

# SURVEY ON SNMP IN NEXT GENERATION NETWORK

Liu Yan, Yin Xia, Wu Jianping

Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Key words: network management, SNMP security access control

Abstract: Network management is a process to control networks with great efficiency. So far, network management protocols have changed from SNMPv1, SNMPv2 to SNMPv3. This paper briefly compares and analyses these versions on SMI & MIB, protocol operation, security and access control. Besides, it thoroughly summarizes most research aspects of recent SNMP developments, especially the next generation network and new technologies. It also analyses and points out the most promising aspects.

## 1 SNMP'S DEVELOPMENT AND HISTORY

With networks' growing popularity in recent years, network management has become more and more difficult and important. In order to effectively manage all kinds of networks and instruments, IAB published the first SNMP (simple network management protocol) in August 1988.

However, SNMPv1 contains several flaws. IAB published a group of standard MIB managed objects called RMON in November 1991. Moreover, in order to strengthen security in SNMPv1, IAB introduced SNMPsec in July 1992. Based on both the RMON and SNMPsec, SMP was put forward and used as a foundation for SNMP version 2.

SNMPv2, published in 1993, makes great progress in distributed network management, data types, ability to deal with malfunctions, compared with SNMPv1. Yet SNMPv2's security performance hasn't been improved significantly. Therefore, SNMPv2u, SNMPv2p and SNMPv2\* were developed under the demands of equipment providers. In order to unify all the versions, IETF published SNMPv2c in 1996, which is a modified version based on SNMPv2, and focuses on functional improvement.

IETF SNMPv3 group released RFC2271-2275 in January 1998, which is SNMPv3. SNMPv3 includes all the functions and frameworks which are implemented in both SNMPv1 and SNMPv2.

Besides, SNMPv3 defines new security characters such as identification and encryption.

## 2 SNMP'S COMPARISON AND ANALYSIS

There are several aspects included in SNMP:

- SMI & MIB
- Management operation
- Security and access control

During SNMP's major versions' developments, three aspects above have been modified and improved continuously. The following parts will tersely discuss and compare the major versions of SNMP separately in three aspects through tables.

### 2.1 SMI and MIB

SMI has two versions. It defines **data types and data structures** used in network management elements; and **clauses** used to regulate logical structure and format in MIB and **management objects**. MIB also has two versions. It uses the data structures defined in SMI to manage all the **network information** and add necessary new MIBs in order to meet the needs of different SNMP versions.

Table 1 compares differences in SMI & MIB among three major versions of SNMP.

### 2.2 Protocol Operation

Because some SNMP versions, such as SNMPv2, SNMPv2p and SNMPv2\*, have made little improvements in management functions and operations, table 2 mainly compares SNMPv1, SNMPv2c and SNMPv3 in protocol operations, including **types and formats of PDUs**, which are

used to transport management information, and different **management frameworks** adopted in three versions.

### 2.3 Security and Access Control

Besides improvement in management function and efficiency, security is also a very important aspect. Table 3 shows different **security models and methods** used in seven major SNMP versions; It

also analyzes **advantages and disadvantages** of these models and methods.

There are several concepts need to be explained. In the community-based model, every community has only one special name used for identity authentication. In the party-based model, every management entity exchanges messages using parties, which can give different access authorities to different objects. In the user-based model, every user has its own key and access authority. The View-based model combines users with MIB view in order to achieve access control.

