

Detecting Sybil nodes in stationary wireless sensor networks using learning automaton and client puzzles

Author(s): [Mojtaba Jamshidi](#)¹; [Mehdi Esnaashari](#)²; [Aso Mohammad Darwesh](#)³; [Mohammad Reza Meybodi](#)⁴
[View affiliations](#)

Source: [Volume 13, Issue 13](#), 13 August 2019, p. 1988 – 1997
DOI: [10.1049/iet-com.2018.6036](#), Print ISSN 1751-8628,
Online ISSN 1751-8636

[Access Full Text](#)[Recommend Title
Publication to
library](#)

- [« Previous Article](#)
- [Table of contents](#)
- [Next Article »](#)

© The Institution of Engineering and Technology

Received [19/10/2018](#), Accepted [13/05/2019](#), Revised [25/04/2019](#), Published [15/05/2019](#)

Article

A well-known harmful attack against wireless sensor networks (WSNs) is the Sybil attack. In a Sybil attack, WSN is destabilised by a malicious node which forges a large number of fake identities to disrupt network protocols such as routing, data aggregation, and fair resource allocation. In this study, the authors suggest a new algorithm based on a composition of learning automaton (LA) model and client puzzles theory to identify Sybil nodes in stationary WSNs. In the proposed algorithm, each node sends puzzles to its neighbours periodically during the network lifetime and tries to identify Sybil nodes among them, considering their response time (puzzle solving time). In this algorithm, each node equipped with a LA to reduce the communication and computation overhead of sending and solving puzzles. The proposed algorithm has been simulated using J-SIM simulator and simulation results have shown that the proposed algorithm can detect 100% of Sybil nodes and the false detection rate is about 5% on average. Also, the performance of the proposed algorithm has been compared to a wellknown neighbour-based algorithm through experiments and the results have shown that the proposed algorithm is significantly better than this algorithm in terms of detection and false detection rates.

Inspecc keywords: [computer network security](#); [telecommunication security](#); [protocols](#); [security of data](#); [resource allocation](#); [wireless sensor networks](#)

Other keywords: [malicious node](#); [Sybil attack](#); [Sybil nodes](#); [network protocols](#); [puzzle solving time](#); [network lifetime](#); [learning automaton](#); [neighbour-based algorithm](#); [stationary wireless sensor networks](#); [false detection rate](#); [client puzzles theory](#); [harmful attack](#); [sending solving puzzles](#)

Subjects: [Data security](#); [Wireless sensor networks](#); [Protocols](#); [Computer communications](#)

References

- Jamshidi, M., Shaltooki, A.A., Dagalzadeh, Z., et al: 'A dynamic ID assignment mechanism 1) to defend against node replication attack in static wireless sensor networks', *Int. J. Inf. Vis.*, 2019, **3**, (1), pp. 13–17.

