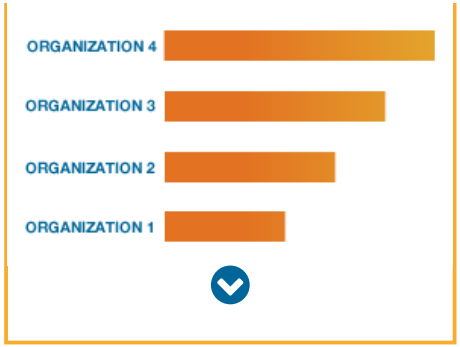
Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning

Publisher: IEEE

Fatima-tuz-Zahra; NZ Jhanjhi; Sarfraz Nawaz Brohi; Nazir A. Malik; Mamoona Humayun All Authors



Abstract: Internet of Things have profoundly transformed the way technology is deployed today in different domains of life. However, its widescale implementation has also caused ma...**View more**

Metadata

Abstract:
Internet of Things have profoundly transformed the way technology is deployed today in different domains of life. However, its widescale implementation has also caused major security concerns in context of data communication because of escalating interconnectivity of resource-constrained smart devices. Due to the exacerbating security attack vulnerability, it has become necessary to address the issue of insecure routing in these devices. Low-power and lossy IoT networks on which they run commonly use RPL for routing due to its lightweight nature and compatibility for data transmission. However, RPL is prone to both WSN-inherited and RPL-specific attacks. Several existing solutions have addressed the detection of some of them. However, lack of mitigation techniques is observed which can extenuate attacks of both types such as wormhole as well as rank attack; when they are launched on an RPL-based network. Therefore, the aim of this study is to introduce RPL, its vulnerability to the two attacks, and the proposition that machine learning techniques like support vector machines can be effectively used to develop a secure and improved version of RPL for mitigation of both WSN-inherited and RPL-specific attacks in an RPL-based IoT network.

Published in: 2020 2nd International Conference on Computer and Information Sciences (ICCIS)

Date of Conference: 13-15 Oct. 2020

DOI: 10.1109/ICCIS49240.2020.9257607

Date Added to IEEE *Xplore*: 24 November 2020

Publisher: IEEE

ISBN Information:

Conference Location: Sakaka, Saudi Arabia, Saudi Arabia

Citation Map

1.*World's smallest IoT project*, Jan. 2018, [online] Available: https://medium.com/@tomsononline/worlds-smallest-iot-project88b9506c6d9d.
Show Context Google Scholar

2.Z.A. Almusaylim and N. Zaman, *A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) Wireless Networks*, vol. 25, no. 6, pp. 3193-3204.
Show Context Google Scholar

3.*IoT Standards and Protocols*, 2019, [online] Available: https://www.postscapes.com/internet-of-things-protocols/.
Show Context Google Scholar

4.M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", *2018 20 th International Conference on Advanced Communication Technology (ICACT)* , pp. 481-487.
Show Context Google Scholar

5.M. Almulhim, N. Islam and N. Zaman, "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications", *International Journal of Computer Science and Network Security*, vol. 19, no. 1, pp. 107-120.
Show Context Google Scholar

6.A. Raoof, A. Matrawy and C.H. Lung, "Routing Attacks and Mitigation Methods for RPL- Based Internet of Things", *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1582-1606, 2019.
Show Context View Article Full Text: PDF (1766KB) Google Scholar

7.B. Ghaleb, A. Al-Dubai, E. Ekonomou, A. Alsarhan, Y. Nasser, L. Mackenzie, et al., "A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-power

and Lossy Networks: A Focus on Core Operations", *IEEE Communications Survevs & Tutorials*, vol. 21, no. 2, Secondauarter 2019.
Show Context View Article Full Text: PDF (3602KB) Google Scholar

8.T. Winter et al., "RPL: IPv6 Routing Protocol for Low Power and Lossy Networks", *Internet Requests for Comments RFC Editor RFC 6550*, March 2012.
Show Context CrossRef Google Scholar

9.R. Jadhav, R. Sahoo, Y. Wu and Huawei, RPL Observations draft-rahul-roll-rpl-observations-01, 2018.
Show Context Google Scholar

10.A. Rehman, S.U. Rehman and H. Raheem, "Sinkhole Attacks in Wireless Sensor Networks: A Survey", *Wireless Pers Commun*, 2019.
Show Context CrossRef Google Scholar

11.C. Gurjar, *Wireless Attacks Unleashed*, [online] Available: https://resources.infosecinstitute.com/wireless-attacks-unleashedl#gref.
Show Context Google Scholar

12.N. Dutta and M.M. Singh, "Wormhole Attack in Wireless Sensor Networks: A Critical Review" in Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing, Singapore:Springer, vol. 702, 2019.
Show Context CrossRef Google Scholar

13.P. Pongle and G. Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things", *International Journal of Computer Applications*, vol. 121, no. 9, pp. 1-9, 2015.
Show Context CrossRef Google Scholar

14.D. Airehrour, J. Gutierrez and S. K. Ray, "Secure Routing for Internet of Things: A Survey", *Journal of Network and Computer Applications*, vol. 66, pp. 198-213, 2016.