Table 1: SNMP's SMI & MIB comparison table

		SNMPv1	SNMPv2	SNMPv3
SMI	<b>SMI version</b>	SMIv1	SMIv2	
	<b>Related RFC</b>	RFC1155 RFC1212 RFC1215	RFC2578-2580	
	<b>Data type</b>	Primitive Types (including INTEGER, OCTET, STRING, OBJECT IDENTIFIER and NULL) Constructor Types Defined Types (including Network Address, IP Address, Time Ticks, Gauge32, Counter32 and Opaque)	1 Primitive Types: changes INTEGER to Integer32; 2 Defined Types: adds new Counter64; require counters without default value; counters can be read only.	The same as SNMPv2
	<b>Clause definition</b>	Defines 7 clauses: SYNTAX, ACCESS, STATUS, REFERENCE, DESCRIPTION, INDEX, DEFVAL	1 Adds AUGMENTS and UNITS clause; 2 MAX-ACCESS clause replaces ACCESS; 3 Changes some options in STATUS clause.	
	<b>Data structure</b>	Uses SEQUENCE and SEQUENCE OF to construct simple two-dimension table for scalar quantities, which is the only table type provided in SMIv1.	1 Changes value option in RowStatus clause in order to delete, add or suspend lines; 2 Adds AUGMENTS clause in order to expand lines easily.	
<b>MIB version</b>	MIB-II	MIB-II	MIB-II	
<b>Related RFC</b>	RFC1213	RFC1451 RFC1573	RFC3411-3415	
MIB	<b>Improve-ment</b>	Defines 171 variables to store all the information, which are divided into 10 groups: System, interface, Address Translation, IP, ICMP, TCP, UDP, EGP, DOT3, SNMP	1 Modifies Interfaces group, add 4 new tables; 2 Adds Manager-to-Manager MIB for new PDU called inform.	Adds 7 new MIBs: snmpFrameworkMIB snmpMPDMIB snmpProxyMIB snmpNotificationMIB snmpTargetMIB snmpUsmMIB snmpVacmMIB

Table 2: SNMP’s management operations comparison table

	SNMPv1	SNMPv2c	SNMPv3
RFC	RFC1157	RFC1901 – 1906	RFC2570-2573
<b>PDU Type</b>	<ol style="list-style-type: none"> <li>1 GetRequest</li> <li>2 GetNextRequest</li> <li>3 SetRequest</li> <li>4 GetResponse</li> <li>5 Trap</li> </ol>	<ol style="list-style-type: none"> <li>1 Adds new GetBulk to improve table’s transportation;</li> <li>2 Adds new Inform to implement communication between managers;</li> <li>3 Improves Get’s efficiency.</li> </ol>	<ol style="list-style-type: none"> <li>1 Improves GetBulk’s efficiency;</li> <li>2 Adds check function to assure Set executed successfully.</li> </ol>
<b>PDU Format</b>	Has two different formats: the format of Trap is different from that of Get and Set.	Unifies format of PDUs in order to improve efficiency to send and receive PDUs.	Adds new security elements in PDU, including authentication and authorization information, in order to strengthen security.
<b>Management framework</b>	Implements centralized management with low efficiency and stiff frameworks.	Implements distributed management which implements communication among managers and is more efficiency.	<ol style="list-style-type: none"> <li>1. Implements distributed management which unifies manager and agent as entity;</li> <li>2. Compatible with version 1,2;</li> <li>3. Provides flexible extension.</li> </ol>

Table 3: SNMP’s security and access control comparison table

Version	Security Model	Security Method	Security Analysis merit-regular demerit-bold
SNMPv1	Community-based model	<ol style="list-style-type: none"> <li>1 Transports community’s name in ASCII</li> <li>2 Provides basic authentication</li> </ol>	A Community’s name which is used in some SNMP agent is easily recognized, thus SNMPv1 cannot provide effective protect against attacks theoretically.
SNMPsec	Party-based model <i>This version develops from SNMPv1.</i>	<ol style="list-style-type: none"> <li>1 Uses MD5 algorithm to authenticate;</li> <li>2 Uses DES algorithm to encrypt;</li> <li>3 Adds timestamp;</li> <li>4 Every SNMP party has a MIB view, which defines all the objects the party learns.</li> </ol>	<ol style="list-style-type: none"> <li>1 MD5 algorithm provides authentication for integrity and origin of message received;</li> <li>2 DES algorithm provides protection to prevent message’s divulging in transport;</li> <li>3 Timestamp assures that messages transported are in time and provides related time synchronizer;</li> <li>4 Party can control access to objects in MIB view depending on request from other parties far away SNMPsec is not implemented.</li> </ol>
SNMPv2p	Party-based model <i>This version develops from SNMPsec.</i>	<ol style="list-style-type: none"> <li>1. Simplifies synchronizer in SNMPsec;</li> <li>2 Adds a context parameter in message in order to implement access control.</li> </ol>	<ol style="list-style-type: none"> <li>1. DES algorithm in SNMPv2p greatly increases calculation burden;</li> <li>2. Implementing party needs too much complex configuration even for a simple function.</li> </ol> <p>According to the reasons above, SNMPv2p is not implemented finally.</p>
SNMPv2c	Community-based model <i>This version develops from SNMPv1.</i>	The same as SNMPv1	The same as SNMPv1
SNMPv2u	Party-based model <i>This version develops from SNMPv2p.</i>	<ol style="list-style-type: none"> <li>1. Uses Keyed-MD5 algorithm with 128-bit keys;</li> <li>2. Uses request-id and time instructor to manage agents;</li> <li>3. Uses DES-CBC;</li> <li>4. Allows multi-management model in</li> </ol>	<ol style="list-style-type: none"> <li>1. Keyed-MD5 algorithm provides authentication for identity and data integrity;</li> <li>2. Prevents message delay and repeated attacks;</li> <li>3. Uses DES-CBC algorithm to encrypt;</li> <li>4. Prevents disguise, message change, message divulging;</li> <li>5. Easy to be implemented and</li> </ol>

