Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Simulation of Novel AI Technique for IoT Security

Pardeep Kumar[1], Dr. Amit Gupta[2]

Research Scholar[1], Assistant Professor[2,] ECE Department
IKGPTU, Jalandhar, Punjab, India
Sharmaashupk@gmail.com

Article Info
Page Number: 10730-10743
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received:
15 September 2022
Revised: 25 October 2022
Accepted: 14 November 2022
Publication: 21 December 2022

Abstract
The Internet of Things (IoT) is quickly becoming a hot topic in the academic world. More and more devices are becoming internet-enabled, elevating the importance of IoT in people's day-to-day lives. In this paper, we take a look at how the Artificial neural network (ANN)-based supervised machine learning solution for attack detection can be the remedy for Intrusion Detection. If the rogue nodes can be identified in time, the network can be protected from the attack's devastating repercussions. Parameter adjustment has resulted in optimal values for the hyperparameters. This paper's model successfully identified each of the aforementioned attacks concurrently and separately. In addition to precision, this analysis considered recall, F1, and the Mathews correlation coefficient (MCC).
Keywords: -Internet of Things, Security, AI,

Introduction

There were limited options for communication between patients and doctors prior to the advent of the Internet of Things. It would be impossible for hospitals and doctors to constantly assess patients' conditions and provide advice.

As part of the Internet of Things (IoT), connected medical devices enable remote monitoring, improving patient safety and allowing for more effective treatment. As communication with doctors has become more streamlined and hassle-free, patient participation and satisfaction have increased. Long-term hospital stays can be cut short and unnecessary readmissions avoided with the use of remote patient monitoring. By connecting medical devices and other systems, IoT can both lower costs and boost the effectiveness of healthcare.

Redefining health care

The market potential for IoT solutions with a focus on healthcare is enormous. Health care could be significantly impacted by the information collected from these interconnected gadgets. The four-part structure of the Internet of Things (See Figure 1). Because of this interconnectedness between the four stages, information gathered or processed at any given phase can be used in subsequent ones. Opportunity and insight are increased when a company's values are fully integrated.

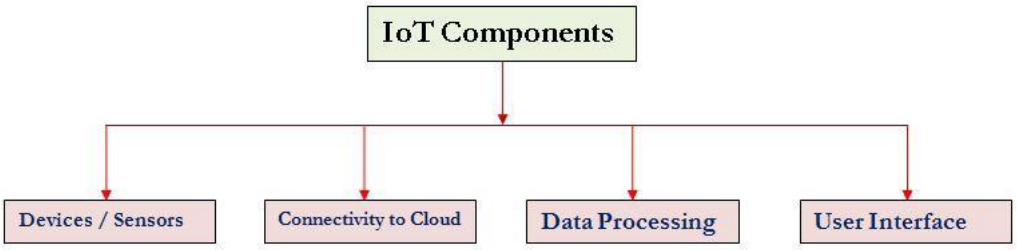

Figure 1: IoT Components

First, equipment such as sensors, actuators, monitors, detectors, cameras, etc., must be set up. That's because they're information gatherers.

Second, digital representations of the analog sensor and device data must be gathered and processed.

After data is digitized and aggregated, it is preprocessed, standardized, and sent to a data center or the Cloud.

Four, control and examine the completed data. Successful business decisions are aided by the actionable insights provided by advanced analytics.

The current state of IoT security is inadequate to protect against the growing number of cyber threats targeting IoT devices and networks. IoT devices are vulnerable to attack due to their lack of security protocols, as well as their limited computing power and memory. As the number of IoT devices grows, so does the attack surface and the potential for malicious actors to exploit these devices.

AI can be used to address this issue by providing a more robust level of security for IoT networks. AI-based security solutions can detect and prevent malicious activities, identify potential vulnerabilities, and respond to potential threats in real-time. These solutions can also be used to monitor and analyze network traffic to detect anomalies and suspicious behavior.

Related Work:

Literature Review:

Security for the Internet of Things (IoT) is an area where several researchers have made reports. Each contributor has contributed something unique to the discussion of the Internet of Things security, and those contributions are listed below. The goals of the design and the routing requirements of the protocol were illustrated in a review of RPL by Gaddour et al. [12]. Energy usage, latency, and data loss have all been analyzed to gauge this protocol's performance. Many intrusion detection systems and mitigation strategies, as well as a review of attacks applicable to RPL, were provided by Pongle et al. [13]. This disconnect between existing smart house utilities and their integration into IoT networks was brought to light by

Biljana et al. [14]. Additionally, a comprehensive model for various smart objects in a cloud-oriented IoT scenario has been proposed. Machine learning (ML) techniques for Internet of Things (IoT) data analysis were described by Mahdavinejad et al. [15]. For smart cities, many ML approaches have been analyzed to determine which ones are most effective at fixing data-related problems in the Internet of Things. For the first time, both the benefits and drawbacks of using ML algorithms to analyze IoT data are clear. In their explanation of a survey on intrusion detection in the IoT, Zarpelao et al. [16] highlighted major trends, unresolved issues, and prospects for future study. Khan et al. [17] presented research into vulnerabilities in IoT infrastructure. Security needs, obstacles, safety concerns, and blockchain support have all been specified. For the purpose of identifying attacks in the IoT, Costa et al. [18] offered an evaluation of IDS strategies based on machine learning. Many potential dangers in the Internet of Things setting were examined in this analysis. Attacks were categorized by Sengupta et al. [19] based on the vulnerabilities of the items and the various tiers of generalized IoT architecture. Resources, topology, and traffic were the primary areas of inquiry for the RPL attacks presented by Verma et al. [20]. In particular, protective measures against RPL in the network layer have been laid out in detail. A comprehensive overview of RPL attack mitigation strategies was provided by Avila et al. [21]. The investigation here has concentrated on the supervision of networks, the selection of parental nodes, and authentication. A study of RPL in terms of available resources, network topology, traffic, and various attacks was presented by Almusaylim et al. [22]. Destination-oriented directed acyclic graph (DODAG) construction was the focus of Simha et al.'s [23] research into RPL and the Contiki operating system. Contiki and Cooja's suitability for RPL implementation has been discussed.

