References

[1] Ahmed, F., and Ko, Y. B. (2016). - Mitigation of Black hole Attacks in Routing Protocol for Low Power and Lossy Networks. Security and Communication Networks, 9(18).

[2] Airehrour, D., Gutierrez, J., and Ray, S. K. (2016). - A Lightweight Trust Design for IoT Routing. International Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd IEEE Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, pp. 552-557.

[3] Airehrour, D., Jairo G., and Ray, S. (2016). - Secure routing for Internet of Things: A Survey. Journal of Network and Computer Applications, pp.198-213.

[4] Alaparthy, V. T., and Morgera, S. D. (2018). - A Multi-Level Intrusion Detection System for Wireless Sensor Networks based on Immune Theory. IEEE Access, 1(1).

[5] Al-Turjman, F., and B, D. (2019). - A Hybrid Secure Routing and Monitoring Mechanism in IoT-based Wireless Sensor Networks. Ad Hoc Networks.

[6] Ancillotti, R., and Conti, M. (2014) - Reliable Data Delivery with the IETF Routing Protocol for Low-Power and Lossy Networks. IEEE Transactions on Industrial Informatics, 10(3), pp. 1864–1877.

[7] Ancillotti, R., Conti, M., Mingozzi, E. and Vallati, C. (2014). - Lightweight link Quality Estimation through Trickle in RPL networks. World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE 15th International Symposium on a. IEEE, pp. 1–9.

[8] Anita, X., Bhagyaveni, M. A., and Martin, J. (2014). - Collaborative Lightweight Trust Management Scheme for Wireless Sensor Networks. Wireless Personal Communications, 80(1), pp. 117–140.

[9] Anita, X., Martin Leo Manickam, J., and Bhagyaveni, M. A. (2013). - Two-Way Acknowledgment-Based Trust Framework for Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 9(5).

[10] Arıs, A., Yalcın, S. B., and Oktug, S. F. (2018). - New Lightweight Mitigation Techniques for RPL Version Number Attacks. Ad Hoc Networks.

[11] Atzori, L., Iera, A., and Morabito, G. (2010). - The Internet of Things: A Survey, Computer networks, 54(15), pp. 2787- 2805.

[12] Ayaz, M., Ammad, M., Sharif, Z., Mansour, A., and Aggoune, M. (2019) – Internet of Things (IoT) based Smart Agriculture: Towards Making the Fields Talk. IEEE Access, pp. 1–1.

[13] Aydogan, E., Yilmaz, S., Sen, S., Butun, I., Forsstrom, S., and Gidlund, M. (2019). - A Central Intrusion Detection System for RPL-Based Industrial Internet of Things. 15th IEEE International Workshop on Factory Communication Systems (WFCS).

[14] Azad, M., Mahmoud, M., Ur Rehman, H., Salah, K., and Arshad, J. (2018). - COLIDE: A Collaborative Intrusion Detection Framework for Internet of Things. IET Research Journals.

[15] Baker, S. B., Xiang, W., and Atkinson, I. (2017). -Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. IEEE Access, 5, pp. 26521–44.

[16] Bandyopadhyay, D., and Sen, J. (2011). - Internet of Things: Applications and Challenges in Technology and Standardization. Wireless Personal Communications, 58(1), pp. 49–69.

[17] Chang, K. (2014). - Bluetooth: a viable solution for IoT. IEEE Wireless Communications, 21(6), pp. 6–7.

[18] Chen Y., Chanet, J. and Hou, K. (2012). - RPL Routing Protocol a Case Study: Precision Agriculture. First China-France Workshop on Future Computing Technology (CF-WoFUCT), pp. 6–10.

[19] Chen, C. M., Hsu, S. C., and Lai, G. H. (2016). - Defense Denial-of-Service Attacks on IPv6 Wireless Sensor Networks. International Genetic and Evolutionary Computing, Springer International Publishing, pp. 319-26.

[20] Chze P. L. R. and Leong K. S. (2014). - A Secure Multi-Hop Routing for IoT Communication. IEEE World Forum on Internet of Things (WF-IoT), pp. 428-32.

[21] Conti, M., Kaliyar, P., Rabbani, M. M., and Ranise, S. (2018). - SPLIT: A Secure and Scalable RPL Routing Protocol for Internet of Things. 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).

[22] Dalipi, F. and Yayilgan, S, Y. (2016).-Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 63-68.

