Review

# The Critical Role of SNMP in Enabling Network Security

mouhammd alkasassbeh [*]

Posted Date: 9 October 2023

doi: 10.20944/preprints202310.0512.v1

Keywords: SNMP, IDS, Security

*Review*

# The Critical Role of SNMP in Enabling Network Security

**Mouhammd Alkasassbeh**

Princess Sumaya University for Technology Amman Jordan; m.alkasassbeh@psut.edu.jo

**Abstract:** Simple Network Management Protocol (SNMP) is extensively utilized for monitoring and managing computer networks. This paper synthesizes and reviews recent research on harnessing SNMP data for developing effective network security solutions driven by artificial intelligence and machine learning techniques. The comprehensive device-level visibility and timely data provided by SNMP offers significant potential to enable high-performance intrusion detection systems, security analytics, and real-time monitoring capabilities to protect against evolving cyber threats. However, inherent vulnerabilities in versions like SNMP v1/v2c persist, especially due to default community strings allowing uncontrolled access. A number of techniques like newer SNMPv3 standard have been proposed to improve security through encryption, authentication, and fine-grained access control. Additionally, general best practices around firewalling, traffic monitoring, and compliance audits are recommended for robust SNMP deployment. The literature reviewed demonstrates SNMP's capabilities in enabling anomaly detection with over 99% accuracy by applying supervised learning methods like random forests and neural networks to SNMP Management Information Base (MIB) data. The network-centric visibility offered by SNMP's extensive statistics on traffic configurations and behaviors provides an invaluable advantage over packetlevel data for developing intelligent detection models. Beyond intrusion detection systems, SNMP data has also shown significant utility for security analytics like attack pattern discovery, bandwidth modeling, and large-scale threat intelligence by aggregating data from distributed network devices. Further research opportunities exist in areas like feature engineering, model optimization, and continued evaluation of evolving attacks patterns. In conclusion, with appropriate secure configurations, SNMP provides the comprehensive and real-time data needed by modern artificial intelligence security applications in a scalable manner due to its device-centric focus, standardized schema, and ubiquitous deployment.

**Keywords:** SNMP; IDS; Security

## 1. Introduction

Network security represents a major challenge in today's interconnected world, with cyber threats capable of immense damage [1]. The rise of distributed denial of service (DDoS) and other threats necessitates robust intrusion detection systems (IDS) that can rapidly identify anomalies and attacks. SNMP is a widely adopted network management protocol that plays a critical role in enabling security solutions by providing comprehensive visibility into network devices and traffic statistics [2].

This paper reviews key research on harnessing SNMP for developing high-accuracy IDS. It also synthesizes studies on utilizing SNMP data for security-related analytics. SNMP's evolution is traced, with a focus on how its security has improved over time. The vulnerabilities that persist are examined along with mitigation strategies. Best practices for secure SNMP deployment are also highlighted.

## 2. Overview of SNMP

Developed in 1988, the Simple Network Management Protocol (SNMP) is a standard TCP/IP protocol for managing and monitoring network devices [3]. It allows collecting data like traffic statistics and device configurations from SNMP agents using basic get/set operations [4]. SNMP exposes management data through a Management Information Base (MIB) that follows a hierarchical tree structure [5].

Versions like SNMPv2 and SNMPv3 enhanced security and administration capabilities [6,7]. For instance, SNMPv3 added encryption and authentication using SHA and AES [8]. The large-scale adoption of SNMP makes it a ubiquitous source of telemetry for managing modern networks.

## 3. Utilizing SNMP Data for Developing Security Solutions

### A) Intrusion Detection Systems

Several studies have successfully demonstrated the utility of SNMP MIB data for building high-accuracy IDS using supervised machine learning techniques like random forest and neural networks.

Al-Naymat et al. [9] detected network attacks with over 99% accuracy using Random Forest and MLP classifiers trained on SNMP data. Focusing on Interface and IP MIB groups further improved performance [10]. Optimizing feature selection using ReliefF reduced overhead and improved anomaly detection [11]. REP Tree and J48 classifiers leveraging the IP MIB group identified anomalies effectively [12]. ICMP variables from MIB data enabled accurate detection of various DoS attacks [13]. Al-Kasassbeh and Adda [14,15] designed mobile agents with statistical methods based on Wiener filtering to detect anomalies and classify faults using local MIB data analysis. This distributed approach improved scalability.

A model developed using Rule-based classifiers including DecisionTable, JRip, OneR, PART and ZeroR detected DoS attacks by leveraging the ICMP variables from the MIB, achieving 99.7% accuracy [16]. Deep learning methods like Stacked Autoencoders applied to MIB data enabled accurate network anomaly detection without complex feature engineering [17].Overall, these works establish SNMP MIB data as an invaluable input for modern AI-driven IDS, providing network visibility unparalleled by other data sources.

### B) Security Analytics

Beyond IDS, studies have shown SNMP's utility for security-relevant network traffic analytics like behavior forecasting [18], attack pattern discovery [19], and bandwidth profiling [20].