Attacks and Mitigation Schemes

The next part details researchers' assaults and mitigation measures. Wallgren et al. [24] showed many security threats on RPL-based IoT networks. A lightweight heartbeat protocol protects against potential attackers. Sehgal et al. [25] analysed DODAG inconsistency attacks and their consequences. Mayzaud et al. [26] studied DODAG version attacks. Attacks increased overhead by 18%, doubled delay, and lowered delivery ratio by 30%. Mayzaud et al. [27] researched on topological inconsistency attack mitigation. Mayzaudet al.[28] clarified RPL naming conventions, research, and countermeasures. Ahmed et al. [29] describe two methods for avoiding blackhole attacks. Thanigaivelan et al. [30] recently described a distributed Internet of Things anomaly detection approach. Network fingerprinting is used to detect topological alterations. Aris et al. [31] studied version number attacks in RPL-based IoT networks, focusing on fixed and mobile nodes of different criticality. Diro et al. [32] shown deep learning's value in spotting threats. Perazzo et al. [33] researched wormhole attacks in IEEE 802.15.4 sensor networks. Jyothisreeet al.[34] reported blackhole and version number attacks. Both types of assaults have detection and preventive techniques. Ahutu et al. [35] suggested a MAC-centralized routing protocol to ecentral WSN worm-hole attacks (MCRP). Sahay et al. [36] illustrated increased version attacks with sky motes and measured legitimate and malicious node energy usage. Pu et al. [37] analysed Sybil attacks on RPL-based IoT networks and suggested defences. SMLC for intrusion detection. SMLC highlighted partially labelled data learning and performance.

Intrusion Detection Schemes

Multiple intrusion IDS have been proposed by researchers. New instruction detection for RPL assaults was provided by Raza et al. [38] using the SVELTE method. Attacks such as spoofing, sinkholes, and selective forwarding routing are all spotted by these IDS systems. Attacks have not been 100% successful in their detection, though. In reference [39, 40], an improved IDS was developed for detecting a denial-of-service attack in networks based on 6LoWPAN. The IDS was built by Kasinathan et al. [39] using the ebbits network model, and it was tested using a penetration testing method to ensure its accuracy. But the important statistics for issues including the type of detection method, characteristics, and deployed agents were provided by Rghioui et al. [40]. In [41], Pongle et al. described a method for detecting intrusion and wormhole attacks in the Internet of Things in real-time. Using the node's neighbor information, this model detected the wormhole assault and the attacker. The given model consumes low amounts of power and a constant number of UDP packets when performing attack recognition. When it comes to the Internet of Things (IoT) security, Sheikhan et al. [42] detailed a hybrid IDS that makes use of the MapReduce policy. Mediating agents have made it possible to distinguish anomalies and misuse. When an internal attack occurs, an unsupervised optimal path forest (OPF) approach is used to determine the source. A specification-based intrusion detection system (IDS) was proposed by Le et al. [43]. This IDS was inspired by a profiling technique that creates a summary of network events at a high level to verify node actions. The presented IDS was able to identify RPL topological assaults in the simulation. When it comes to detecting intrusions, Jarrah et al. [44] discussed a semi-supervised multilayered clustering model (SMLC). This study compared the SMLC's performance to that of the tri-training, random forest, bagging, and AdaboostM1 models, all of which were found to be superior at learning from partially labeled data. With only 80% of the training data labeled, SMLC was able to achieve the same level of detection accuracy as tri-training. Four different kinds of ANN models were analyzed by Lee et al. [45] and compared to the multinomial logit model (MNL) in terms of their ability to make accurate predictions. Hold-out and tenfold cross-validation, as well as sensitivity analysis, have been used to assess the predictive efficacy of four ANNs. Through a multilayer perceptron, Anitha et al. [46] analysed an artificial neural network (ANN)-based intrusion detection system (ANNIDS) for Internet of Things (IoT) networks (MLP). These IDS were mostly concerned with detecting DIS attacks and versions attacks. In order to detect wormhole attacks in RPL-based IoT, Bhosale et al. [47] suggested an intrusion detection system that relies on the critical metric RSSI (received signal strength indicator). This defence mechanism has been implemented to prevent wormhole attacks by balancing the two main types of security measures, ecentraliz and ecentralized. About 90% of the assault was spotted. For three common RPL attacks, Kfoury et al. [48] introduced an IDS based on self-organizing maps (SOM). SOM has been applied to categorical problems as an unsupervised machine learning approach. The expected IDS used a visual representation of a map to classify the varied RPL attacks. To study the effects on cyber-physical systems, Sharma et al. [49] simulated four different RPL attacks. With a random forest classifier, the proposed model accurately predicted and classified the four attacks 99.33% of the time. A new two-part design, involving threshold modulation and attack detection, was presented by Qureshi et al. [50]. With the current architecture in place,

we can successfully identify four distinct RPL assaults. Higher delivery rates with lower latency and packet loss were found in simulations.

