A Study of SNMP Developments Regarding to Security and Performance

Diogo Nunes de Oliveira, Sérgio Granato de Araújo, Getúlio Antero de Deus Júnior, Marcelo Stehling de Castro, Thiago Lara Vasques, Adriano Bittar
Escola de Engenharia Elétrica e de Computação (EEEC), Universidade Federal de Goiás (UFG), Goiânia – GO, 74000-000, Brasil
diogo.dno@gmail.com, getulio@eeec.ufg.br, granato@eeec.ufg.br, mcastro@eeec.ufg.br, thiago_lv@hotmail.com, adrianobittar@gmail.com

Aderbal Alves Borges
Innovation Consulting (InnovaCon), Goiânia – GO, 74000-000, Brasil
aborges.consulting@gmail.com

Roberto Ibrahim Brihi Badur
BLM Inovações Tecnológicas, Goiânia – GO, 74000-000, Brasil, rbadur@gmail.com

Abstract

Telecommunication network availability is essential for all companies because their income is directly related to it. Because of this fact, network management systems also became essential, but the importance of managed information is faced by most network administrators as useless to others, therefore securing the management data is not considered. The main goal of this article is to show the importance of network management data and stimulate the use of security in network management systems. The good performance of network management systems are also important, therefore some tests are performed to verify how intensively the network and network manager performance can be injured by the use of cryptography algorithms and specially by the AES cryptographic standard in order to study the viability of the SNMPv3 with AES set. These tests are taken as a preview of a Broadband Power Line Network Management pilot project that is being implemented in the main electrical power transmission company in Goiás, Brazil.
Keywords: Cryptography, Network Management, PLC, BPL, SNMP.

Resumen

La disponibilidad de la red de telecomunicaciones es esencial para todas las empresas porque sus ingresos están directamente relacionados con él. Así, los sistemas de gestión de red también se convirtieran en esencial. Sin embargo la importancia dada a la gestión de información por la mayoría de los administradores de red, los demás la consideran como inútil. Por lo tanto, la garantía de la gestión de datos no es levada en cuenta. El principal objetivo de este artículo es mostrar la importancia de la gestión de la red de datos y estimular el uso de la seguridad en los sistemas de gestión de red. El buen desempeño de los sistemas de gestión de red es también importante. Por lo tanto, algunas pruebas se realizan para verificar con qué intensidad lo rendimiento de los sistemas de gestión y de la red puede verse perjudicado por el uso de la criptografía y algoritmos, especialmente por el estándar cifrado AES, a fin de estudiar la viabilidad de lo conjunto SNMPv3 con AES. Estas pruebas se toman como una vista previa de una banda ancha de lo proyecto piloto Power Line Network Management (que traducido al español vendría a ser Gestión de la Comunicación por la Red Eléctrica) que se llevará a cabo en la principal empresa de transmisión de la red eléctrica en Goiás, Brasil.
Palabras-clave: Criptografía, Gestión de Redes, PLC, BPL, SNMP.

1 INTRODUCTION AND MOTIVATION

There are a lot access technologies competing each other such as ADSL, PLC/BPL and wireless trying to deliver the best data transmission services to companies and end users, but companies depend more on the quality of these services because most of them, if not all, have their profit directly related to email, company-to-company integrated systems, e-commerce and so on.

To avoid unexpected and injurious situations, such as network devices downtime disabling Internet access or e-commerce web servers, a Network Management System (NMS) is indicated. A NMS permits a better network control such as detection of network traffic and overload, network device outage and security breaches. This control generates the possibility to take decisions before network problems come forward.

A NMS depends on the Network Management Protocol. In Section 2 the IP-based network management protocol named Simple Network Management Protocol (SNMP) is presented. The SNMP is a management protocol with three different useful versions: v1, v2c and v3. This article presents the basic differences between the SNMPv2c and SNMPv3 versions.

It is important to understand how a cryptographic algorithm works, specially Data Encryption Standard (DES) and Advanced Encryption Standard (AES) because these are the algorithms implemented in SNMPv3 and the objects of the tests performed, and this is the subject in Section 3.

To ease the network management tasks some Network Management softwares are available. The softwares used in the tests are presented in Section 4. Some free softwares are used to perform the network monitoring, requiring just a few configurations or scripts developments.

In Section 5 the article proposal is presented. Some performance tests are realized in order to bring up viability and security combination of SNMPv2c and several SNMPv3 possible implementations. Section 6 concludes this work.

This article was mainly motivated by a pilot project of Broadband Power Line (BPL) Network Management System that is being implemented in an electrical power transmission company in Brazil, in the state of Goiás. The BPL technology is calling attention as a new Broadband access solution especially for regions that are hardly reached by other technologies. A great number of companies implement network management systems without any security care. It is critical to understand that management data are not only important to the network manager, but also for possible attackers, which is the reason for implementing security and keeping management data confidential. Another motivation is some comparison tests taken in [1] between SNMPv2c and SNMPv3 before the SNMPv3 AES support.