		order to accept new security protocols.	comprehended.
<b>SNMPv2*</b>	Party-based model <i>This version develops from SNMPv2u.</i>	1 Similar to SNMPv2u in security; 2 Has more single management model than multi-model in SNMPv2u.	Too complex to be implemented
<b>SNMPv3</b>	User-based & View-based model <i>This version develops from SNMPv2* and SNMPv2u.</i>	1. Uses HMAC-MD5-96 and HMAC-SHA-96 as authentication algorithm <sup>1</sup> ; 2. Uses DES-CBC; 3. Introduces local key concept.	1 Every user key's divulging will not effect each other's security; 2 Improves security function through intensifying encryption and authentication; 3 Introduces view-based control model to control access.

### 3 SUMMARY OF SNMP RESEARCH

The research areas of SNMP are so wide that they include not only improvements in functions and security models for SNMP itself, but also a lot of new technologies and test systems based on SNMP. All of these research fields, which are divided into several aspects, will be thoroughly discussed later.

#### 3.1 Research Focused on SNMP

Research in SNMP mainly focuses on SMI & MIB, management framework and security mechanism, which have been discussed above.

Currently the research of SMI and MIB focuses on efficiency of browsing and transporting MIB tables, and flexibly extending MIB without too much restrictions and complexity.

Because of the development of management framework, distributed network management has become necessary, especially for overcoming centralized NMS's limitations such as scalability and inefficient use of network resources. Distributed network management systems, based on SNMP, mainly care about how to implement and how to balance loads among different managers.

In SNMP security protocols, most security algorithms are too complex to put into use. At the same time, the protection function also needs to be intensified.

Table 4 analyzes the main research aspects in three areas above, including not only the problems we face, but also the newest solutions:

Table 4: Research focused on SNMP

Research areas	Problems need to be solved	Methods to solve the problems
<b>Research based on SMI &amp; MIB</b>	1.How to browse MIB tables fast.	Proposes a GetPrev, which enables the retrieval of the previous instances of columnar objects or scalar MIB objects and uses only standard SNMP GetNext and Get requests to carry on a fast and bandwidth efficient search for the required object instance.
	2.How to improve efficiency of transporting data in MIB tables.	Proposes a GetModify mechanism, which is a tool that substantially reduces bulk transfers of dynamic, large MIB tables by transferring changed data only during polling intervals from SNMP agents .
	3.How to implement dynamic SNMP SMI & MIB extension.	Implements a exchangeable interface between MIB and entities which will simplify dynamic addition and deletion of MIB tables. Proposes a network management toolkit which uses XML and the Document Object Model (DOM) to specify a MIB at runtime and allows the MIB structure to be serialized and shipped over the network between managers and agents. Discusses the concept of a custom screens builder for network elements management and proposes XML-based templates employing a few simple but flexible constructs that significantly