[23] David, A., Jairo, G., and Ray, S. (2016) – Secure Routing for Internet of Things: A Survey, Journal of Network and Computer Applications, 66, pp.198–213.

[24] Dawans, S., and Bonaventure, O. (2012) - On link Estimation in Dense RPL Deployments. Local Computer Networks Workshops (LCN Workshops), IEEE 37th Conference, pp. 952–55.

[25] Din, I. U., Guizani, M., Kim, B., Hassan, S., and Khan, M. K. (2018). - Trust Management Techniques for the Internet of Things: A Survey. IEEE Access, 1–1.

[26] Ding, Y., Zhou, X. W., Cheng, Z. M., and Lin, F. H. (2013). - A Security Differential Game Model for Sensor Networks in Context of the Internet of Things. Wireless Personal Communications, 72(1), pp. 375-88.

[27] Djedjig, N., Tandjaoui, D., Medjek, F. (2015). - Trust-based RPL for the Internet of Things. IEEE Symposium on Computer and Communication (ISCC).

[28] Djedjig, N., Tandjaoui, D., Medjek, F., and Romdhani, I. (2017). - New trust metric for the RPL routing protocol. 8th International Conference on Information and Communication Systems (ICICS).

[29] Duan, J., Gao, D., Yang, D., Foh, C. H., and Chen, H. H, (2014). - An Energy-Aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications. IEEE Internet of Things Journal, 1(1), pp.58-69.

[30] Duan, J., Yang, D., Zhu, H., Zhang, S., and Zhao, J. (2014). - TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 10(1).

[31] Dvir A., Holczer T., and Buttyan L. (2011) - VeRA- Version Number and Rank Authentication in RPL Mobile Adhoc Sensor System (MASS). IEEE 8th International Conference, pp.709–14.

[32] Dziak, D., Jachimczyk, B., and Kulesza, W. (2017). - IoT-Based Information System for Healthcare Application: Design Methodology Approach. Applied Sciences, 7(6), pp. 596.

[33] Feng, S. Che, X. Wang, and J. Wan. (2014) - An Incentive Mechanism based on Game Theory for Trust Management," Security and Communication Networks, 7, pp. 2318-25.

[34] Furkan, Y., Devrim, U., and Ensar, G. (2018). - Deep Learning for Detection of Routing Attacks in the Internet of Things. International Journal of Computational Intelligence Systems, 12(1), pp. 39-58.

[35] Gaddour, O., Koubaa, A., and Abid, M. (2015). – Quality of Service Aware Routing for Static and Mobile IPv6 based Low Power and Lossy Sensor Networks using RPL. Ad Hoc Network, 33, pp. 233–256.

[36] Gaddour, O., Koubaa, A., Rangarajan, R., Cheikhrouhou, O., Tovar, E., and Abid, M. (2014). - Co-RPL: RPL Routing for Mobile Low Power Wireless Sensor Networks using Corona Mechanism. Proceedings of the 9th IEEE International Symposium on Industrial Embedded Systems (SIES), pp. 200–209.

[37] Gara, F., Ben Saad, L., Ben Ayed, R., and Tourancheau, B. (2015). - RPL Protocol Adapted for Healthcare and Medical Applications. Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, pp. 690–95.

[38] Gartner. (2013) - Internet of Things Installed Base Will Grow to 26 Billion Units By 2020.

[39] Guclu, S. O., Ozcelebi, T., and Lukkien, J. (2016). - Trust-Based Neighbor Unreachability Detection for RPL. 25th International Conference on Computer Communication and Networks (ICCCN).

[40] Han, D., and Lim, J. (2010). - Design and implementation of smart home energy management systems based on ZigBee. IEEE Transactions on Consumer Electronics, 56(3), pp. 1417– 1425.

[41] Hancke, G., Silva, B., and Hancke, G. (2012). - The Role of Advanced Sensing in Smart Cities. Sensors, 13(1), pp. 393–425.

[42] Ibarra, J., González, F., Flores-Rios, B., Burtseva, L., and Astorga, M. (2017) - Tracking the Evolution of the Internet of Things Concept across Different Application Domains. Sensors, 17(6), pp. 1-24.

[43] Jeonggil, A., Dawson, S., Culler, D. E., Hui, J. W., and Levis, P. (2011). - Connecting Low Power and Lossy Networks to the Internet of Things. IEEE Communications Magazine, 49(4), pp. 96–101.