Centralized and decentralized techniques have been proposed for large-scale aggregation and mining of SNMP data for security analytics [21,22]. This allows leveraging SNMP as a sensor network for cyber threat intelligence.

### C) Real-Time Monitoring

SNMP provides timely data for real-time network security systems. MIB statistics have proven useful for building distributed IDS [23], early warning systems [24], and streaming analytics [25].

## 4. Evolution of SNMP Security

While providing invaluable data, SNMP faces vulnerabilities if not properly secured. Unchanged default community strings in versions like SNMP v1/v2c enable uncontrolled access [26]. Possible mitigations include community string management, access control, encryption, firewalling and securing SNMP with SSH [27].

To improve security, SNMPv3 added encryption and authentication using SHA and AES [8]. User-based Security Model (USM) enables verification and encryption between SNMP engines [28]. Secure Shell (SSH) provides protected tunnels for SNMP [29], while AES support enhances confidentiality [30].

Access control frameworks like View-based Access Control Model (VACM) allow fine-grained control by restricting MIB views [31]. Integrating SNMP with AAA systems improves access management. Firewalls and proxies help control and filter SNMP traffic [32].

## 5. Best Practices for Secure SNMP Deployment

Recommended best practices for secure SNMP deployment include [33]:

- Use newer versions like SNMPv3 with encryption
- Frequently change default community strings
- Leverage firewalls to filter SNMP traffic
- Integrate SNMP with AAA infrastructure
- Restrict MIB access via VACM model
- Monitor for anomalies in SNMP patterns
- Utilize SSH or TLS for secure transport
- Develop SNMP security and compliance monitoring

## 6. Conclusion

This paper has reviewed and synthesized research on the critical role of SNMP in enabling effective network security solutions. The comprehensive device-level visibility and timely data provided by SNMP offers significant potential to power modern AI-driven cybersecurity tools to protect against evolving threats. However, SNMP has notable vulnerabilities that need to be mitigated through proper security measures for it to serve as a secure and scalable data source. The literature reviewed demonstrates SNMP’s capabilities in enabling high-performance intrusion detection systems and anomaly detection using machine learning techniques. Supervised learning methods like random forests and neural networks have proven highly effective when applied to SNMP MIB data, with detection accuracies consistently over 99% across multiple studies. The network-centric visibility offered by SNMP's extensive statistics on traffic, configurations, and behaviors provides an invaluable advantage over packet-level data for developing intelligent anomaly detection models. Beyond IDS, SNMP data has also shown great utility for security analytics like attack pattern discovery, bandwidth modeling, and large-scale threat intelligence by aggregating data from distributed network devices. However, inherent vulnerabilities in versions like SNMP v1/v2c persist, especially due to default community strings enabling uncontrolled access. A number of techniques have been proposed and standardized to improve SNMP security, including newer versions like SNMPv3 that incorporate encryption and authentication using algorithms such as SHA and AES. Additional access control frameworks like VACM enable granular control over data access. Integrating SNMP with AAA infrastructure and leveraging tunneled transports via SSH also enhances security. Furthermore, general best practices around firewalling, traffic monitoring, and compliance audits are recommended for robust SNMP deployment.

In conclusion, with appropriate selection of secure configurations and versions, SNMP can provide the comprehensive and real-time data needed by modern AI security applications in a scalable manner. With its device-centric focus, standardized schema, and ubiquitous deployment, SNMP offers unmatched network visibility that can allow intelligent algorithms to model baseline behaviors, detect anomalies, identify malicious patterns, and generate threat intelligence. The research synthesis provided in this paper firmly establishes SNMP's current and future criticality for advancing network security in the face of increasingly sophisticated cyber threats. Further optimizations in areas like feature engineering, model selection, and parameter tuning can help continue to improve SNMP's capabilities as an enabler for AIpowered security.

## References

1. H. Debar, M. Dacier, A. Wespi. Towards a taxonomy of intrusion-detection systems. Computer Networks, 31(8):805–822, 1999.
2. J. Yu, H. Lee, M.S. Kim, D. Park. Traffic Flooding Attack Detection with SNMP MIB using SVM. Computer Communications, 31(17):4212-4219, 2008.
3. J. Case, M. Fedor, M. Schoffstall, J. Davin. A Simple Network Management Protocol (SNMP). IETF RFC 1157, 1990.