Artificial Neural Networks

Scientists have proposed alternative intrusion IDSs. Raza et al. [38] used SVELTE to detect RPL assaults. IDS can detect spoofing, sinkholes, and selective forwarding routing. Attacks are usually detected, but not always. Better IDS was built to detect DoS attacks on 6LoWPAN networks (references [39, 40]). Kasinathan et al. [39] built the IDS using the ebbits network model and tested it through penetration testing. Rghioui et al. [40] provided statistics on detection methods, agent characteristics, and deployment. Pongle et al. [41] reported a strategy for real-time infiltration and wormhole assaults in IoT. This approach identified the attacker by studying the node's neighbours. The model employs a consistent quantity of UDP packets and little power during attack recognition. Sheikhan et al. [42] presented an IoT-protecting hybrid IDS that uses MapReduce. With intermediates, abnormalities and misuse can be identified and addressed. Unsupervised OPF is used to trace an inside attack. Le et al. [43] recommended a specification-based IDS. This IDS was inspired by a method of ecentral network events to validate node actions. The simulation IDS detected RPL topological assaults. Jarrah et al. [44] discussed semi-supervised multilayered clustering for intrusion detection. (SMLC). In this paper, the SMLC's performance was compared against tri-training, random forest, bagging, and AdaboostM1 models, all of which were superior at learning from partially labelled data. SMLC matched tri-detection training's accuracy ecentral only 80% of labelled training data. Lee et al. [45] compared four ANN models to the multinomial logit model (MNL). Four ANNs were assessed using hold-out, tenfold, and sensitivity cross-validation. Anitha et al. [46] studied an ANN-based intrusion detection system for IoT networks (MLP). These IDS focused on DIS and version attacks. Bhosale et al. [47] suggested an RSSI-based IoT wormhole intrusion detection system (received signal strength indicator). This protection mechanism balances ecentraliz and ecentralized security to prevent wormhole attacks. The attack was uncovered 90%. Kfoury et al. [48] presented a self-organizing-maps-based IDS for RPL assaults (SOM). Categorical unsupervised machine learning uses SOM. The imagined IDS grouped RPL attacks by map. Sharma et al. [49] simulated four RPL assaults on cyber-physical systems. The suggested model used a random forest classifier, which classified the four attacks with 99.33% accuracy. Qureshi et al. [50] introduced a two-part architecture with threshold modulation and attack detection. Current infrastructure can identify four RPL attacks. Simulations showed improved delivery rates, decreased latency, and packet loss. Number of classes needed to accurately classify dataset instances. Varied challenges may require a different number of hidden layers. Each unit-to-unit relationship is valued. This measures the original unit's force.

Proposed ANN-Based IDS

To detect the three security assaults depicted in Fig. 2, this section details the ANN-based system proposed for doing so. The Cooja [56] simulator is included in the Contiki [55] OS. Then, the three security attacks—hello flood, raised version and decreased rank attack—are implemented using the RPL assaults framework [57]. All nodes' estimated energy usage is

calculated using the Cooja simulator's power tracker module. There are four distinct ways in which each node consumes energy: "ON" (idle but powered), "TX" (transmitting data), "RX" (receiving data), and "INT" (entering or leaving a network) (interference). These four measurements are normalized to the node's vitality. This is done so that the relative energy usage of each node may be calculated. When running a simulation, the RPL assaults framework generates DODAG graphs, graphs of power usage, and packet capture files. The outputs of the RPL assaults framework accurately depict how the network operates with and without the attack. To begin, Cooja simulations are run for each of the three attacks independently. The next step is to run a simulation while simultaneously launching all of the attacks. The packet capture files (pcap) are then converted to comma-separated values (csv) using the Wireshark program after the necessary simulations have been run. Spyder is used to import these CSV files into a Python data frame. After that, the python data frame undergoes preprocessing in preparation for the ANN's training and testing phases. The preparation stage entails addressing any gaps in the data, extracting any necessary features, and standardizing the information. In addition, the dataset is used for training and testing the ANN model's ability to detect attacks. Through weight modification via backpropagation, the training optimizes the final model. The testing phase involves validating the trained model's ability to accurately detect attacks. Both the hold-out and k-fold cross-validation techniques are used to determine how accurate the predicted model is.

Parameter tuning is used to fine-tune the ANN learning hyperparameters. ANN is trained using the following assumptions about the sizes of the input, hidden, and output layers: p, q, and r. This suggests that the number of components in each layer can vary.