		augment the SMI and MIBs definitions.
	4.How to extend MIBs under the distributed management environment.	Proposes a Script MIB extension with new objects able to control the usage of specific resources (physical memory, processing cycles, among others) for each script launched inside the distributed environment. Uses expressions to perform decentralized processing of management information called the Expression MIB.
<b>Distributed network management framework based on SNMP</b>	1.How to implement distributed management in SNMP.	Proposes multiple SNMP agents running a Hi-ADSD with Timestamps, a Hierarchical Distributed System-Level Diagnosis algorithm with Timestamps, monitor themselves and a configurable set of network services and devices, issuing controlling commands depending on the results. Proposes a new model Meta-Management of dynamic Distributed network managers (MEMAD) which enable Peered Distributed Managers to manage the network by executing delegated or predetermined common management tasks. Presents a new clustering architecture for SNMP agents that supports semi-active replication of managed objects.
	2.How to balance dynamic load among managers.	Proposes a new dynamic load balancing method and decides execute management programs dynamically based on CPU utilization for each system and the bandwidth required for executing all management programs.
<b>SNMP Security Research</b>	1.How to simplify security algorithm in SNMP.	Proposes a new security algorithm called Application Secure SNMP, which requires less resources and can be patched into devices more easily compared to SNMPv3 by finishing authentication via AAR value and providing an in-built intrusion detection mechanism.
	2.How to intensify SNMP security protection.	Proposes a policy-based SNMP security management architecture using XML to deal with the access, service refusal, or unstable action in which SNMPv3 is inefficient.
		Addresses the provisioning of a security “continuum” for management frameworks based on XML/SNMP gateways and provides an in depth security extension of the gateway using the Role Based Access Control paradigm, which is integrated within a broader XML-based management framework.
		Proposes a new security model named Role-based Security Model (RSM) with security management policy, to support scalable and centralized security management for SNMP-based networks.
	Explains how Aglets, a Java open-source MA framework, not a proprietary system, can be used for security-enhanced network management and complementing the security of the Simple Network Management Protocol (SNMP) version 3.	

### 3.2 Network Test System Based on SNMP

Basically, SNMP defines a relationship between managed devices and management applications, and how information has to be structured. Compared to other approaches, its main advantages are a simple structure, a low memory footprint and resource consumption, which make it easy to develop and deploy. That is why SNMP is used to test network

parameters and performance in a number of fields. It attracts many papers to evaluate the tests made by SNMP systems.

Besides, to overcome the limitation of areas SNMP system covers, people add necessary components and mechanism into SNMP system in order to meet different needs of all kinds of tests.

Table 5 shows both changes made in SNMP systems to test special objects and evaluations about SNMP test systems:

Table 5: Network test system based on SNMP

Research areas	Problems need to be solved	Methods to solve the problems
<b>Monitor system Based on SNMP</b>	1.How to inspect and detect intrusion.	Describes attack signatures that should be monitored by using a state machine-based language called PTSL (Protocol Trace Specification Language). Proposes a methodology for the early detection of Distributed Denial of Service (DDoS) attacks; and examines the applicability of Proactive Intrusion Detection.
	2.How to detect and monitor network fault.	Improves the accuracy of remote fault diagnoses by using an effective method of fault inference called a 'run-test', taking advantage of the active moving and sensing ability of autonomous mobile robots. Presents the design and evaluation of a SNMP-based distributed network fault detection/monitoring system. This system involves the integration of recently developed ML-ADSD algorithm for diagnosis of faults in a distributed system of processors into the SNMP framework.
	3.How to monitor multicast.	Presents a framework (SMRM) for monitoring the health and the quality of multicast delivery paths (or forwarding tree) at real-time. This framework combines distributed monitoring and centralized control by using SNMP as a core component.
<b>SNMP system Evaluation</b>	1.How to evaluate network performance measurement made by SNMP.	Evaluates the feasibility, validity of network performance measurement based on SNMP, and the advantages of acquiring network performance measurement data based on SNMP.
	2.How to evaluate network traffic anomalies detected by SNMP and other test systems.	Compares the traffic anomaly signals detected in SNMP and IP flow data; and shows that more coarse-grained SNMP data can also be used to expose anomalies effectively.
	3.How to evaluate interface test systems based on SNMP.	Shows properties of SNMP network management interface testing, basic testing method and key contents of the testing based on analysis of SNMP network management interface.
	4.How to evaluate backbone internet traffic tests based on SNMP.	Uses SNMP traffic data covering an entire Tier 1 ISP backbone for more than one year to address the question of how backbone network traffic should be modeled. The limitations of SNMP measurements do not permit to comment on the fine timescale behavior of the traffic.
	5.How to evaluate distributed network tests based on SNMP.	Implements a distributed diagnosis tool by using MIB. The tool assumes that a fault-free agent running a previously defined test is able to correctly determine the state of the tested entity.