2 THE SIMPLE NETWORK MANAGEMENT PROTOCOL AND ITS VERSIONS

A Network Management System is a set composed of Network Manager, Network Agents and Network Management Protocol. The Network Manager is a host target to collect or receive information from managed devices. The Network Agents are softwares implemented in the network devices that are intended to be managed and the Network Management Protocol is the protocol used to exchange information among managers and agents.

The two most well known and used management protocols are the OSI-based CMIP protocol and the TCP/IP-based SNMP [2] protocol. The Simple Network Management Protocol (SNMP) is a protocol used to manage IP-based network devices using a management database called MIB (Management Information Base) and by means of four basic SNMP operations [3]. *Get* is the operation where the manager queries the agent for specific information such as when it was booted for the last time or how many erroneous packets were received. *Set* is executed when the

manager wants do modify specific information in the agent. Not all information can be altered by *Set* operation. *Trap* is an asynchronous operation performed by the agents. It can be configured to send information to the manager in a specified time slot. The fourth operation is *Inform* (not implemented in SNMPv1, therefore this version does not support distributed management). It enables the manager-to-manager communication when distributed management is used. Each device can have unique objects/attributes because some information are specific to some kinds of devices. For instance, BPL devices probably have attributes in their MIBs related to Signal-Noise relation, which is not present in hosts MIBs.

SNMP *Get, Set and Trap* operations are implemented in all versions of SNMP (v1 [2], v2c [4] and v3 [5]) and *Inform* is implemented in versions v2c and v3. The main difference between SNMPv2c and SNMPv3 is the security issue, which is pretty slim in SNMPv2c.

SNMPv2c security is based on community authentication. Before the SNMP operations are executed using SNMPv2c the community authentication is required. This authentication is based on a pre-established string that is transmitted in plain text. As example, if the manager wants to perform a *Get* operation on a specific network router it must inform the community string as an authentication string. If that string is correct, then the agent answers the *Get* operation. This security method is a critical security breach because with a simple packet sniffer (software to capture data being transmitted over the bus) someone can discover the community name and perform operations.

A lot of network administrators consider monitoring data useless to others. On the other hand SNMP data can be most valuable for attackers. Using SNMP it is possible to discover the router of routing tables, which helps the attacker to map the whole network architecture, and, depending on the router's MIB configuration it is also possible to change the routing tables. Some attacks are based on the network device's uptime, information that can also obtained using SNMP. A lot of important information can be obtained or altered via SNMP, therefore it must be noticed that securing management data is indispensable.

The SNMPv3 brings real security implementation. It has a User Security Model (USM) [6] responsible for realizing authentication and data encryption. The authentication is performed by checking username and password. The informed password is hashed. There are two possible hashing algorithms: HMAC-MD5-96 and HMAC-SHA-96. Data encryption can be performed to prevent transmitted data to be captured in simple text, as it happens in SNMPv2c. DES and AES are the two possible encryption standards. These cryptographic algorithms are presented in Section 4.

There are three possible configurations for SNMPv3 involving security. *noAuthNoPriv* avoids authentication and encryption. *authNoPriv* obligates the authentication process but dismiss the encryption process, and *authPriv* forces the authentication and encryption process, which is the most secure method.

The SNMPv3 with AES support was standardized in RFC 3826 in 2004 [7] and since it is a relatively new Internet standard it is not commonly implemented in managed devices. Most network devices with SNMPv3 only support DES as privacy protocol.

3 PRIVACY ALGORITHMS

The Data Encryption Standard (DES) became an encryption standard in 1977. It was developed by IBM based on an algorithm called Lucifer [8].

DES receives a 64-length bitstring plaintext and uses a 56-length bitstring cryptographic key. It generates a 64-length bit string ciphertext. Basically, DES is based on permutation tables and exclusive-OR operations. If the input plaintext is bigger than eight bytes (sixty four bits), this bitstring is segmented on blocks of eight bytes ciphering each block at a time.

The permutation tables are used to swap the plaintext and key bitstring values. DES executes sixteen rounds of permutation and XOR operations, and after these rounds it executes one last

permutation, obtaining the ciphertext bitstring. The only arithmetic operation performed by DES is the XOR operation (this operation is executed in all sixteen rounds), which proves it great performance.