Show Context CrossRef Google Scholar

15.L. Wallgren, S. Raza and T. Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things", *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, 2013.
Show Context CrossRef Google Scholar

16.A. Mayzaud, R. Badonnel and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", *International Journal of Network Security*, 2016.
Show Context Google Scholar

17.U. Guler, M.S.E. Sendi and M. Ghovanloo, "Dual-mode passive rectifier for wide-range input power flow", *IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug. 2017.
View Article Full Text: PDF (610KB) Google Scholar

18. Nagasai, *Classification of IoT Devices*, 2017, [online] Available: https://www.cisoplatform.com/profiles/blogs/classification-of-iotdevices.
Google Scholar

19.S. Raza, L. Wallgren and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661-2674, 2013.
Show Context CrossRef Google Scholar

20.C. Cervantes, D. Poplade, M. Nogueira and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things", *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 606611, 2015.
Show Context View Article Full Text: PDF (871KB) Google Scholar

21.H. Sedjelmaci, S. M. Senouci and T. Taleb, "An Accurate Security Game for Low-Resource IoT Devices", *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9381-9393, Oct. 2017.

Show Context View Article Full Text: PDF (1377KB) Google Scholar

22.F. Yusuf, D. Unal and E. Gul, "Deep Learning for Detection of Routing Attacks in the Internet of Things", *International Journal of Computational Intelligence Systems*, vol. 12, pp. 39-58, June 2018.
Show Context CrossRef Google Scholar

23.K. Heurtefeux, O. Erdene-Ochir, N. Mohsin and H. Menouar, "Enhancing RPL Resilience Against Routing Layer Insider Attacks", *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*, pp. 802807, 2015.
Show Context View Article Full Text: PDF (222KB) Google Scholar

24.C. Pu and S. Hajjar, "Mitigating Forwarding misbehaviors in RPLbased low power and lossy networks", *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1-6, 2018.
Show Context View Article Full Text: PDF (328KB) Google Scholar

25.B. A. Alabsi, M. Anbar, S. Manickam and O. E. Elejla, "DDoS attack aware environment with secure clustering and routing based on RPL protocol operation", *IET Circuits Devices & Systems*, vol. 13, no. 6, pp. 748-755, 2019.
Show Context View Article Full Text: PDF (1673KB) Google Scholar

26.A. Tandon and P. Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT", *2019 Twelfth International Conference on Contemporary Computing (IC3)*, pp. 1-7, 2019.
Show Context View Article Full Text: PDF (722KB) Google Scholar

27.A. Mayzaud, R. Badonnel and I. Chrisment, "A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks", *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 472-486, June 2017.
Show Context View Article Full Text: PDF (2039KB) Google Scholar

28.A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment and J. Schonwalder, "Using the RPL Protocol for Supporting Passive Monitoring in the Internet of Things", *Proc. of the IEEE/IFIP Network Operations and Management Symposium (NOMS)*, Apr. 2016.
Show Context View Article Full Text: PDF (620KB) Google Scholar

29.B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani and L. Mackenzie, "Addressing the DAO Insider Attack in RPL's Internet of Things Networks", *IEEE Communications Letters*, vol. 23, no. 1, pp. 68-71, Jan. 2019.
Show Context View Article Full Text: PDF (724KB) Google Scholar

30.*Attack mitigation using learning machines*, Jul. 2016.
Show Context Google Scholar

31.K. Hussain, S.J. Hussain, NZ. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", *International Conference on Computer and Information Sciences (ICCIS)*, pp. 1-4, 2019.
Show Context View Article Full Text: PDF (1562KB) Google Scholar

32.S.H. Kok, A. Abdullah, N.Z. Jhanjhi and M. Supramaniam, "A Review of Intrusion Detection System using Machine Learning Approach", *International Journal of Engineering Research and Technology*, vol. 12, no. 1, pp. 8-15.
Show Context Google Scholar

33.R. Case, *Machine Learning Part 2: Supervised Learning*, Oct. 2019, [online] Available: https://towardsdatascience.com/machine-learning-part-2-supervisedlearning-632621f77188.
Show Context Google Scholar

34.M. Wadkar, F. D. Troia and M. Stamp, "Detecting Malware Evolution Using Support Vector Machines", *Expert Systems With Applications*, 2019.
Show Context Google Scholar