### 3.3 SNMP Used into New Generation Network

Admittedly, most of the existing network management applications are based on SNMP protocol. However, because networks evolve rapidly and newer protocols keep emerging, for example, wireless mobile networks, IPv6 and active networks, it has become more and more challenging to monitor and manage the new generation networks. How to use SNMP in these new kinds of networks needs enough attention and immediate solutions.

Because of wireless networks' low bandwidth, high delay and mobility, traditional SNMP, which is characterized by their centralization, lack of scalability, complexity to configure and not strong local processing ability, is inappropriate. Therefore, modifying SNMP for mobile agents has been proposed as a solution to the problems.

When SNMP is transferred from IPv4 to IPv6, there are several problems need to solve, such as what parts should be modified for IPv6, or whether SNMP in IPv6 can perform as well as in IPv4.

Table 6 shows SNMP used in new generation networks:

Table 6: SNMP used into new generation networks

Research areas	Problems need to be solved	Methods to solve the problems
SNMP used in wireless network	1.How to implement dynamic distributed management in wireless networks.	Proposes a model consisting of a base station manager (BS), a SNMP agent, and a user-friendly graphic user interface (GUI). The manager-to-SNMP agent communicates through a mechanism based on the extensible SNMP trap feature. Records and refreshes the effective network topology by a discovery process. By mixing collected information at each sub-network, an itinerary can be obtained which spans the whole administrative domain.
	2.How to efficiently utilize limited bandwidth in wireless networks.	Researches "serial" and "concurrent" SNMP, investigates the behavior of Wireless SNMP in different scenarios, and specifies particular wireless channel state conditions (good/bad) and background traffic loads.
	3.How to manage wireless networks with unstable connections.	Describes problems caused by simplicity of the information model used by SNMP in low-rate networks; and provides the solution through which the problems are overcome by actively discovering new node and continuously monitoring message changes.
	4.How to implement a mobile agent based on SNMP.	Designs a wireless network management protocol based on SNMP, in order to support fault management and use mobile agents to detect, diagnose and recover from faults in wireless and mobile networks. Presents a solution to extend an existing legacy network management framework targeted at network management with an interface for integration with mobile agents; and implements it by using Java technology and aglet which is a mobile agent system from IBM.
SNMP used in IPv6	1.Which aspects need to be changed.	Firstly changes transport mapping from SNMP-over-UDP-over-IPv4 to SNMP-over-UDP-over-IPv6 by modifying the parameter values in netsnmp_transport structures; Secondly adds some MIBs IPv6 needs, by using some functions to increase MIB variables and modify the objects in PDU, or by unifying address structure and differentiating special functions used in IPv4 and IPv6.
	2.How to evaluate the performance of SNMP in IPv6.	Analyzes the effect on the number of SNMP PDUs and MIB information when IPv6 messages with different header lengths are transported; and considers SNMP delay and bandwidth in IPv6.

#### 4 CONCLUSION

This paper summarizes both SNMP protocols' development and research directions. Firstly, it compares the main SNMP versions in SMI & MIB, protocol operations and security. Secondly, it thoroughly analyzes all the research areas based on SNMP and divides them into four main aspects, especially about the new generation networks and technologies. Aside from the existing research areas, the paper also provides other original SNMP research fields, which are worth consideration. Now SNMP, which still has some defects, needs further research and improvement.

#### REFERENCES

Hu xuekun Xiong Yan Miao Fuyou Jan 2004, Distributed network management in Mobile IP mini-micro systems (in Chinese) (journal)

You-Sun Hwang, Eung-Bae Kim, 2003. The management of the broadband wireless access system with SNMP Korea Electron. & Telecommun. Res. Inst., Daejeon, South Korea Telecommunications, ICT 2003:122~132(journal)

Kantorovitch J, Mahonen P, 2002, Case studies and experiments of SNMP in wireless networks IEEE WORKSHOP ON IP OPERATIONS AND MANAGEMENT 2002:179-183(journal)