Four modes of operation have been developed for DES. *Electronic Codebook Mode* (ECB), *Cipher Feedback Mode* (CFB), *Cipher Block Chaining Mode* (CBC) and *Output Feedback Mode* (OFB). The SNMPv3 DES implements the CBC mode. CBC mode uses an Initialization Vector IV (y_0=vector IV) and xor it with the first input plaintext ($y_1=y_0 \oplus x_1$) before initiating the regular DES encryption method. Then, for the next plaintext bitstrings to be ciphered the previous ciphered text is used in the xor operation ($y_i=y_i\text{-}1 \oplus x_i$) [8], where y_0 means the initialization vector IV, y_1 is the first x-ored bitstring used as input for the first DES ciphering operation, x_1 is the first plaintext bitstring to be ciphered, y_i is the ith x-ored input bitstring and x_i is the ith plaintext bitstring. The last 64 bits from the secret key are used as the Initialization Vector.

Although SNMPv3 DES in CBC mode generates a dynamic security architecture due to the use of previous ciphered text and some SNMPv3 dynamic header fields (*EngineID* and *snmpGroupID* header fields are used to generate the private key, therefore they are used to generate the Initialization Vector [6]), it is still a cipher algorithm that uses a 56-bits key. The use of 56-bits key cipher algorithm means that there are 2^{56} possible ciphertexts for a specific plaintext. Due to DES short key length a lot of brute force attacks have been made against this algorithm and with the constant and exponential hardware development attacks began to come up with fast cracking results. According to [9], if is assumed that a cracker can perform one million decryptions per ms, a DES code would take about 10 hours to crack while a 128 bits code, such as Advanced Encryption Standard (AES) would take 10^{18} years (2^{128} possible combinations).

Because of the DES short key length issue, in 1997 NIST [10] (National Institute of Standards and Technology) called for proposals for a new encryption standard named Advanced Encryption Standard [11], which should have 128-bits block length and support 128, 192 and 256-bits keys lengths. The chosen algorithm was Rijndael [10].

In AES, the 128 bit plaintext is arranged as a square matrix of bytes. 128 bits equals 16 bytes, which is arranged as a matrix of 4x4. This matrix arrangement is copied into the so called State array, which is modified at each stage of encryption or decryption.

The key that is provided as input is expanded into an array of forty four 32-bit words. Four distinct words are used as round key for each round. Ten rounds are performed using substitution tables, permutation tables and xor arithmetic operation. After the last round, a 128-bit length ciphertext is generated.

The SNMPv3 AES mode is CFB. The difference between CFB and CBC (used by DES) is that before x-oring the plaintext bitstring with the previous ciphertext bitstring as performed in CBC, the previous ciphertext block is encrypted, and then the xor operation is performed. CFB might be represented as $y_i=x_i \oplus e(y_{i\text{-}1})$, where y_i is the output ciphertext, x_i is the input plaintext, *e* is the encryption function and $y_{i\text{-}1}$ is the previous ciphertext. The Initialization Vector has 128-bit length and is obtained as the concatenation of two 32-bit SNMPv3 header values (*snmpEngineBoots* and *snmpEngineTime*) and a local 64-bit integer.

4 NETWORK MANAGEMENT AND DATA CAPTURING SOFTWARES

A number of softwares have been designed to manage data networks. Some of them are free while others are not, such as the well-known HP OpenView [12]. This article proposes a NMS using only free softwares because of two reasons: they are free of license expenses and permit full software technology control. To perform the network management tasks the chosen softwares are Nagios and Net-SNMP. To reach the final results proposed in this article some data transmitted must be captured and this will be done using Wireshark.

Nagios [13] is a software designed to monitor network devices and services through external plugins (or scripts). There are a lot of plugins available on Internet to ease network administrator's job, but Nagios special feature is the possibility to design specific plugins and attach them to Nagios. The plugin can be designed in many different programming languages, such as C, C++, PERL, Python, Bash, Java or any other script-capable language.

Net-SNMP [14] is a free combination of the SNMP protocol, SNMP tools and most MIBs and is available for Linux, Unix and Microsoft Windows. This software implements the SNMP protocol and brings tools for exchanging SNMP data.

Wireshark [15] is a packet sniffing software. It uses a C library called pcap to capture data being transmitted over the bus and permits an easy-to-understand graphical analysis of the captured data, such as data transfer time and packet size. Wireshark will be used to collect information to be presented in test results.

5 PERFORMANCE VERIFICATION PROPOSAL

The proposal of the performed tests is to verify the performance and therefore the viability of four different security configurations of SNMPv3. All tests are done using the *authPriv* security method and the tested configurations are both possible HMAC authentication methods with both possible privacy methods. The SNMP configurations tested are 1) HMAC-MD5-96 authentication with DES encryption, 2) HMAC-MD5-96 authentication with AES encryption, 3) HMAC-SHA-96 authentication with DES encryption and 4) HMAC-SHA-96 with AES encryption.

The SNMP performance tests performed are not only intended to verify whether better encryption causes higher overload, but also to stimulate the use of SNMPv3 with AES encryption if possible. Despite the fact that security is a major factor, some manufacturers persist to develop equipment with only SNMPv2c implemented, and Broadband Power Line equipments are in this situation.

