technology has long been pursued but its applications in network management are still rudimentary. Bieszczad et al. (1998) described theoretical views on application of mobile agents for network management that lack concrete implementation. Gavalas et al. (2000) presented the application of mobile agents in bulk transfer of network monitoring data, data aggregation and acquiring atomic SNMP table views. They analyzed the usage of mobile agents in network management with regard to the bandwidth utilization. The work addresses the issue of mobile agents for network monitoring, but did not consider provisioning services. Pinheiro et al. described a conceptual model which collects management related data across a changing set of networked components and periodically compute aggregated statistics using mobile agents. More concentrated towards aggregation of network monitoring data and exploring mechanisms for agent adaptation.

Figure 1. Hybrid SMAN model



Keys:
 GUI – Graphical user Interface
 CNMP – Conventional Network Management Protocol
 MIB – Management Information Base
 MN_i – Managed Nodes where i = 1 to n

Figure 2. SMAN station



3.0 OBJECTIVES

1. To provide a comprehensive review of mobile agent architectures, development tools and emerging agent technologies
2. To develop a prototype application system that will allow the development of the network management system using a secure mobile agent oriented approach
3. To employ the use of discrete logarithm based multi-signcryption for the secure protocol.

4.0 SMAN ARCHITECTURE

SMAN station assumes responsibilities of a client. All managed nodes are servers, which has mobile agent execution environment and respond to SNMP queries from mobile agents when they visit the servers and manipulate data locally. When the client in the SMAN needs access to data in a network-connected device, it does not talk directly to the server over the network but dispatches a mobile agent to the server's machine. On arriving at the servers' machine, the mobile agent makes its request and return to the management station with the results.

The SMAN architecture consists of the following major components:

- Management application (MAP)
- Mobile Agent Execution Environment (MAEE)
- Secure Mobile Agent Producer (SMAP)
- Mobile Agents (MA)
- Modified Multi-signcryption protocol (MMSP)

The mobile agent development environment is the Aglet Software Developer Kit (ASDK), which provides a modular structure, easy-to-use API for programming of mobile agents and excellent documentation.

Figures 1 and 2 show the hybrid model of SMAN and architecture for network management using secure mobile agents. The administrator/manager is given the flexibility of deciding whether to use SNMPv3 or mobile agents.

6.0 CONCLUSION

This paper has demonstrated that it is possible to develop a secure mobile agent network management system using Java components and cryptography. To this end, the paper has presented reasonable detail on design level view.

REFERENCES

- Bieszczad, A., Pagurek, B. and White, T. (1998a): Mobile Agents for Network Management. IEEE Communication Survey, Vol. 1 No. 1
- Bieszczad, A., Raza, S. K., Pagurek, B. and White, T. (1998b): Agent-based Schemes for Plug-and-Play Network Components. Proceedings of the 3rd International Workshop on Agents in Telecommunication Applications. IATA '98
- Feng, X. (2002): "Design and Analysis of Mobile Agent Communication Protocols", Master of Science (M.Sc) paper, Institute of Computer Software, Nanjing University, China
- Gavalas, D., Greenwood, D., Ghanbari, M. and Mahogany, M. O. (2000): Advance Network Monitoring Applications based on Mobile Intelligent Agent Technology. Computer Communications.
- Kona, M. K. and Xu, C. (2002): "A Framework for Network Management using Mobile Agents", available at <http://www.ernie.eng.wayne.edu>
- Pinheiro, R., Pohylisher, A. and Caldwell, H. (2000): Mobile Agents for Aggregation of Network Management Data, Telecordia Technologies, University of Warwick, Bell South Telecommunications.
- Stallings, W. (1999): SNMP, SNMPv2 and RMON: Practical Network Management. Addison-Wesley.
- Yang, K., Galis, A., Mota T., and Michalas, A. (2003): "Mobile Agents Security Facility for Safe Configuration of IP Networks" EU IST project MANTMP, funded by commission of EU.
- Zheng, Y. (1997): "Digital Signcryption or How to achieve cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)" "Advances in cryptology - crypto '97, Lecture Notes in Computer Science, Vol. 1294 pgs 165-179, Springer-Verlag

0 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/proceeding-paper/conceptualization-secure-agent-based-network/33341

Related Content

Classification of Sentiment of Reviews using Supervised Machine Learning Techniques

Abinash Tripathy and Santanu Kumar Rath (2017). *International Journal of Rough Sets and Data Analysis* (pp. 56-74).

www.irma-international.org/article/classification-of-sentiment-of-reviews-using-supervised-machine-learning-techniques/169174

Use of Online Social Networking and Academic Performance of Students

Maslin Masrom and Selisa Usat (2015). *Encyclopedia of Information Science and Technology, Third Edition* (pp. 2654-2661).

www.irma-international.org/chapter/use-of-online-social-networking-and-academic-performance-of-students/112682

Dotted Raster-Stereography

Muhammad Wasim, Fauzan Saeed, Abdul Aziz and Adnan Ahmed Siddiqui (2018). *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 166-179).

www.irma-international.org/chapter/dotted-raster-stereography/183731

Women's Employment in Turkey's ICT Sector: An Examination From a Social Inclusion Perspective

Selda Gorkey (2019). *Gender Gaps and the Social Inclusion Movement in ICT* (pp. 63-86).

www.irma-international.org/chapter/womens-employment-in-turkeys-ict-sector/218439

Health Information Technology/BioDefense Needs to Fight Bio-Terrorism

Tanushree Govil and Jivesh Govil (2015). *Encyclopedia of Information Science and Technology, Third Edition* (pp. 3366-3375).

www.irma-international.org/chapter/health-information-technologybiodefense-needs-to-fight-bio-terrorism/112767