35.A. Souri and R. Hosseini, "A state of the art survey of malware detection approaches using data mining techniques", *Human-centric Computing and Information Sciences*, vol. 8, pp. 1-22, 2018.
Show Context CrossRef Google Scholar

36.D. Ucci, L. Aniello and R. Baldoni, "Survey of machine learning techniques for malware analysis", *Computers & Security*, vol. 81, pp. 123-147, 2019.
Show Context CrossRef Google Scholar

37.Y. Ye, T. Li, D. Adjeroh and S.S. Iyengar, "A Survey on Malware Detection Using Data Mining Techniques", *ACM Computing Surveys*, vol. 50, no. 3, 2017.
Show Context Access at ACM Google Scholar

Contents

IoT has attained massive recognition for its smart implementation in diverse systems as well as industries. Starting from a small project like an IoT button [1] as its implementation to as big as a smart home [2] and a smart city, the magnitude of IoT application has immensely grown wider with time. Despite its popularity in today's technological world, security remains a vital domain of concern in terms of data communication and routing. One of the main reasons is the widescale interconnection of not only digital gadgets but also 'things' that humans use in their daily life because they are connected to the internet. Considering the expansive use of technology to volumize smart infrastructure, active exploration and development is being done in regards with suitable protocols, standards [3], and schemes for different layers of IoT architecture to provide authentication [4], [5], authorization and integrity among other security traits. Same is the case when dealing with routing in this type of network.

Authors

Figures

References

Citation Map

1. *World's smallest IoT project*, Jan. 2018, [online] Available: https://medium.com/@tomsononline/worlds-smallest-iot-project88b9506c6d9d.
Show Context Google Scholar

2. Z.A. Almusaylim and N. Zaman, *A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) Wireless Networks*, vol. 25, no. 6, pp. 3193-3204.
Show Context Google Scholar

3. *IoT Standards and Protocols*, 2019, [online] Available: https://www.postscapes.com/internet-of-things-protocols/.
Show Context Google Scholar

4. M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", *2018 20 th International Conference on Advanced Communication Technology (ICACT)* , pp. 481-487.
Show Context Google Scholar

5. M. Almulhim, N. Islam and N. Zaman, "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications", *International Journal of Computer Science and Network Security*, vol. 19, no. 1, pp. 107-120.
Show Context Google Scholar

6. A. Raoof, A. Matrawy and C.H. Lung, "Routing Attacks and Mitigation Methods for RPL- Based Internet of Things", *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1582-1606, 2019.
Show Context View Article Full Text: PDF (1766KB) Google Scholar

7.B. Ghaleb, A. Al-Dubai, E. Ekonomou, A. Alsarhan, Y. Nasser, L. Mackenzie, et al., "A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-power and Lossy Networks: A Focus on Core Operations", *IEEE Communications Survevs & Tutorials*, vol. 21, no. 2, Secondauarter 2019.
Show Context View Article Full Text: PDF (3602KB) Google Scholar

8.T. Winter et al., "RPL: IPv6 Routing Protocol for Low Power and Lossy Networks", *Internet Requests for Comments RFC Editor RFC 6550*, March 2012.
Show Context CrossRef Google Scholar

9.R. Jadhav, R. Sahoo, Y. Wu and Huawei, RPL Observations draft-rahul-roll-rpl-observations-01, 2018.
Show Context Google Scholar

10.A. Rehman, S.U. Rehman and H. Raheem, "Sinkhole Attacks in Wireless Sensor Networks: A Survey", *Wireless Pers Commun*, 2019.
Show Context CrossRef Google Scholar

11.C. Gurjar, *Wireless Attacks Unleashed*, [online] Available: https://resources.infosecinstitute.com/wireless-attacks-unleashedl#gref.
Show Context Google Scholar

12.N. Dutta and M.M. Singh, "Wormhole Attack in Wireless Sensor Networks: A Critical Review" in Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing, Singapore:Springer, vol. 702, 2019.
Show Context CrossRef Google Scholar

13.P. Pongle and G. Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things", *International Journal of Computer Applications*, vol. 121, no. 9, pp. 1-9, 2015.
Show Context CrossRef Google Scholar

14.D. Airehrour, J. Gutierrez and S. K. Ray, "Secure Routing for Internet of Things: A Survey", *Journal of Network and Computer Applications*, vol. 66, pp. 198-213, 2016.
Show Context CrossRef Google Scholar

15.L. Wallgren, S. Raza and T. Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things", *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, 2013.
Show Context CrossRef Google Scholar

16.A. Mayzaud, R. Badonnel and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", *International Journal of Network Security*, 2016.
Show Context Google Scholar