A network management system will be implemented and adapted using Nagios in a Broadband Power Line pilot project in Goiás, Brazil. All BPL network devices will be managed using SNMPv2c, but the results presented in this article may be used as important data if manufacturers start designing BPL devices with SNMPv3 support.

Broadband Power Line [16][17] is a broadband technology starting to grow especially because of its capability to reach geographically difficult places for inexpensive investments. BPL transmits data over power transmission lines and can be used for several purposes, such as Automatic Meter Reading (AMR), Internet connection, VoIP, LAN.

CELG [18] is one of the biggest electrical power transmission companies in Brazil and it started in February its pilot project of PLC/BPL Network Management named *Practical Management Model for Telecommunication Platform Involving PLC Technology*. Several PLC equipments are being acquired and the network management system is being implemented to manage the whole PLC network.

Although SNMPv2c performance results are described in this article, it must be emphasized that SNMPv2c should not be used, if possible, because of its lack of security. The main idea in the

article is to verify performance differences among the available security methods implemented in the SNMP User Security Model (USM).

Three tests are performed in order to track four characteristics: CPU usage, memory usage, size of transmitted packets and the transmission rate. The first test is done by monitoring characteristics during a *Get* operation, where the manager host retrieves from a managed host an attribute called *sysDescr.0*. The second test performs a similar operation, but not only one attribute value is retrieved, but a lot of them, precisely 207 attribute values. It is done by a sequence of *Get* operations, called *walk*. The third test performs a *Set* operation and the SNMP manager host changes an attribute called *sysContact.0* in the managed host. To obtain a more realistic result, each of these three tests is looped for a hundred times and during this loop the memory usage and CPU load characteristics are monitored and an average for each test and characteristic is obtained as a result.

The fourth and final test is performed by monitoring the Nagios server (SNMP manager) CPU load during a 15 minutes period for each of the four possible SNMP cryptographic configurations while it executes four different *Get* operations on five hosts. The idea of this test is to verify the burden generated on the manager when it has to obtain various information from various devices using authentication and cryptography seeking for more realistic practical results.

As illustrated in figure 1 the network architecture created for the tests is composed of six hosts. Their specifications are shown in table I.

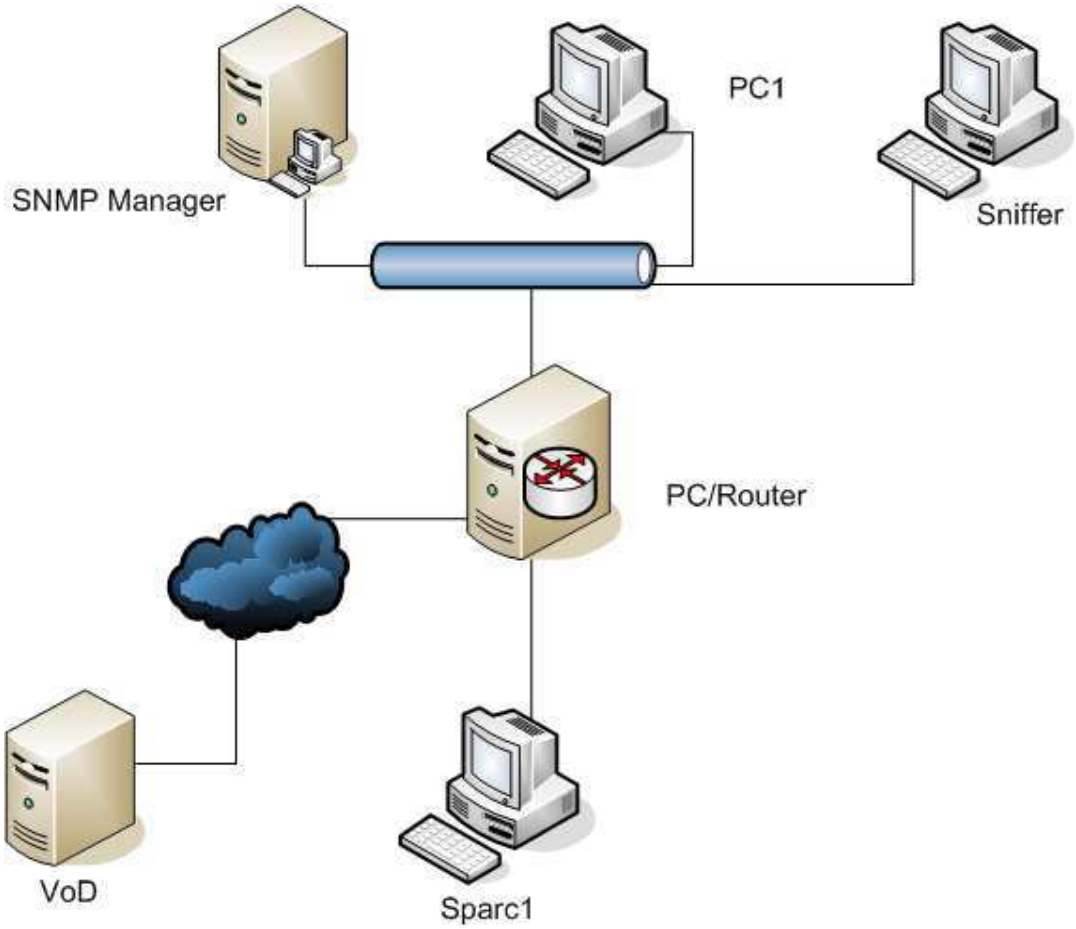

Figure 1: Network Architecture.