[44] Jiang, J., Liu, Y., and Dezfouli, B. (2018). - A Root-based Defense Mechanism against RPL Blackhole Attacks in Internet of Things Networks. Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC).

[45] Jiang, Y., Zhang, L., and Wang, L. (2013). - Wireless Sensor Networks and the Internet of Things. International Journal of Distributed Sensor Networks, 9(6).

[46] Jorge, E., Ibarra E., Felix F., Gonzalez N., Brenda L., Flores R., Larysa B., and Maria A. (2015). - Internet of Things (IoT): Definitions, Challenges and Recent Research Directions, International Journal of Computer Applications, 128(1), pp.37-47.

[47] Josang, A., Ross H., and Simon P. (2006). - Trust Network Analysis with Subjective Logic. Proceedings of the 29th Australasian Computer Science Conference, 48.

[48] Karlof C., and D. Wagner, (2003). - Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Ad Hoc Networks, 1(2), pp. 293-315.

[49] Kasinathan P., Pastrone C., Spirito M., and Vinkovits M. (2013). – Denial of Service detection in 6LoWPAN based Internet of Things. IEEE 9th Internal Conference Wireless Mobile Computing, Network Communication (WiMob).

[50] Khan R, S. U., and Khan, R. Z. (2012). - Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT), pp. 257–60.

[51] Ko, J., Jeong, J., Park, J., Jun, J.A., Gnawali, O., and Paek, J. (2015) - Dual MOP-RPL: Supporting Multiple Modes of Downward Routing in a Single RPL Network. ACM Transaction Sensor Network (TOSN), 11(39).

[52] Krentz K., Rafiee, H., and Meinel C., (2013) - 6LoWPAN Security: Adding Compromise Resilience to the 802.15.4 Security Sublayer. Proceedings of the International Workshop on Adaptive Security, Zurich.

[53] Krishna, C. S., and Sampath, N. (2017). - Healthcare Monitoring System Based on IoT. 2017 2nd International Conference on IEEE Computational Systems and Information Technology for Sustainable Solution (CSITSS).

[54] Kyriazis, D., Varvarigou, T., Rossi, A., White, D., and Cooper, J. (2013). – Sustainable Smart City IoT Applications: Heat and Electricity Management & Eco-Conscious Cruise Control for Public Transportation. IEEE 14th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM).

[55] Lazarescu, and M. T. (2016). - Wireless Sensor Networks for the Internet of Things: Barriers and Synergies. Components and Services for IoT Platforms, pp. 155–86.

[56] Le A., Loo J., Lasebae A., Aiash M., and Luo Y. (2012). - 6LoWPAN: A Study on QoS Security Threats and Countermeasures using Intrusion Detection System Approach. International Journal Communication System, 25, pp.1189–212.

[57] Liu H., Bolic M., Nayak A., and Stojmenovic I., (2008) - Taxonomy and Challenges of the Integration of RFID and Wireless Sensor Networks. IEEE Network, 22(6), pp. 26–32.

[58] Maalel, N., Natalizio, E., Bouabdallah, A., Roux, P., and Kellil, M. (2013). - Reliability for Emergency Applications in Internet of Things. IEEE International Conference on Distributed Computing in Sensor Systems.

[59] Alzubaidi M., Anbar, M., Chong, Y., and Shadi A., (2018) - Hybrid Monitoring Technique for Detecting Abnormal Behaviour in RPL-Based Network, 13 (5).

[60] Mashal, I., Alsaryrah, O., Chung, T., Yang, C., Kuo, W., and Agrawal, D. (2015) - Choices for Interaction with Things on Internet and Underlying issues. Ad Hoc Networks, 28, pp. 68– 90.

[61] Mayzaud, A., Badonnel, R. and Chrisment, I. (2016). - A Taxonomy of Attacks in RPL based Internet of Things.

[62] Mercy, C., and Renold A. (2014). - Routing Protocol for Low Power Lossy Networks. IEEE International Conference on Advanced Communications, Control and Computing Technologies.

[63] Mitrokotsa, A., and Douligeris, C. (2009). - Integrated RFID and Sensor Networks: Architectures and Applications, RFID and Sensor Networks: Architectures, Protocols, Security and Integrations, pp. 511–35.