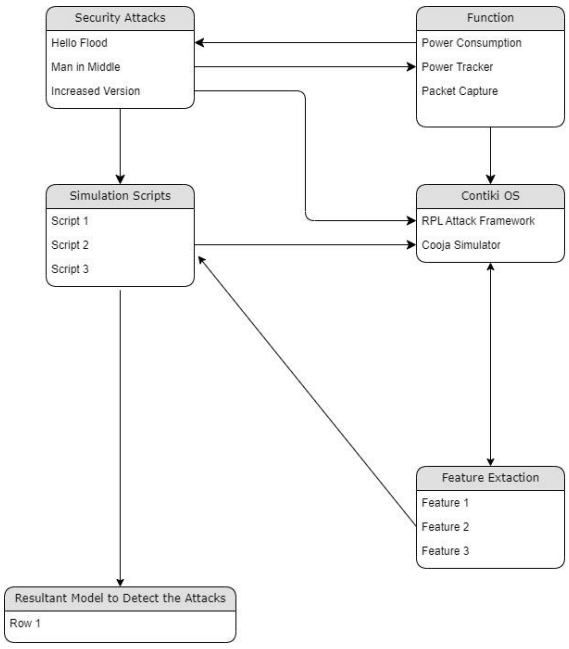

Figure 2: Simulation Model

ANN Based Solution for Security exploits

This section describes the ANN-based approach for detecting Figure 2's three security exploits. Contiki [55]'s initial configuration includes Cooja [56]. Hello flood, raised version, and decreased rank attack are implemented using the RPL assaults framework [57]. Cooja's power tracker module estimates node energy usage. Each node utilises energy in four ways: ON, TX, RX, and INT (interference). All four indicators are based on a node's health. This calculates each node's energy usage. During simulation, RPL assaults generates DODAG, power, and packet capture files. All RPL attacks framework outputs show network behaviour during an attack. First, three Cooja simulations are run. Next, all attacks are simulated in parallel. Wireshark transforms packet capture files (pcap) into csv after simulations. Spyder converts CSV files into a Python data frame. The Python data frame is then ready for ANN training and testing. Preprocessing includes missing data, feature extraction, and data normalisation. ANN is trained and assessed using the dataset to detect assaults. Backpropagation modifies model weights during training. The testing verifies the trained model's capacity to detect attacks accurately. Hold-out and k-fold cross-validation evaluate the projected model's accuracy.

Tuning maximises ANN learning hyperparameters. Figure 3's ANN has p, q, and r input, hidden, and output units. This shows that layer counts may be different.

Results and discussions

This section displays the outcomes of the four simulation scenarios. Individual hello flood simulation is Scenario 1. Scenarios 2 and 3 simulate Man in Middle and Increased Version, respectively. Scenario 4 included all three attacks simultaneously. Figure 3 illustrates the network configurations for scenarios 1, 2, 3, and 4.