TABLE I
Managed Devices Specification.

	OS	CPU (MHz)	RAM (MB)
Manager	Linux	320	128
PC1	Windows XP	3000	512
Sniffer	Windows XP	3000	512
Router	Linux	3000	512
VoD Server	Linux	3000	3000
Sparc1	Linux	320	128

The SNMP Manager is a SPARC machine running Linux placed in the same network (10.0.3.0/255.255.255.0) of PC1 and Sniffer, which are both running Windows XP Professional. Sparc1, a SPARC machine running Linux, is placed in a logically separated network (192.168.15.0/255.255.255.0). The routing featuring is performed by the Router machine, which is also running Linux.

Net-SNMP has been installed, configured and initiated in five of the six hosts to allow SNMP operations. The Sniffer host was not configured as an SNMP agent. SNMPv2 has been configured to use the community name *telecom* with read and write permissions (otherwise the *Set* operation would not occur successfully). Four SNMPv3 users were configured, each one for a possible authentication and privacy combination. Write privilege is assumed to all users.

The first test involving performance and data rate was executed between the SNMP Manager and Sparc1 using *snmpget* command (from Net-SNMP package), followed by the second test that was performed using the *snmpwalk* command and the third test that was executed using the *snmpset* command. The management operations were performed between the Manager and Sparc1 because they are in logically separated networks although connected to the same backbone (router). This brings more realistic results considering that many managed devices may be hierarchically separated from the Manager, which might generate some latency. Three results are presented in tables II, III and IV.

Table I presents the *Get* operation results:

TABLE II
Get Operation Results.

	SNMPv2c	SNMPv3			
		MD5		SHA	
		DES	AES	DES	AES
Frames	2	4	4	4	4
Delay (ms)	0.75	3.7	3.7	4.1	3.9
CPU Usage (%)	24	38.1	41.6	47.1	27.2
Memory Usage (%)	1.8	1.8	1.8	1.8	1.8
Bytes Transmitted	249	703	703	693	696

It can be observed from table II that despite the fact that SNMPv2c generates pretty low CPU usage, SNMPv3 is a better solution because about 40% CPU usage on a 320MHz host would represent about 4% load for current server hosts. Also the packets transmitted are also very small because for both DES and AES algorithms the ciphertext block has the same or almost the same size of the plaintext block (bitstring completion might be needed). The biggest transmission (sent and received) is smaller than 1 kilobyte, which is smaller than most channel Maximum Transfer

Unit (MTU). The MTU represents the maximum data size the channel can transmit at a time. The Ethernet MTU, for instance, is 1540 bytes.

TABLE III
Walk Operation Results.

	SNMPv2c	**SNMPv3**			
		MD5		**SHA**	
		DES	**AES**	**DES**	**AES**
Frames	416	418	418	418	418
Delay (s)	0.42	0.70	0.70	0.74	0.73
CPU Usage (%)	24	54.5	54.3	58.8	57.6
Memory Usage (%)	1.8	1.8	1.8	1.8	1.8
Kilo Bytes Transmitted	37	77	78	79	80

Table III shows that SNMPv3 with AES is, in fact, the best solution. Even for a sequence of *Get* operations, the use of DES and AES generates almost the same CPU usage and data overload. One important characteristic to be observed from table III is the transmission delay. If observed the difference of transmission delay among SNMP implementations in table II (in percentage) with the delay among SNMP implementations in table III it comes clear that the encryption characteristic does not generate network overload. The SNMPv3 packets are bigger because of the SNMPv3 header fields, not the SNMP data itself. Using both privacy algorithms, the ciphertext block is the same or almost the same of the plaintext block.

Notice that an amount of 207 OID ciphered values has been retrieved in less than one second by *snmpwalk*, which can be considered an excellent performance.

Table IV presents *Set* operation results:

TABLE IV
Set Operation Results.