[64] Nikravan, M., Movaghar, A., and Hosseinzadeh, M. (2018). - A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks. Wireless Personal Communications, 99(2), pp. 1035–59.

[65] Ning H., and Wang Z. (2011), - Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework. IEEE Communications Letters, 15(4), pp. 461–63.

[66] Noor, M., Binti, M., and Hassan, W. H. (2018). - Current Research on Internet of Things (IoT) Security: A Survey. Computer Networks.

[67] Oliveira, A., and Vazao, T. (2016). - Low-power and Lossy Networks under Mobility: A Survey. Computer Networks, 107, pp. 339–52.

[68] Perazzo, P., Vallati, C., Varano, D., Anastasi, G., and Dini, G. (2018). - Implementation of Wormhole Attack Against a RPL Network: Challenges and Effects. 14th Annual Conference on Wireless on Demand Network Systems and Services (WONS).

[69] Perrey H, Landsmann M, Ugus O, Schmidt TC, and Wahlisch M. (2013) - TRAIL: Topology Authentication in RPL.

[70] Philokypros P., Vassilios G., Ioannis D., and Michael D. (2018). - A Signature-based Intrusion Detection System for the Internet of Things. Information and Communication Technology Forum (ICTF).

[71] Pu, C., and Hajjar, S. (2018). - Mitigating Forwarding Misbehaviors in RPL-based Low Power and Lossy Networks, 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC).

[72] Raza S., Shafagh H., Hewage K., Hummen R., and Voigt (2013). - Lithe: Lightweight Secure CoAP for the Internet of Things, IEEE Sensors Journal 2013, 13(37), pp.11–20.

[73] Riazul Islam, S., Daehan Kwak, M., Hossain, M., and Kyung-Sup K. (2015). - The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 3, pp. 678–708.

[74] Rolf , H., Romana W. (2010) - Internet of Things, Springer, pp. 41-68.

[75] Sabah, S., Pandey, S., and Hong, C. (2018). - Detection of Malicious Node in RPL based Internet of Things through Provenance.

[76] Said, O., and Masud, M. (2013). - Towards Internet of Things: Survey and Future Vision. International Journal of Computer Networks, 5(1), pp. 1–17.

[77] Saled, Y. (2013) - Trust Management system Design for the Internet of Things: A Context-aware and Multi-service approach. Computers & security, 39, pp.361-65.

[78] Savolainen, T., Soininen, J., and Silverajan, B. (2013). - IPv6 Addressing Strategies for IoT. IEEE Sensors Journal, 13(10), pp. 3511–19.

[79] Shafique, U., Khan, A., Rehman, A., Bashir, F., and Alam, M. (2018). - Detection of Rank Attack in Routing Protocol for Low Power and Lossy Networks. Annals of Telecommunications, 73(7), pp. 429–438.

[80] Shahid, R., and Linus, W. (2013) - SVELTE: Real-time Intrusion Detection in the Internet of Things, Ad Hoc Networks (Elsevier), 11(8), pp.2661–74.

[81] Shaikh, R. A., Jameel, H., Auriol, B. J., Lee, H., Lee, S., and Song, Y. (2009). - Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, 20(11), pp. 1698–1712.

[82] Sobral, J., Rodrigues, J., Rabelo, R., Saleem, K., and Furtado, V. (2019). - LOADng-IoT: An Enhanced Routing Protocol for Internet of Things Applications over Low Power Networks.

[83] Sobral, J., Rodrigues, J., Rabelo, R., Filho, J., Sousa, N., Araujo, H., and Filho, R. (2018) - A Framework for Enhancing the Performance of Internet of Things Applications based on RFID and WSNs. Journal of Network Computing Application, 107, pp. 56–68.

[84] Sobral, J., Rodrigues, J., Rabelo, R., Saleem, K., and Furtado, V. (2019). - LOADng-IoT: An Enhanced Routing Protocol for Internet of Things Applications over Low Power Networks, 19, 150.

[85] Sonar, K., and Upadhyay, H. (2016). - An Approach to Secure Internet of Things Against DDoS. In Proceedings of International Conference on ICT for Sustainable Development, pp. 367-376.

[86] Stephen, R., and Arockiam, L. (2018). - E2V: Techniques for Detecting and Mitigating Rank Inconsistency Attack (RInA) in RPL based Internet of Things. Journal of Physics: Conference Series.