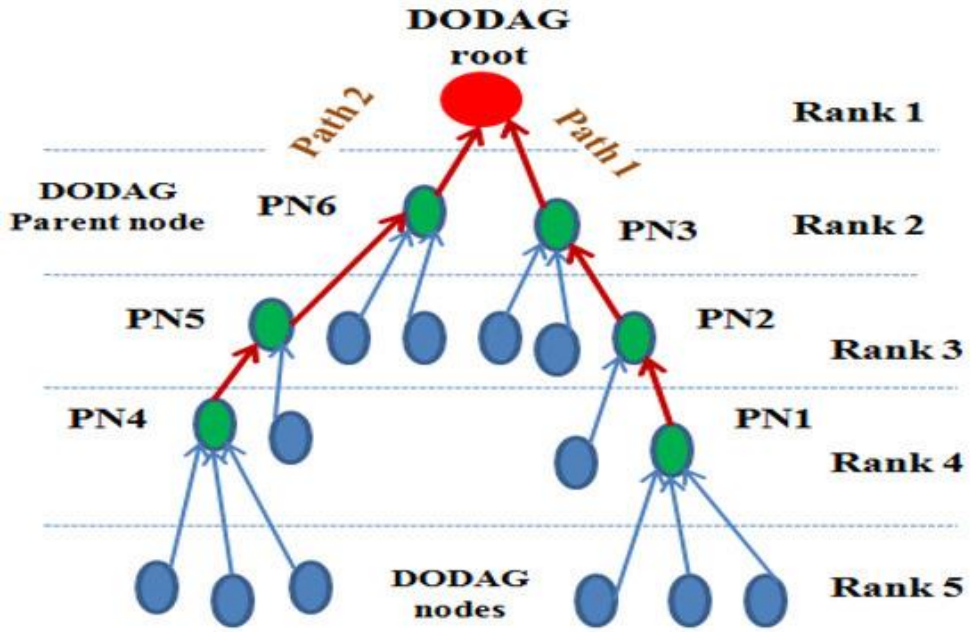

Figure 3: Network Configuration

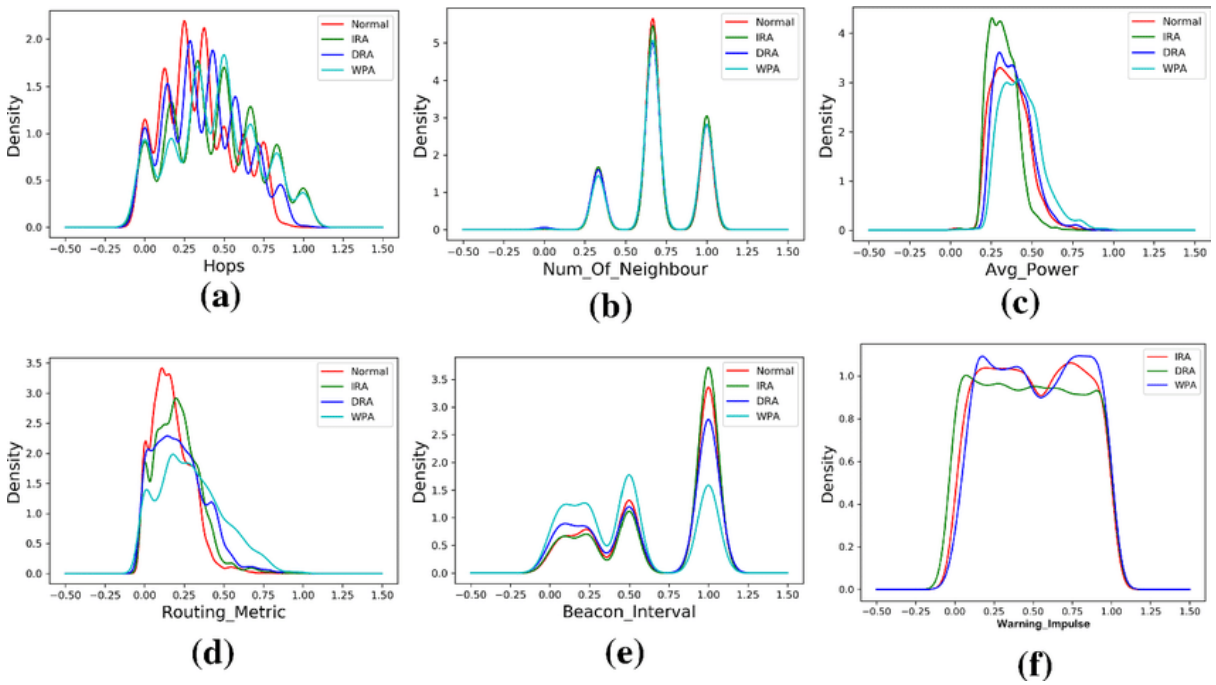

Figure 4: Characteristics of Network

Figure 4 displays the Network configuration. Figure 4a, b, and c represent, Hops, Num of Neighbor and Avg_power for scenarios 1, 2, 3, and 4. Fig 4 d, e and f represent the timings of the Routing Metric, Beacon Interval and Warning Impulse.

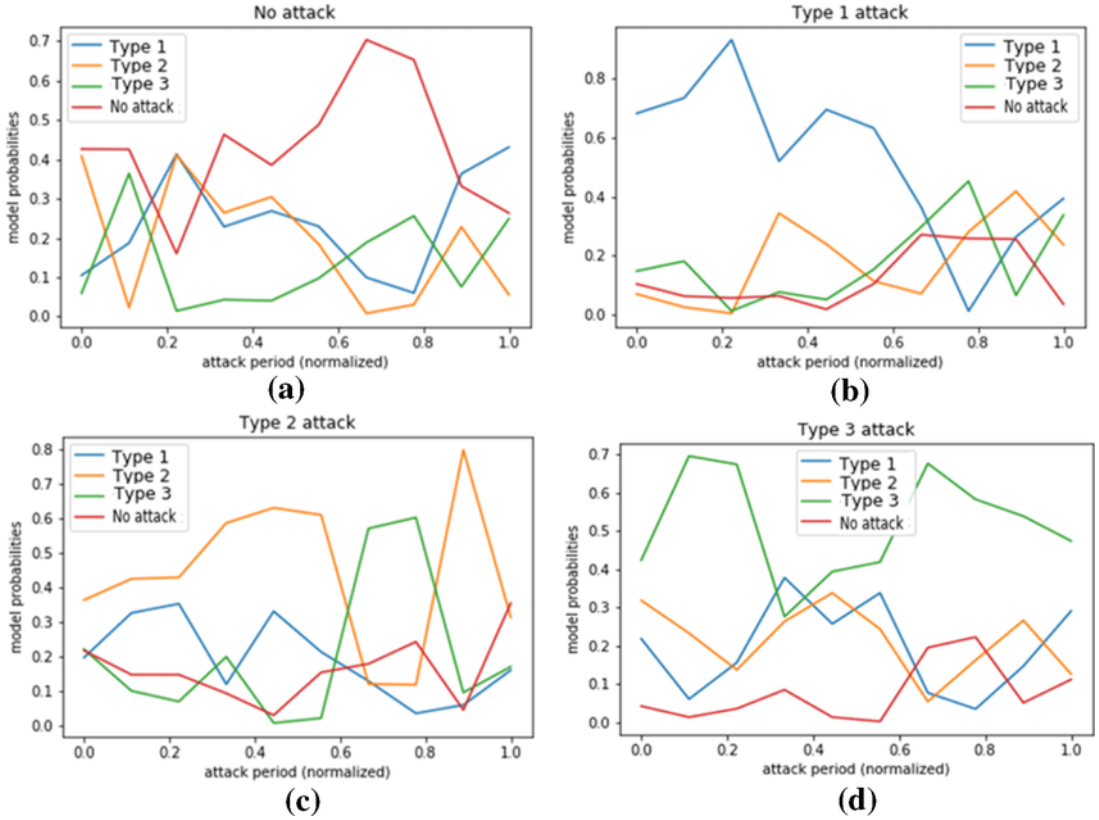

Fig 5, Energy Levels

As depicted in Figure 5a, the hello flood malicious node spends the greatest energy. It increases the neighbors' electricity consumption. Figure 5b illustrates how the fraudulent node in Scenario 2 leads other nodes to consume more electricity. In case 3, as depicted in Figure 5c, the fake node has no influence on network power consumption. Figure 5d demonstrates that all attacks impact the power consumption of the nodes.

Number is the serial number of the packet and is used to index the dataframe. The 'Time' and 'Length' parameters represent the time and size of a packet. Four qualities are qualitative independent variables. Source and Destination define the source and destination IP addresses, respectively. Protocol displays the pertinent protocol, whereas Info represents metadata. An output-dependent variable differentiates fraudulent and ordinary packets.