	SNMPv2c	**SNMPv3**			
		MD5		**SHA**	
		DES	**AES**	**DES**	**AES**
Frames	2	4	4	4	4
Delay (ms)	6.6	9.3	9.4	9.6	9.7
CPU Usage (%)	18.1	38.8	39.8	42	42
Memory Usage (%)	1.66	1.73	1.74	1.8	1.8
Bytes Transmitted	182	626	636	624	626

Table IV presents similar results to the *Get* operation with lower CPU usage. The SNMPv2c reached the best results because it has got no security implemented. The authentication is realized by informing a simple string that is transmitted in plain text and the management data is transmitted also in plaintext. The SNMPv3 security implementations present similar results when performance is considered, but when security is weighted, the use of AES as privacy algorithm is the best option, due to DES limited key length.

For the fourth test Nagios has been configured to perform *Get* operations on hosts Sparc1, Router, VoD, PC1 and itself. For each managed host it was decided to retrieve four OIDs values: *tcpInErr.0, snmpInErrors.0, snmpOutErrors.0* and *ifInErrors.0.* But Nagios cannot manage devices using SNMP by itself. To realize SNMP tasks it is necessary to download or create Nagios external

plugins. A few plugins are available in [19], which is the official Nagios plugins repository, but the SNMP available plugins were designed to search for specific information (attributes) or only to perform DES cryptography. Since Nagios is a software designed initially to manage computer networks only, the SNMP plugins are normally designed to manage computers or computer network equipments such as routers.

This article also proposes a NMS capable of managing IP-based networks using Nagios, therefore a generic Nagios SNMP plugin with AES support was designed. It is a shell script that runs the *snmpget* command (included in Net-SNMP software) on any SNMP agent retrieving any SNMP object value. The script also receives limiting values to judge if the obtained value is in normal, warning or critical condition. This plugin is ideal for a generic SNMP network management because it does not depend on the network technology. Some OIDs are specific for computer network equipments, while others are specific for BPL equipments such as signal-noise relation, so it is only necessary to specify the desired OID to be retrieved. Also the plugin allow the administrator to inform which SNMP version and which privacy algorithm (if needed) Nagios must use to perform the *Get* operation. Although SNMPv3 should be used, some devices do not have the third version of SNMP implemented yet, therefore the plugin can be configured to use SNMPv2c.

The generic SNMP plugin must receive some parameters. If the SNMP version to be used is v2c then it must receive a community name. If the SNMP version to be used is v3 then the administrator must pass six additional parameters: the security model (*noAuthNoPriv*, *authNoPriv* or *authPriv*), the authentication user, the authentication method (MD5 or SHA), the authentication password, the privacy algorithm (DES or AES) and the privacy password. The privacy password is used by DES to generate the Initialization Vector. For both SNMP versions two other parameters are required, the hostname or IP address of the device to be managed and the OID to be consulted.

For instance, if the desired object to be retrieved is *tcpInErrs.0*, which represents how many erroneous TCP segments the managed device has received, the command /path/snmp.sh -v 3 -l authPriv -u secure –a SHA -A password -x AES -X password -H 10.0.3.1 -o tcpInErrs.0 -W 10 -C 20$ must be used. In this case the command represents SNMP version 3, security model authPriv, secure as user, SHA as authentication method, password as the authentication password, AES as the encryption algorithm, password as the privacy password, 10.0.3.1 as the host to be managed, tcpInErrs.0 as the target OID, 10 as the default value, between 10 and 20 as a warning value and above 20 as a critical value, respectively. The command response could be "OK - Normal Value: 0", "WARNING - Value above expected: 15" or "CRITICAL - Very High Value: 30".

Nagios was configured to perform 20 *Get* operations (4 *gets* on each agent) per minute during 15 minutes. All four cryptographic configurations have been monitored for fifteen minutes, but only the first minute is graphically represented. First configuration was using SNMPv2c, followed by SNMPv3 with MD5 authentication and DES encryption, SNMPv3 with MD5 authentication and AES encryption, SNMPv3 with SHA authentication and DES encryption and SNMPv3 with SHA authentication and AES encryption. The graphical representation of the CPU usage results is illustrated in figure 2. Also the HMAC-MD5 authentication is not presented because SHA is recommended to be used for security reason and the results show that MD5 brings no performance improvement over SHA. Basically the graphic represents a comparison of CPU usage among SNMPv2c, SNMPv3 HMAC-SHA-96 authentication with DES encryption and SNMPv3 HMAC-SHA-96 authentication with AES encryption.