- 2) Douceur, J.R.: 'The sybil attack, first international workshop on peer-to-peer systems (IPTPS)' (Springer, Berlin, Heidelberg, 2002), pp. 251–260.
- 3) Newsome, J., Shi, E., Song, D., et al: 'The sybil attack in sensor networks: analysis and defenses'. Int. Symp. on Information Processing in Sensor Networks, ACM, Berkeley, CA, USA, April 2004, pp. 259–268.
- 4) Misra, S., Myneni, S.: 'On identifying power control performing sybil nodes in wireless sensor networks using RSSI'. Global Telecommunications Conf., Miami, FL, USA, December 2010, pp. 1–5.
- 5) Jamshidi, M., Ranjbari, M., Esnaashari, M., et al: 'A new algorithm to defend against sybil attack in static wireless sensor networks using mobile observer sensor nodes', Ad Hoc Sensor Wirel. Netw., 2019, **43**, pp. 213–238.
- 6) Ssu, K.F., Wang, W.T., Chang, W.C.: 'Detecting sybil attacks in wireless sensor networks using neighboring information', Comput. Netw., 2009, **53**, (18), pp. 3042–3056.
- 7) Rupinder, S., Singh, J., Singh, R.: 'TBSD: a defend against sybil attack in wireless sensor networks', Int. J. Comput. Sci. Netw. Secur. (IJCSNS), 2016, **16**, (11), pp. 90–99.
- 8) Dhamodharan, U.S., Vayanaperumal, R.: 'Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method', Scientific World J., 2015, **1**, (1), pp. 13–17.
- 9) Rafeh, R., Khodadadi, M.: 'Detecting sybil nodes in wireless sensor networks using two-hop messages', Indian J. Sci. Technol., 2014, **7**, (9), pp. 1359–1368.
- 10) Sarigiannidis, P., Karapistoli, E., Economides, A.: 'Detecting sybil attacks in wireless sensor networks using UWB ranging-based information', Expert Syst. Appl., 2015, **42**, (21), pp. 7560–7572.
- 11) Tang, Q., Wang, J.: 'A secure positioning algorithm against sybil attack in wireless sensor networks based on number allocating'. 17th Int. Conf. on Communication Technology (ICCT), Chengdu, China, October 2017, pp. 932–936.
- 12) Chen, S., Yang, G., Chen, S.: 'A security routing mechanism against sybil attack for wireless sensor networks'. Int. Conf. on Communications and Mobile Computing, Shenzhen, China, April 2010, pp. 142–146.
- 13) Jangra, A., Priyanka, S.: 'Securing LEACH protocol from sybil attack using jakes channel scheme (JCS)'. Int. Conf. on Advances in ICT for Emerging Regions, Sri Lanka Foundation Institute, Colombo, Sri Lanka, 2011, pp. 79–87.
- 14) Jan, M.A., Nanda, P., He, X., et al: 'A sybil attack detection scheme for a centralized clustering-based hierarchical network'. Trustcom/BigDataSE/ISPA1, Helsinki, Finland, August 2015, pp. 318–325.
- 15) Jamshidi, M., Zangeneh, E., Esnaashari, M., et al: 'A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it', Wirel. Pers. Commun., 2018, **105**, (1), pp. 145–173.
- 16) Piro, C., Shields, C., Levine, B.N.: 'Detecting the sybil attack in mobile Ad hoc networks'. Securecomm and Workshops, Baltimore, MD, USA, August 2006, pp. 1–11.
- 17) Jamshidi, M., Zangeneh, E., Esnaashari, M., et al: 'A lightweight algorithm for detecting mobile sybil nodes in mobile wireless sensor networks', Comput. Electr. Eng., 2017, **64**, pp. 220–232.