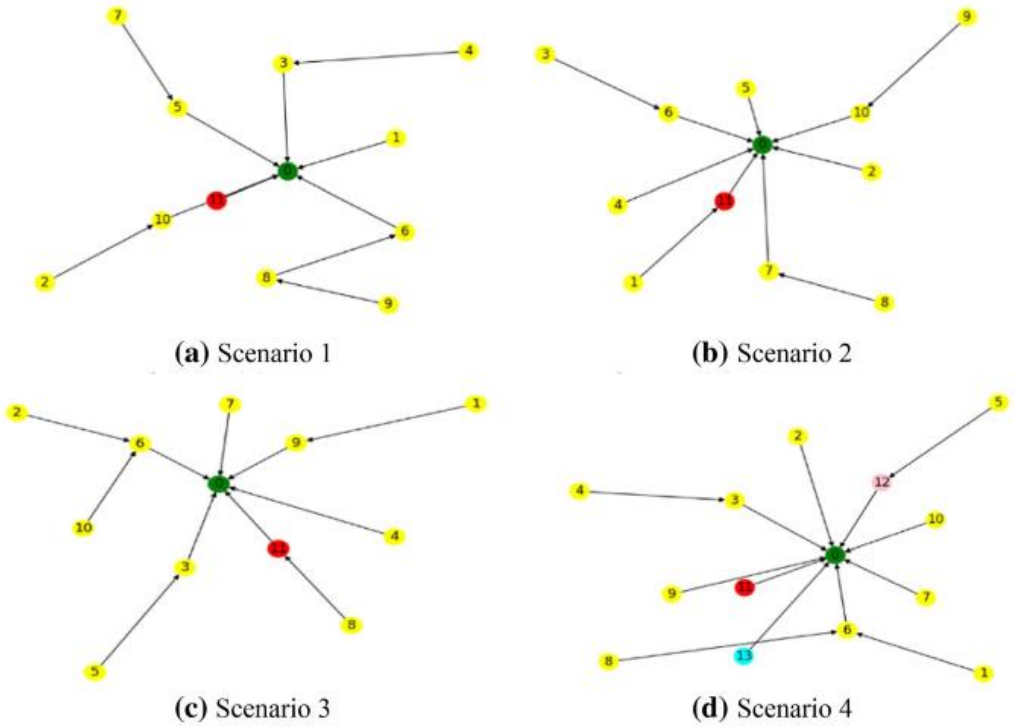

Figure 6 DODAG Graphs generated in each scenario

Figure 6 indicates that false nodes generate the most packets during a hello flood assault. Malicious nodes generate many DIS messages as opposed to only one. In the improved version of the attack, malicious nodes encourage other nodes to generate additional packets. This occurs as a result of the deceitful node initiating global DODAG repairs. The misleading node of a lower-rank assault transmits the fewest packets. Due to this, attacks with a low rank do not do damage to the network. It is capable of eavesdropping on downward DODAG node transmission. All nodes in scenarios 1, 2, 3, and 4 generated 38,365, 50,414, 28,376, and 53,684 packets, as depicted in Figure 6. Due to late source or destination information, ACK packets are omitted in the packet capture. In scenarios 1, 2, and 3, malicious nodes transmit a total of 15,508, 2672, and 630 packets, respectively. Scenario 4 false nodes generate 12,790, 3559, and 2342 packets, respectively, for hello flood, increased version, and decreased rank attacks.

ANN has data that has been preprocessed. The proposed ANN included hidden, input, and output layers. Adding additional hidden layers does not increase the performance of the model. In the first three instances, the output layer only has a single unit due to fraudulent and legitimate packets. The fourth scenario contains four outcomes. One is for no assault and three are for each attack. Scenario 4 contains four output units. Similarly, the input layer unit count for each scenario was optimized. Similar to case 1, 'Protocol' only has one value. There are currently only three category variables in the dataset. There are 12, 9, and 12 observations for 'Source,' 'Destination,' and 'Info,' correspondingly.

Conclusion

In this study, supervised machine learning was utilized to identify three phenomena: hello flood, Mam In Middle, and Increased Version. Artificial neural networks and machine learning are used in this study. Three security attacks across four scenarios were utilized to illustrate this topic. Individual assaults were used in the first three scenarios. Every single one of them is based on the fourth simulation scenario. It has been demonstrated through simulations that security attacks have an impact on the DODAG graph, energy consumption, and traffic production. The malicious hello flood node generates the greatest traffic.

Points of connection in a network Although it has no effect on the DODAG building, it increases energy expenses for nearby residents. The false node has effects on DODAG and energy consumption, just like the upgraded version attack. This occurred because of the presence of other network nodes, which generate more packets than the original network. The fake node in a ranked-down attack broadcasts the fewest messages. Effective for spying and decreasing DODAG. A program based on artificial neural networks was able to spot the threats in each scenario.

The proposed model achieves optimal results in terms of accuracy, recall, F1, and the Matthews correlation coefficient (MCC). Modifying parameters improves performance by maximizing batch size, epochs, and the optimizer.

Future Scope

The integration of AI and IoT is a powerful tool for mitigating security risks. AI can effectively monitor and detect any suspicious activities, and can quickly respond to security threats. This can help businesses protect sensitive data, maintain compliance, and reduce the cost of responding to security incidents. Additionally, AI can be used to automate security processes such as patching, vulnerability remediation, and access control. Furthermore, AI can be used to further enhance the security of IoT networks by monitoring network traffic and identifying malicious activities. As IoT technology continues to grow and evolve, AI will play an increasingly important role in providing secure and reliable IoT solutions.