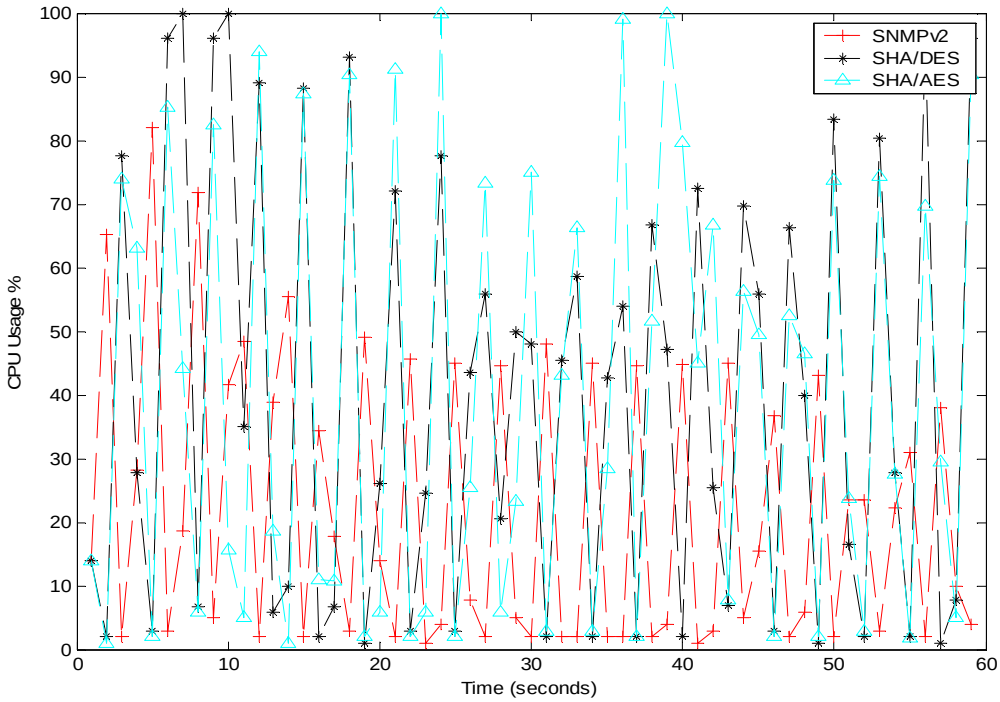

Figure 2: CPU Usage.

The CPU usage increased if compared to the SNMP operation tables. This increasing was caused by Nagios. But the important information to extract from figure 2 is that DES and AES cause the same impact on CPU load. During the SNMP generic plugin execution, another script was running to capture packets sent and received by the manager to generate a graphical representation of network load, which is represented in figure 3.

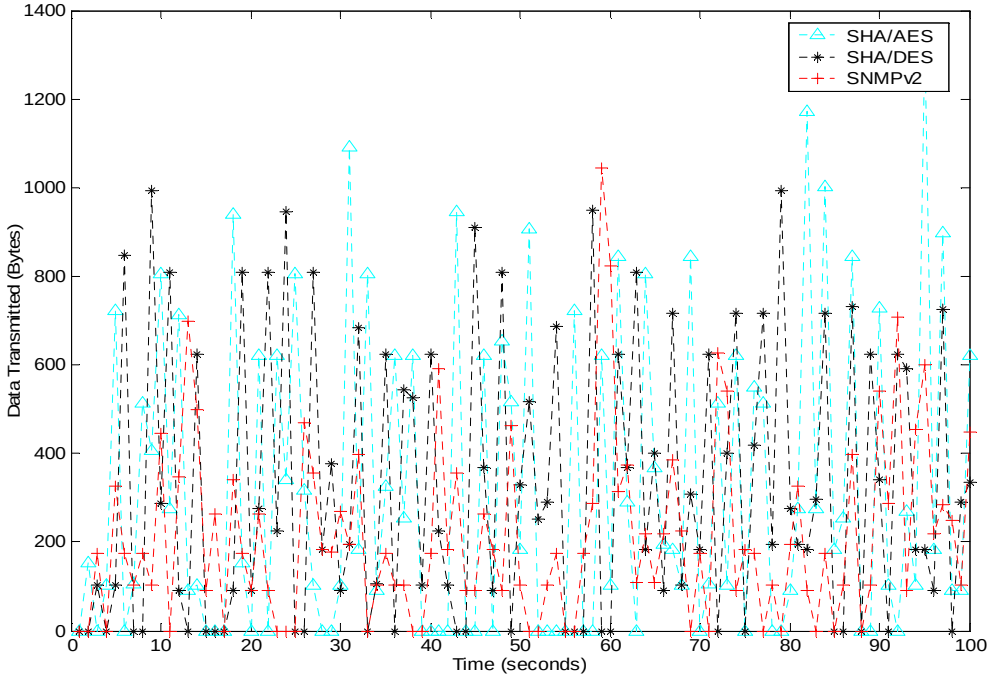

Figure 3: Network Load.

As it can be observed in Figure 3, using SNMPv3 with AES is the best solution because AES does not cause network traffic. The generated network traffic is due to the SNMPv3 header. Based on theoretical issues and on tests results, it is strongly recommended to use SNMP version 3 in combination with AES encryption, if possible. Most network devices bring SNMP support, but it is common to find these devices with SNMPv1 and SNMPv2c support only. Most recent designed devices bring SNMPv3 support, but still, most of them support DES encryption. Probably due to the fact that SNMP AES support is a relatively recent standard, manufacturers are only now starting to design devices with SNMP/AES support, but it is not a commonly spread practice. Most recently designed routers and switches bring this possibility, but in the BPL area it does not happen. It is expected that this scenario changes in short period.