Reuter E, Baude F, 2002, A mobile-agent and SNMP based management platform built with the Java ProActive library IEEE WORKSHOP ON IP OPERATIONS AND MANAGEMENT 2002:140-145(journal)

- Zhang, Puhan, Sun, Yufang. April, 2003. A method for interaction of mobile agent and SNMP, Chinese Journal of Electronics, v 12, n 2, April, 2003:p 283-286(journal)
- Malowidzki, Marek, 2001, The management of the mobile network with COM+ and SNMP Proceedings - IEEE Military Communications Conference MILCOM, v 2, 2001: p 1456-1460(conference)
- Gaspary LP, Meneghetti E, Throuco LR, 2003, An SNMP agent for stateful intrusion inspection INTEGRATED NETWORK MANAGEMENT VIII - MANAGING IT ALL INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING, 118, 2003:3-16(journal)
- Su MS, Thulasiraman K, Das A. 2002, A scalable on-line multilevel distributed network fault detection/monitoring system based on the SNMP protocol GLOBECOM'02: IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, VOLS 1-3, CONFERENCE RECORDS - THE WORLD CONVERGES 2002:1960-1964(conference)
- Yan T, Ota J, Nakamura A, Arai T, 2002, Development of a remote fault diagnosis system applicable to autonomous mobile robots ADVANCED ROBOTICS 16 (7) 2002: 573-594(journal)
- Al-Shaer, Ehab, Tang Yongning, 2002, SMRM: SNMP-based multicast reachability monitoring IEEE Symposium Record on Network Operations and Management Symposium, 2002:467-482(conference)
- Hossen, M.J. Ramli, A.R. Abdullah, M.K. 2003, Web-based network device management using SNMP servlet Multimedia & Imaging Syst. Lab., Universiti Putra Malaysia, Selangor, Malaysia Telecommunication Technology, Jan. 2003:145-152(journal)
- Breitgand David, Raz Danny, 2002, SNMP GetPrev: An efficient way to browse large MIB tables, IEEE Journal on Selected Areas in Communications, v 20, n 4, May, 2002: 656-667(journal)
- Park SH, Park MS, 2003, An efficient transmission for large MIB tables in polling-based SNMP ICT'2003: 10TH INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS, 2003:246-252(conference)
- Lanbo, Yangqin, 2004, Design and Implementation of Dynamic Extended MIB Based on SNMP, Computer Engineering, April 2004 :45-53(journal)
- Malowidzki M, 2002, Custom screens builder for SNMP MIBs 2002 IEEE WORKSHOP ON IP OPERATIONS AND MANAGEMENT 2002:80-84(journal)
- Shufen Liu, Lu Han, Xinjia Zhang, 2004, Study of network performance measurement based on SNMP, Computer Supported Cooperative Work in Design, 2004. Proceedings. The 8th International Conference on 26-28 May 2004:224-230(conference)
- Barford P, Kline J, Plonka D, 2002, A signal analysis of network traffic anomalies IMW 2002: PROCEEDINGS OF THE SECOND INTERNET MEASUREMENT WORKSHOP 2002:71-82(journal)
- Lin, Wei, Guo, Rong, Ning Kai, 2003, Study on SNMP-based network management interface testing Proceeding of the International Conference on Telecommunications, 2003:134-141(conference)
- Roughan, Matthew, Gottlieb Joel, 2002, Large-scale measurement and modeling of backbone internet traffic, Proceedings of SPIE - The International Society for Optical Engineering, v 4865, 2002: 190-201(journal)
- Yoshihara K, Isomura M, Horiuchi H, 2003, Dynamic load balancing for distributed network management INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING, 118 2003:277-290(journal)
- Lopes RP, Oliveira JL, 2003, Delegation of expressions for distributed SNMP information processing INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING, 118, 2003: 395-408(journal)
- Duarte Jr., Elias Procopio, 2002, A dependable SNMP-based tool for distributed network management International Conference on Dependable Systems and Networks, 2002: 279-284(conference)
- Keeni GM, Chakraborty D, Koide K, 2003, SNMP in the IPv6 context, YMPOSIUM ON APPLICATIONS AND THE INTERNET WORKSHOPS, PROCEEDINGS 2003:254-257(journal)
- Ajita John, Keith Vanderveen, Binay Sugla, 2003, An XML-Based Framework for Dynamic SNMP MIB Extension, 10th IFIP/IEEE International Workshop on Distributed Systems 2003:107 – 120(journal)
- A. da Rocha, C. Amon da Rocha, J. Neuman de Souza, 2004, Script MIB Extension for Resource Limitation in SNMP Distributed Management Environments, ICT 2004: 11th International Conference on Telecommunications, July 2004: 835 – 840(conference)
- Ran Giladi and Merav Gat, 2003, Meta-management of Dynamic Distributed Network Managers (MEMAD), 11th IFIP/IEEE International Workshop on Distributed Systems, June 2003, Chapter: p. 119(conference)
- Aldri L. dos Santos, Elias P. Duarte, Glenn M. Keeni, 2004, Reliable Distributed Network Management by Replication, Journal of Network and Systems Management, June 2004: 191 – 213(journal)
- Chin Mun Wee, M. Salim Beg, 2002, Thresholds: Performance Evaluation for APSSNMP: An Alternative Security Algorithm for SNMP, Springer Science+Business Media B.V., Formerly Kluwer Academic Publishers B.V. December 2002: 411 – 415(journal)
- Choong Seon Hong and Joon Heo, 2004, A Policy-Based Security Management Architecture Using XML Encryption Mechanism for Improving SNMPv3, Computational Science and Its Applications – ICCSA 2004: 755 – 764(conference)
- HyungHyo Lee and BongNam Noh, 2002, Information Networking. Wireless Communications Technologies