17.U. Guler, M.S.E. Sendi and M. Ghovanloo, "Dual-mode passive rectifier for wide-range input power flow", *IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug. 2017.
View Article Full Text: PDF (610KB) Google Scholar

18. Nagasai, *Classification of IoT Devices*, 2017, [online] Available: https://www.cisoplatform.com/profiles/blogs/classification-of-iotdevices.
Google Scholar

19.S. Raza, L. Wallgren and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661-2674, 2013.
Show Context CrossRef Google Scholar

20.C. Cervantes, D. Poplade, M. Nogueira and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things", *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 606611, 2015.
Show Context View Article Full Text: PDF (871KB) Google Scholar

21.H. Sedjelmaci, S. M. Senouci and T. Taleb, "An Accurate Security Game for Low-Resource IoT Devices", *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9381-9393, Oct. 2017.
Show Context View Article Full Text: PDF (1377KB) Google Scholar

22.F. Yusuf, D. Unal and E. Gul, "Deep Learning for Detection of Routing Attacks in the Internet of Things", *International Journal of Computational Intelligence Systems*, vol. 12, pp. 39-58, June 2018.
Show Context CrossRef Google Scholar

23.K. Heurtefeux, O. Erdene-Ochir, N. Mohsin and H. Menouar, "Enhancing RPL Resilience Against Routing Layer Insider Attacks", *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*, pp. 802807, 2015.
Show Context View Article Full Text: PDF (222KB) Google Scholar

24.C. Pu and S. Hajjar, "Mitigating Forwarding misbehaviors in RPLbased low power and lossy networks", *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1-6, 2018.
Show Context View Article Full Text: PDF (328KB) Google Scholar

25.B. A. Alabsi, M. Anbar, S. Manickam and O. E. Elejla, "DDoS attack aware environment with secure clustering and routing based on RPL protocol operation", *IET Circuits Devices & Systems*, vol. 13, no. 6, pp. 748-755, 2019.
Show Context View Article Full Text: PDF (1673KB) Google Scholar

26.A. Tandon and P. Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT", *2019 Twelfth International Conference on Contemporary Computing (IC3)*, pp. 1-7, 2019.
Show Context View Article Full Text: PDF (722KB) Google Scholar

27.A. Mayzaud, R. Badonnel and I. Chrisment, "A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks", *IEEE Transactions on*

Network and Service Management, vol. 14, no. 2, pp. 472-486, June 2017.
Show Context View Article Full Text: PDF (2039KB) Google Scholar

28.A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment and J. Schonwalder, "Using the RPL Protocol for Supporting Passive Monitoring in the Internet of Things", *Proc. of the IEEE/IFIP Network Operations and Management Symposium (NOMS)*, Apr. 2016.
Show Context View Article Full Text: PDF (620KB) Google Scholar

29.B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani and L. Mackenzie, "Addressing the DAO Insider Attack in RPL's Internet of Things Networks", *IEEE Communications Letters*, vol. 23, no. 1, pp. 68-71, Jan. 2019.
Show Context View Article Full Text: PDF (724KB) Google Scholar

30.*Attack mitigation using learning machines*, Jul. 2016.
Show Context Google Scholar

31.K. Hussain, S.J. Hussain, NZ. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", *International Conference on Computer and Information Sciences (ICCIS)*, pp. 1-4, 2019.
Show Context View Article Full Text: PDF (1562KB) Google Scholar

32.S.H. Kok, A. Abdullah, N.Z. Jhanjhi and M. Supramaniam, "A Review of Intrusion Detection System using Machine Learning Approach", *International Journal of Engineering Research and Technology*, vol. 12, no. 1, pp. 8-15.
Show Context Google Scholar

33.R. Case, *Machine Learning Part 2: Supervised Learning*, Oct. 2019, [online] Available: https://towardsdatascience.com/machine-learning-part-2-supervisedlearning-632621f77188.
Show Context Google Scholar

34.M. Wadkar, F. D. Troia and M. Stamp, "Detecting Malware Evolution Using Support Vector Machines", *Expert Systems With Applications*, 2019.
Show Context Google Scholar

35.A. Souri and R. Hosseini, "A state of the art survey of malware detection approaches using data mining techniques", *Human-centric Computing and Information Sciences*, vol. 8, pp. 1-22, 2018.
Show Context CrossRef Google Scholar

36.D. Ucci, L. Aniello and R. Baldoni, "Survey of machine learning techniques for malware analysis", *Computers & Security*, vol. 81, pp. 123-147, 2019.
Show Context CrossRef Google Scholar

37.Y. Ye, T. Li, D. Adjeroh and S.S. Iyengar, "A Survey on Malware Detection Using Data Mining Techniques", *ACM Computing Surveys*, vol. 50, no. 3, 2017.
Show Context Access at ACM Google Scholar

Keywords