5 CONCLUSIONS

The advance of data transmission technology generates a great deal of complexity, considering the coexistence of heterogeneous devices from different technologies and different manufacturers. This complexity must be properly managed otherwise outages, leakages, errors and security breaches might probably come up.

In order to manage data networks a number of network management softwares have been designed based on the SNMP protocol. Despite the effort of the Internet Working Group to keep improving SNMP, administrators and manufacturers continue to implement and configure network management systems based on the second version of this protocol, which has critical security flaws.

The tests presented in this paper show that the use of SNMP version 3 with security characteristics such as authentication and privacy, specially using AES encryption, turns to be a great option and must be encouraged because some very important and critical information may be transmitted, and it cannot occur in plaintext. Also, the load generated on the network is meaningless and the CPU load caused by encryption is too little for current processing units capability since the only arithmetic operation performed is the XOR operation.

The tests show that some CPU usage peaks happen, but it must be noticed that the Manager host is an old UltraSparcII with 320 MHz clock and 128 MB of RAM, a pretty out-of-date machine when compared to actual servers solutions with dual/quadruple processing.

From the results obtained it comes clear that managing a complex data network with free softwares and the SNMP protocol does not generate network overload. The network usage during SNMP operations, despite the possibility to manage several network elements and several OIDs concurrently, is very low. Each SNMP *Get* operation generates a data flow of approximately 700 bytes, which is less than most MTU channels, therefore no fragmentation is necessary.

For CELG pilot project of BPL network management, these results demonstrate that once the access to MIB devices are reached, the presented NMS using the developed plugin will ease the management of the heterogeneous devices, since equipments from different manufacturers with different SNMP implementations will coexist. This paper also presents a perspective of how the BPL network will be impacted if future BPL devices bring SNMPv3 support.

REFERENCES

[1] Corrente A. and Tura L. Security Performance Analysis of SNMPv3 with Respect toSNMPv2c. *Network Operations and Management Symposium, 2004*. IEEE/FIP. 23: 829-742. April 2004.

[2] Network Working Group. RFC 1157 - Simple Network Management Protocol (SNMP). *The Internet Engineering Task Force*. May 1990

[3] Stallings W. SNMPv3: A Security Enhancement for SNMP. *IEEE Communications Surveys*. 1998. Vol.1 No. 1. Fourth Quarter 1998.

[4] Network Working Group. RFC 1901 - Introduction to Community-based SNMPv2. *The Internet Engineering Task Force.* January 1996.

[5] Network Working Group. RFC 2570 - Introduction to Version 3 of the Internet-standard Network Management Framework. *The Internet Engineering Task Force.* April 1999.

[6] Network Working Group. RFC 2574 – User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3). *The Internet Engineering Task Force*. April 1999.

[7] Network Working Group. *RFC 3826* - The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model. *The Internet Engineering Task Force*. June 2004.

[9] W. Stallings. Network Security Essentials. 2nd Edition. Prentice Hall. 2003.

[10] National Institute of Standards and Technology. Available at http://www.nist.gov. Visited in July 14, 2008.

[11] FIPS Publication 197. Announcing the Advanced Encryption Standard (AES). Available at http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Visited in July 14, 2008.

[8] B. Schneier. Applied Cryptography. 2nd Edition. John Wiley & Sons. 1996.

[9] J. McCaffrey. Keep Your Data Secure with the New Advanced Encryption Standard. Microsoft MSN. 2003.

[10] B. Schneier and D. Whiting. A Performance Comparison of the Five AES Finalists. Third AES Candidate Conference. 2000.

[12] HP OpenView. Available at http://www.hp.com. Visited in April 20, 2008.

[13] Nagios. Available at http://www.nagios.org. Visited in April 20, 2008.

[14] Net-SNMP. Available at http://net-snmp.sourceforge.net. Visited in April 20, 2008.

[15] Wireshark. Available at http://www.wireshark.org. Visited in April 20, 2008.

[16] OPERA. Available at http://www.ist-opera.org. Visited in April 20, 2008.

[17] PLC. Available at http://pt.wikipedia.org/wiki/PLC. Visited in April 20, 2008.

[18] CELG PLC. Available at http://www.celg.com.br. Visited in April 20, 2008.

[19] Nagios Exchange. Available at http:://www.nagiosexchange.org. Visited in April 20, 2008.

[20] J. Lee, C. Hong, J. Kang and J. Hong. Power Line Communication Network Trial and Management in Korea. *International Journal of Network Management*. 16(6): 443-447. November 2006.