- and Network Applications : International Conference, ICOIN 2002, Cheju Island, Korea, January 30 - February 1, 2002. Revised Papers. Part II: p. 430
- Lopes RP, Oliveira JL, 2002, A multi-protocol architecture for SNMP entities, 2002 IEEE WORKSHOP ON IP OPERATIONS AND MANAGEMENT, 2002: 75-79(journal)
- Kastner W, Sauter T, 2002, Network management of fieldbus systems with limited devices: A case study for EIB and Palm OS, ISIE 2002: PROCEEDINGS OF THE 2002 IEEE INTERNATIONAL SYMPOSIUM ON INDUSTRIAL ELECTRONICS, 2002:VOLS 1-4,129-134(journal)
- Cabrera JBD, Lewis L, Qin X, Gutierrez C, Lee W, Mehra RK, 2003, Proactive intrusion detection and SNMP-BASED security management: New experiments and validation, INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING 2003, 118:93-96(journal)
- Luis Carlos Erpen De Bona, Elias Procópio Duarte, 2004, A Flexible Approach for Defining Distributed Dependable Tests in SNMP-Based Network Management Systems, Journal of Electronic Testing, August 2004: 447 – 454(journal)
- Zhang, Pu-Han, Sun, Yu-Fang, 2002, Intelligent mobile agents-based architecture for network fault detection, Journal of Software, v 13, n 7, July, 2002: p 1209-1219(journal)
- Niki Pissinou, Bhagyavati Bhagyavati, Kia Makki, 2000, Mobile Agents to Automate Fault Management in Wireless and Mobile Networks, Parallel and Distributed Processing: 15 IPDPS 2000 Workshops, Cancun, Mexico, May 2000. Proceedings: p. 1296(conference)
- Andreas Pashalidis, Martin Fleury, 2004, Secure Network Management Within an Open-Source Mobile Agent Framework, Journal of Network and Systems Management, March 2004: 9 – 31(journal)
- Liu Ying, Ren Xinhua, Duan Lintao, 2004, the discussion of SNMP Transition mechanism from IPv4 to IPv6[J], Journal of Taiyuan University of technology, Nov 2004:Vol.35 No.6(in Chinese)(journal)
- Ma Long, Zhang Sidong, Zhang Hongke, 2003, SNMP agent implementation in IPv6[J], China Data Communications, 2003:Vol. 8 p65-67(in Chinese)(journal)
- Dominic P.A. Greenwood, Damianos Gavalas, 2004, Using Active Processes as the Basis for an Integrated Distributed Network Management Architecture, Active Networks: First International Working Conference, IWAN'99, online date: February 2004: 199-212(conference)