[87] Kim, T., Robles, R., and Rosslin J. (2010) - A Review on Security in Smart Home Development. International Journal of Smart Home, 15.

[88] Taghizadeh, S., Bobarshad, H., and Elbiaze, H. (2018). - CLRPL: Context-Aware and Load Balancing RPL for IoT Networks under Heavy and Highly Dynamic Load. IEEE Access, 6, pp. 23277–90.

[89] Talari, S., Shafie, M., Siano, P., Loia, V., Tommasetti, A., and Catalao, J. (2017). - A Review of Smart Cities Based on the Internet of Things Concept. Energies, 10(4).

[90] Tavakoli, A., and Dawson, S. (2009) - Overview of Existing Routing Protocols for Low Power and Lossy Networks. In Internet-Draft draft-ietf-roll-protocols-survey-07, Work in Progress, Internet Engineering Task Force.

[91] Tozlu, S., Senel, M., Wei Mao, and Keshavarzian, A. (2012). - Wi-Fi Enabled Sensors for Internet of Things: A Practical Approach. IEEE Communications Magazine, 50(6), pp. 134–43.

[92] Vasseur, JP., Agarwal, N., Hui, J., Shelby Z., Chauvenet C. (2011) - RPL: The IP routing protocol designed for low power and lossy networks," Internet Protocol for Smart Objects (IPSO).

[93] Wallgren, L., Raza, S., and Voigt, T. (2013). - Routing Attacks and Countermeasures in the RPL-Based Internet of Things. International Journal of Distributed Sensor Networks, 9(8).

[94] Khan, W., and Aalsalem, M. (2011). - Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks. International Journal of Computer Network and Information Security, 1, pp. 1-10.

[95] Whitmore A., Agarwal, A., and Xu, L. (2015) - The internet of Things: A Survey of Topics and Trends," Information Systems Frontiers, 17(2), pp. 261–274.

[96] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., and Alexander, R. (2012) - RPL: IPv6 Routing Protocol for Low Power and Lossy Networks, RFC.

[97] Wu M., Lu, T., Ling, F., Sun, F., and Du, H. (2010). - Research on the Architecture of Internet of Things. International Proceedings of 3rd International Conference on IEEE Advanced Computer Theory and Engineering (ICACTE), 5, pp. 487.

[98] Zheng, Y., Zhang, P., and Athanasios V. (2014) - A survey on Trust Management for Internet of Things" Journal of Network and Computer Applications, 42, pp.120-34.

[99] Yi, J. and Clausen, Y. (2014). - Collection Tree Extension of Reactive Routing Protocol for Low-Power and Lossy Networks. International Journal of Distributed Sensor Network, 10.

[100] Zanella, A., Bui, N., Castellani, A., Vangelista, L., and Zorzi, M. (2014). - Internet of Things for Smart Cities. IEEE Internet Things Journal, 1, pp. 22–32.

[101] Zeng D., Guo S., and Cheng Z. (2011), - The Web of Things: A Survey, Journal of Communications, 6(6), pp. 424–438.

[102] Zhang, C., and Green, R. (2015). - Communication Security in Internet of Thing: Preventive Measure and avoid DDoS Attack over IoT Network, Proceedings of 18th Symposium on Communications & Networking, pp. 8-15.

List of Publication

International Journals

Accepted/Published

1. **Vidhu Kiran**, Shaveta Rani **,** and Paramjeet Singh,"Multi Level Trust Based Secure RPL against Selective Forwarding Attack detection in IoT," Sylwan, 163(2), Feb. 2019.

2. **Vidhu Kiran**, Shaveta Rani **,** and Paramjeet Singh, "Trust Based Defence System for DDoS Attack Detection in RPL over IoT," International Journal of Computer Science and Network Security (IJCSNS),18(12), pp. 239-245, Dec. 2018.

3 **Vidhu Kiran**, Shaveta Rani**,** and Paramjeet Singh, "Trust Based Selective Forwarding Attack Detection in RPL over IoT," International Journal of Research and Analytical Reviews, 6(11), pp. 434-441, Jan. 2019.

4. Vidhu Kiran, Shaveta Rani **,** and Paramjeet Singh,"Towards a Light Weight Routing Security in IoT using Non-Cooperative Game Models and Dempster-Shaffer Theory," Wireless Personal Communication, Sept, 2019.