- 18) Jamshidi, M., Ranjbari, M., Esnaashari, M., et al: 'Sybil node detection in mobile wireless sensor networks using observer nodes', *Int. J. Inf. Vis.*, 2018, **2**, (3), pp. 159–165.
- 19) Jamshidi, M., Darwesh, A.M., Lorenc, A., et al: 'A precise algorithm for detecting malicious sybil nodes in mobile wireless sensor networks', *IEEE Trans. Smart Process. Comput.*, 2018, **7**, (6), pp. 457–466.
- 20) Juels, A., Brainard, J.: 'Client puzzles: a cryptographic countermeasure against connection depletion attacks'. *NDSS*, 99, 1999, pp. 151–165.
- 21) Aura, T., Nikander, P., Leiwo, J.: 'DOS-resistant authentication with client puzzles'. *Int. Workshop on Security Protocols*, Berlin, Heidelberg, April 2000, pp. 170–177.
- 22) Dwork, C., Naor, M.: 'Pricing via processing or combating junk mail'. *Annual Int. Cryptology Conf.*, Berlin, Heidelberg, May 1993, pp. 139–147.
- 23) Singh, V.P., Jain, S., Singhai, J.: 'Hello flood attack and its countermeasures in wireless sensor networks', *Int. J. Comput. Sci. Issues*, 2010, **7**, (11), pp. 23–27.
- 24) Bocan, V.: 'Threshold puzzles: the evolution of DOS-resistant authentication', *Periodica Politecnica, Trans. Autom. Control Comput. Sci.*, 2004, **49**, p. 63.
- 25) Dong, Q., Gao, L., Li, X.: 'A new client-puzzle based DoS-resistant scheme of IEEE 802.11i wireless authentication protocol'. *3rd Int. Conf. on Biomedical Engineering and Informatics (BMEI)*, Yantai, China, October 2010, pp. 2712–2716.
- 26) Ranjbari, M., Torkestani, J.A.: 'A learning automata-based algorithm for energy and SLA efficient consolidation of virtual machines in cloud data centers', *J. Parallel Distrib. Comput.*, 2018, **113**, pp. 55–62.
- 27) Esnaashari, M., Meybodi, M.R.: 'A cellular learning automata-based deployment strategy for mobile wireless sensor networks', *J. Parallel Distrib. Comput.*, 2011, **71**, (7), pp. 988–1001.
- 28) Jangirala, S., Dheerendra, M., Sourav, M.: 'Secure lightweight user authentication and key agreement scheme for wireless sensor networks tailored for the internet of things environment'. *Int. Conf. on Information Systems Security*, Cham, November 2016, pp. 45–65.
- 29) Dutta, P.K., Hui, J.W., Chu, D.C., et al: 'Securing the deluge network programming system'. *Proc. of the 5th Int. Conf. on Information Processing in Sensor Networks*, ACM, Nashville, Tennessee, USA, April 2006, pp. 326–333.
- 30) Sobeih, A., Hou, J.C., Kung, L.C., et al: 'J-Sim: a simulation and emulation environment for wireless sensor networks', *IEEE Wirel. Commun.*, 2006, **13**, (4), pp. 104–119.



Related content

Server notaries: a complementary approach to the web PKI trust model

- Emre Yüce and Ali Aydın Selçuk
- [View description](#) [Hide description](#)
- Secure socket layer/transport layer security (TLS) is the de facto protocol for providing secure communications over the Internet. It relies on the web PKI model for authentication and secure key exchange. Despite its relatively successful past, the number of web PKI incidents observed have increased recently. These incidents revealed the risks of forged certificates issued by certificate authorities without the consent of the domain owners. Several solutions have been proposed to solve this problem but no solution has yet received widespread adoption due to complexity and

deployability issues. In this study, the authors propose an effective solution for this problem that allows a TLS server to detect a certificate substitution attack against its domain across the Internet. The proposed solution is practical and allows a smooth and gradual transition. They also give a triangulation algorithm enabling the server to find out the origin of the attack. They conducted simulation experiments using real-world BGP data and showed that their proposal can be effective for detecting and locating attacks using relatively few vantage points over the Internet.

An adaptive membership protocol against Sybil attack in unstructured P2P networks

- Haowen Liu ; Chao Ma ; R. Walshe
- [View description](#) [Hide description](#)
- A Sybil attack refers to a network attack against identify in which a malicious user obtains multiple fake identities and creates fake nodes which are inserted amongst honest nodes in the system simultaneous. By controlling a large percentage of the system, or a large section of the local scope, the malicious user can take further boring actions like DDos attacks, False Voting, Invalid DHT routing, identifying worm spam and so on. This type of network intrusion is often found in Peer-to-Peer (P2P) and other decentralized, distributed systems. It can be difficult to predict or defend the Sybil Attack due to the open and anonymous in P2P networks. Although it is possible to identify some sybil nodes or edges, one must consider the critical case where some of the sybil nodes may have left the network prior to search, and as a result of churn attack is not prevented. In this paper, the authors present a novel protocol with a positive communication policy among peers and adaptive neighbour monitoring and maintenance scheme to counter sybil, preventing malicious nodes and maintaining desirable properties such as a low network diameter and clustering. The protocol is resilient against the Sybil and Churn attacks, and is particularly suitable for information dissemination and files sharing in unstructured P2P systems.