References

[1.] Lee I, Lee K (2015) The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus Horiz 58(2015):431–440

[2.] Chen S, Xu H, Liu D, Hu B, Wang H (2014) A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective. IEEE Int Things J 1(4):349–359

[3.] Purri S, Choudhury T, Kashyap N, Kumar P (2017) "Specialization of IoT applications in health care industries", International Conference on Big Data Analytics and Computational Intelligence (ICBDACI), pp. 1–5

[4.] Botta A, Donato WD, Persico V, Pescape A (2016) Integration of cloud computing and internet of things: a survey. FuturGenerComputSyst 56:684–700

[5.] Singh S, Verma VK, Pathak NP (2015) Sensors augmentation influence over trust and reputation models realization for dense wireless sensor networks. IEEE Sens J 15(11):6248–6254

[6.] Verma VK, Singh S, Pathak NP (2015) Optimized battery models observations for static, distance vector and on-demand based routing protocols over 802.11 enabled wireless sensor networks. Wireless PersCommun 81(2015):503–517

[7.] Verma VK, Singh S, Pathak NP (2016) Analytical event-based investigations over delphi random generator distributions for data dissemination routing protocols in highly dense wireless sensor network. Wireless PersCommun 87(2016):1209–1222

[8.] Verma VK (2017) Pheromone and path length factor-based trustworthiness estimations in heterogeneous wireless sensor networks. IEEE Sens J 17:215–220

[9.] Verma VK, Singh S, Pathak NP (2017) Towards comparative evaluation of trust and reputation models over static, dynamic and oscillating wireless sensor networks. Wireless Netw 2017:1–9

[10.] Verma VK, Ntalianis K, Singh S, Pathak NP (2018) Data proliferation based estimations over distribution factor in heterogeneous wireless sensor networks. ComputCommun 124:111–118

[11.] Kawamoto D (2017) "IoT security incidents rampant and costly", https://www.darkreading.com/vulnerabilities---threats/iot-security-incidents-rampant-and-costly/d/d-id/1329367, pp. 1–9

[12.] Gaddour O, Koubaa A (2012) RPL in a nutshell: a survey. ComputNetw 56(14):3163–3178

[13.] Pongle P, Chavan G (2015) A survey: attacks on RPL and 6LoWPAN in IoT. IntConf Pervasive Comput (ICPC) 2015:1–6

[14.] Biljana L, Risteska S, Kire TV (2017) A review of internet of things for smart home: challenges and solutions. J Clean Prod 140(2017):1454–1464

[15.] Mahdavinejad MS, Rezvan M, Barekatain M, Adibi P, Barnaghi P, Sheth AP (2017) "Machine learning for internet of things data analysis: a survey", Dig Commun Netw-2017, pp. 1–56

[16.] Zarpelão BS, Miani RS, Kawakani CT, Alvarenga SCD (2017) "A survey of intrusion detection in internet of things", J Netw Comput Appl-2017, pp. 1–46

[17.] Khan MA, Salah K (2018) IoT security: review, blockchain solutions, and open challenges. Future Gen ComputSyst 82(2018):395–411

[18.] Costa KAPD, Papa JP, Lisboa CO, Munoz R, Albuquerque VHCD (2019) Internet of things: a survey on machine learning-based intrusion detection approaches. ComputNetw 151(2019):147–157

[19.] Sengupta J, Ruj S, Bit SD (2019) A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J NetwComputAppl 2019:1–51

[20.] Verma A, Ranga V (2020) "Security of RPL based 6LoWPAN networks in the internet of things: a review", IEEE Sens J-2020, pp. 1–24

[21.] Avila K, Jabba D, Gomez J (2020) "Security aspects for Rpl-based protocols: a systematic review in IoT", Appl Sci-2020, pp. 1–20

[22.] Almusaylim ZA, Alhumam A, Jhanjhi NZ (2020) Proposing a secure RPL based internet of things routing protocol: a review. Ad Hoc Netw 101(2020):1–17

[23.] Simha SNV, Mathew R, Sahoo S, Biradar RC (2020) "A review of RPL protocol using contiki operating system", Proceedings of the Fourth International Conference on Trends in Electronics and Informatics (ICOEI 2020), pp 259–264

[24.] Wallgren L, Raza S, Voigt T (2013) "Routing attacks and countermeasures in the RPL-based internet of things", Int J Dist Sens Netw-2013, pp 1–11

[25.] Sehgal A, Mayzaud A, Badonnel R, Chrisment I, Schönwälder J (2014) "Addressing DODAG inconsistency attacks in RPL networks", Proc. of GIIS Conference, pp 1–8

[26.] Mayzaud A, Sehgal A, Badonnel R, Chrisment I, Schonwalder J (2014) "A study of RPL DODAG version attacks," in AIMS'14 Springer, pp 92–104

[27.] Mayzaud A, Sehgal A, Badonnel R, Chrisment I, Schönwälder J (2015) Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks. Int J Net Manag. https://doi.org/10.1002/nem.1898

[28.] Mayzaud A, Badonnel R, Chrisment I (2015) A taxonomy of attacks in RPL-based internet of things. Int J Netw Sec 18(3):459–473

[29.] Ahmed F, Ko YB (2016) Mitigation of black hole attacks in routing protocol for low power and lossy networks. Sec CommNetw 9(18):1–27

[30.] Thanigaivelan NK, Nigussie E, Kanth RK, Virtanen S, Isoaho J (2016) "Distributed internal anomaly detection system for Internet-of-Things", 13th IEEE Annual Consumer Communications Networking Conference (CCNC), pp.319–320

[31.] Aris A, Oktug SF, Yalcin SBO (2016) "RPL version number attacks: In-depth study", 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016), pp. 776–779

[32.] Diro AA, Chilamkurti N (2018) Distributed attack detection scheme using deep learning approach for Internet of Things. FuturGenerComputSyst 82(2018):761–768