4. D. Levi, P. Meyer, B. Stewart. SNMP Applications. IETF RFC 2573, 1999.
5. K. McCloghrie, M. Rose. Management Information Base for Network Management of TCP/IP-based internets: MIB-II. IETF RFC 1213, 1991.
6. J. Case, K. McCloghrie, M. Rose, S. Waldbusser. Introduction to Community-based SNMPv2. IETF RFC 1901, 1996.
7. U. Blumenthal, B. Wijnen. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). IETF RFC 3414, 2002.
8. R. Presuhn. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP). IETF RFC 3416, 2002.
9. G. Al-Naymat, M. Al-Kasassbeh, E. Al-Hawari. Exploiting snmp-mib data to detect network anomalies using machine learning techniques. Intelligent Systems and Applications, 2018.
10. G. Al-Naymat, M. Al-Kasassbeh, E. Al-Hawari. Using machine learning methods for detecting network anomalies within SNMP-MIB dataset. International Journal of Web and Grid Services, 14(4), pp.398423, 2018.
11. G. Al-Naymat, A. Hambouz, M. Al-Kasassbeh. Evaluating the Impact of Feature Selection Methods on SNMP-MIB Interface Parameters to Accurately Detect Network Anomalies. 2019 International Conference on Smart Homes and Health Telematics, 2019.
12. A. Manna, M. Alkasassbeh. Detecting network anomalies using machine learning and SNMP-MIB dataset with IP group. 2019 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2019.
13. Y.K. Shaheen, M. Al Kasassbeh. A Proactive Design to Detect Denial of Service Attacks Using SNMPMIB ICMP Variables. 2019 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2019.
14. M. Al-Kasassbeh, M. Adda. Network fault detection with Wiener filter-based agent. Journal of Network and Computer Applications, 32(4), 824-833, 2009.
15. M. Al-Kasassbeh. Network intrusion detection with wiener filter-based agent. World Appl. Sci. J, 13(11), 2372-2384, 2011.
16. A. Hwoij, M. Al-Kasassbeh, M. Al-Fayoumi. Detecting Network Anomalies using Rule-based Machine Learning within SNMP-MIB Dataset. arXiv preprint arXiv:2002.02368, 2020.
17. G. Al-Naymat, H. Hussain, M. Al-Kasassbeh, N. Al-Dmour. Accurate detection of network anomalies within SNMP-MIB data set using deep learning. International Journal of Computer Applications in Technology, 66(1), 74-85, 2021.
18. K. Hu, A. Sim, D. Antoniades, C. Dovrolis. Estimating and Forecasting Network Traffic Performance based on Statistical Patterns Observed in SNMP Data. In Machine Learning and Data Mining in Pattern Recognition, pp. 264-278. Springer, Berlin, Heidelberg, 2013.
19. W. Cerroni, G. Moro, R. Pasolini, M. Ramilli. Decentralized Detection of Network Attacks through P2P Data Clustering of SNMP Data. Computers & Security, 49:131-149, 2015.
20. J. Yu, H. Lee, M.S. Kim, D. Park. Traffic Flooding Attack Detection with SNMP MIB using SVM. Computer Communications, 31(17):4212-4219, 2008.
21. L.P. Gaspary, R.N. Sanchez, D.W. Antunes. A SNMP-based platform for distributed Stateful Intrusion Detection in Enterprise Networks. Journal of Network and Systems Management, 13(4):437–467, 2005.
22. M. Zapf, K. Herrmann, K. Geihs. Decentralized SNMP Management with Mobile Agents. Proceedings of the 6th IEEE International Workshop on Network Management, 1999.
23. G. Rajakumaran, N. Venkataraman. Early Detection of LDOS Attack using SNMP MIBs. ITM Web of Conferences, 37: 01025, 2021.
24. S. Alhaidari, A. Alharbi, M. Alshaikhsaleh et al. Network Traffic Anomaly Detection based on Viterbi Algorithm using SNMP MIB Data. Proceedings of the 2019 7th International Conference on Software and Information Engineering, 2019.
25. M. Cheikhrouhou, J. Labetoulle. An Efficient Polling Layer for SNMP. Proceedings of the IEEE/IFIP Network Operations and Management Symposium, 2000.
26. P. Chatzimisios, A.C. Boucouvalas, V. Vitsas. Security issues and vulnerabilities of the SNMP protocol. Proceedings of the 1st IEEE International Conference on Electrical and Electronics Engineering, 2004.
27. J.J.C Gondim, R. de Oliveira Albuquerque. Mirror Saturation in Amplified Reflection Distributed Denial of Service: A Case of Study Using SNMP, SSDP, NTP and DNS Protocols. Future Generation Computer Systems, 100:344-358, 2019.
28. U. Blumenthal, F. Maino, K. McCloghrie. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model. IETF RFC 3826, 2004.
29. V. Marinov, J. Schönwälder. Performance Analysis of SNMP over SSH. Lecture Notes in Computer Science, 4268:252–263. Springer, 2006.
30. S. Fang, K.P. Bhat, G. Parks. Authentication and Authorization for Simple Network Management Protocol (SNMP). US Patent 7,877,469, 2011.
31. B.Wijnen, R. Presuhn, K.C. Norseth. View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). IETF RFC 3415, 2002.

32. J. Palmer, G.O. Vazquez. SNMP Firewall for Network Identification. US Patent 7,606,884, 2009.
33. OWASP. Securing SNMP. https://owasp.org/www-pdf-archive/OWASP-SNMP-Security-Guide-v1.pdf

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.