Computationally efficient mutual authentication protocol for remote infant incubator monitoring system

- Subramani Jegadeesan ; Muneeswaran Dhamodaran ; Maria Azees ; Swaminathan Sri Shanmugapriya
- [View description](#) [Hide description](#)
- Internet of Things (IoT), cloud computing and wireless medical sensor networks have significantly improved remote healthcare monitoring. In a healthcare monitoring system, many resource-limited sensors are deployed to sense, process and communicate the information. However, continuous and accurate operations of these devices are very important, especially in the infant incubator monitoring system. Because important decisions are made on the received information. Therefore, it is necessary to ensure the authenticity between the incubator monitoring system and doctors. In this work, a public key encryption based computationally efficient mutual authentication protocol is proposed for secure data transmission between incubator monitoring systems and doctors or administrators. The proposed protocol improves performance and reduces the computational cost without compromising the security. The security analysis part shows the strength of the proposed protocol against various attacks, performance analysis part shows that the proposed protocol performs better than other existing protocol based on Rivest–Shamir–Adleman and elliptic-curve cryptography schemes.

Privacy and data security for grid-connected home area network using Internet of Things

- Arunmozhi Manimuthu and Ramadoss Ramesh
- [View description](#) [Hide description](#)
- Sensors with IoT assistance provides secured communication and data integrity inside HAN. Energy reading and information flow from the smart grid, together with sensors, bring about a new perspective on energy management. This paper primarily investigates the secured data flow in HAN and assures data privacy of customers during critical and emergency operations. Data are made available in real time with

minimum transit time delay. Devices are continuously monitored for vital and emergency services. This paper focuses on machine to machine data flow and packet delivery using IoT. It helps in making user's power consumption data available over the cloud and also in customised electronic devices in real-time. This research work showcases the requirements for developing a cost-effective IoT-HAN connected with smart grid for energy aware routing. The advanced design scheme helps to place sensors, and control gateway in a well-defined boundary, consuming less energy for data transfer and data processing. Data flow pattern and packet delivery rate is tested using both simulated and actual data from sensors and concentrators. The obtained results and flow pattern is evaluated using MATLAB and network simulator. The developed IoT-HAN setup is optimally helpful in secured data exchange among different connected devices inside HAN.

Zero-knowledge Proofs in M2M Communication

- M. Schukat and P. Flood
- [View description](#) [Hide description](#)
- The advent of the IoT with an estimated 50 billion internet enabled devices by the year 2020 raises questions about the suitability and scalability of existing mechanisms to provide privacy, data integrity and end-entity authentication between communicating peers. In this paper we present a new protocol that combines zero-knowledge proofs and key exchange mechanisms to provide secure and authenticated communication in static M2M networks, therefore addressing all the above problems. The protocol is suitable for devices with limited computational resources and can be deployed in wireless sensor networks. While the protocol requires an a-priori knowledge about the network setup and structure, it guarantees perfect forward secrecy.

Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks

- Movva Pavani and Polipalli Trinatha Rao
- [View description](#) [Hide description](#)
- One of the important considerations in a sensor network is energy consumption. Cluster-based routing protocols are often proposed to reduce energy consumption. However, clusters are vulnerable due to malicious nodes. Malicious nodes inject fake messages to cluster-header, which increases communication overhead and energy consumption. Secure cluster-based routing is one of the most required solutions to consume more energy during data transmission. In this study, the authors propose a secure cluster-based routing protocol (SCBRP) that uses adaptive particle swarm optimisation (PSO) with optimised firefly algorithms during data transmission in a wireless sensor network. The objective of this study is to minimise energy consumption over an individual node to improve the whole network lifetime. The proposed SCBRP is based on the hexagonal sensor network architecture, and it is designed by three processes to include energy-efficient clustering, secure routing, and security verification. The performance of the proposed SCBRP is evaluated using NS-3, and it is estimated by different metrics such as encryption time, decryption time, energy consumption, packet drop rate, and network lifetime. The simulation results are compared with the previous approaches and finally, the authors' proposed SCBRP is proved that it obtained better performance than previous approaches.