[33.] Perazzo P, Vallati C, Varano D, Anastasi G, Dinni G (2018) "Implementation of a wormhole attack against a RPL network: challenges and effects", 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), pp 95–102

[34.] Jyothisree MVR, Sreekanth S (2019) "Attacks in RPL and detection technique used for internet of things", Int J Recent Technol Eng (IJRTE) ISSN: 2277–3878, 8(1) 1876–1879

[35.] Ahutu OR, El-Ocla H (2020), “Centralized routing protocol for detecting wormhole attacks in wireless sensor networks”, IEEE Access 8 pp. 63270–63282

[36.] Sahay R, Geethakumari G, Mitra B, Sahoo I (2020) “Efficient framework for detection of version number attack in internet of things”, Abraham A., Cherukuri A., Melin P., Gandhi N. (Eds) Intelligent systems design and applications (ISDA 2018). Advances in Intelligent Systems and Computing (AISC 941), pp. 480–492

[37.] Pu C (2020) Sybil attack in RPL-based internet of things: analysis and defenses. IEEE Int Things J 7(6):4937–4949. https://doi.org/10.1109/JIOT.2020.2971463

[38.] Raza S, Wallgren L, Voigt T (2013) SVELTE: Real-time intrusion detection in Internet of Things. Ad Hoc Netw 11(2013):2661–2674

[39.] Kasinathan P, Pastrone C, Spirito MA, Vinkovits M (2013) "Denial-of-Service detection in 6LoWPAN based internet of things.", Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on. IEEE, pp. 600–607

[40.] Rghioui A, Khannous A, Bouhorma M (2014) Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition. J AdvComputSciTechnol 3(2):143

[41.] Pongle P, Chavan G (2015) Real Time Intrusion and Wormhole Attack Detection in Internet of Things. Int J ComputAppl 121(9):1–13

[42.] Sheikhan M, Bostani H (2016) “A hybrid intrusion detection architecture for internet of things”, 8th International Symposium on Telecommunications, IEEE, pp 601–606

[43.] Le A, Loo J, Chai KK, Aiash M (2016) A specification-based IDS for detecting attacks on RPL-based network topology. Information 7(2):1–19

[44.] Jarrah OYA, Hammdi YA, Yoo PD, Muhaidat S, Qutayri MA (2017) “Semi-supervised Multi-Layered Clustering Model for Intrusion Detection”, Digital Communications and Networks, pp. 1–12

[45.] Lee D, Derrible S, Pereira FC (2018) “Comparison of four types of artificial neural network and a multinomial logit model for travel mode choice modeling”, transportation research board-2018, pp.1–12

[46.] Anitha AA, Arockiam L (2019) “ANNIDS: artificial neural network based intrusion detection system for internet of things”, Int J Innov Technol ExplEng (IJITEE) ISSN: 2278–3075, 8(11), 2583–2588

[47.] Bhosale SD, Sonavane SS (2019) “A real-time intrusion detection system for wormhole attack in the rpl based internet of things”, The 12th International Conference Interdisciplinarity in Engineering, Procedia manufacturing 32, 840-847

[48.] Kfoury E, Saab J, Younes P, Achkar R (2019) A self organizing map intrusion detection system for rpl protocol attacks. Int J InterdisTelecommunNetw 11(1):30–43

[49.] Sharma M, Elmiligi H, Gebali F, Verma A (2019) “Simulating attacks for RPL and generating multi-class dataset for supervised machine learning”, 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 20-26

[50.] Qureshi KN, Rana SS, Ahmed A, Jeon G (2020) A novel and secure attacks detection framework for Smart Cities Industrial Internet of Things. Sustain Urban Areas 2020:1–33

[51.] Sharma S, Verma VK (2020) Security explorations for routing attacks in low power networks on internet of things. J Supercomput 2020:1–35

[52.] Thubert P (2012) "Objective function zero for the routing protocol for low-power and lossy networks (RPL)", RFC 6552; IETF Secretariat: Fremont, CA, USA, pp. 1–14

[53.] Gnawali O, Levis P (2012) "The minimum rank with hysteresis objective function", RFC 6719; IETF Secretariat: Fremont, CA, USA, pp. 1–13

[54.] Jain AK, Mao J, Mohiuddin KM (1996) "Artificial neural networks: a tutorial", Computer, 29(3), pp. 31–44

[55.] Dunkels A, Gronvall A, Voigt T (2004) "Contiki–a lightweight and flexible operating system for tiny networked sensors". 29th Annual IEEE International Conference on Local Computer Networks (LCN'04), IEEE Computer Society, pp. 455–462

[56.] Sterlind FO, Dunkels A, Eriksson A, Finne J, Voigt T (2006) "Cross-level sensor network simulation with Cooja", IEEE 31st Conference on Local Computer Networks, LCN '06, IEEE Computer Society, pp. 641–648.

[57.] Hondt AD, Bahmad H, Vanhee J (2016) "RPL attacks framework", mobile and embedded computing LINGI2146 Report, pp.1–14

[58.] Hendrawan INR, Arsa IGNW (2017) "Zolertia Z1 energy usage simulation with Cooja simulator", Informatics and Computational Sciences (ICICoS) 2017 1st International Conference on, pp. 147–152

[59.] Chicco D, Jurmaan G (2020) The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. BMC Genomics 21:6. https://doi.org/10.1186/s12864-019-6413-7

[60.] Hussain F, Hussian R, Hassan SA, Hosssain E (2020) Machine learning in IoT security: current solutions and future challenges. IEEE CommunSurv Tutor 22(3):1686–1721