Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 165 (2019) 565–572

Procedia Computer Science

www.elsevier.com/locate/procedia

INTERNATIONAL CONFERENCE ON RECENT TRENDS IN ADVANCED COMPUTING 2019, ICRTAC 2019

Intrusion Detection for Enhancing RPL Security

Deepali Bankatsingh Gothawal *, S.V. Nagaraj

Vellore Institute of Technology, Chennai - 600127

Abstract

Internet of things is a new paradigm that connects the internet to the physical objects of different domain viz. home automation, human health services, and industrial process automation and environmental monitoring. It is deeply presented in our daily activities through various devices. The devices connected with the internet bring many benefits but simultaneously bringing the security issues also. For protecting the network and information systems the intrusion detection system is an important tool. However traditional techniques used for intrusion detection are not sufficient to protect the network consists of specific characteristics like constraint resourced devices and specific protocol stacks. In this paper, we proposed an intrusion detection system for RPL (Routing Protocol for Low power and lossy networks) which is focused on WSN and constrained resources. Proposed IDS follows detection of an attack, IDS placement strategy, and validation process.

Keywords: IoT, Secure RPL, IDS, Routing performance.

1. Introduction

IoT market brings an industrial revolution and growing at a rapid pace, and expected a rise of 200% by 2020. IoT sensors collect and process the data including the spatial and temporal data for every situation and handle various challenges. The application area of IoT is including all areas like education, energy, domestic, entertainment,

* Corresponding author. Tel.: 9860516959
E-mail address: *dgohil.1519@gmail.com*

10.1016/j.procs.2020.01.051

Logistics, finances, healthcare, tourism, smart cities, and transportation as well. The various entities interested in IoT exploration integrate the fast commercialization of IoT techniques without paying much attention to the security and safety of IoT devices and the whole network.

The Intrusion Detection System [1] is the primary tool for protecting networks and information. Any security violations occurred in IDS alerts the system administrator since it is monitoring the operations of the host network. Though IDS technology is mature enough, current solutions are insufficient for IoT. The major considerations are the processing and storage capacity of the network nodes while designing security agents or IDS for IoT networks. Therefore implementation of IDS is done on the nodes which can support IDS agents. IoT networks are multi-hop rather the traditional networks are directly connected to the specific nodes for packets forwarding to the destinations. IoT networks use the protocols which are not used in traditional like IPv6 over Low-power wireless personal area network, IPv6 Routing protocol for low-power and lossy network (RPL) and constrained application protocol.

The IDS detects the activity [1] which intruders carry out against the IoT network system. These intruders aim to gain unauthorized access to the network system. Intruders may be from inside or outside of the network. Components of an intrusion detection system are sensors, an analysis engine with a reporting system. Sensors collect network or host data including traffic data, packet information, and file system data. Then a sensor sends the collected data to analyze for detecting ongoing intrusions. After analyzing the data by analysis engine reports are generated for alerting the network administrator to take actions. Any physical smart object can be connected to the RPL network using IPv6 (Figure 1). These physical objects may be part of different applications which include smart home appliances, industrial automation, energy monitoring, surveillance and military, and other security monitoring.

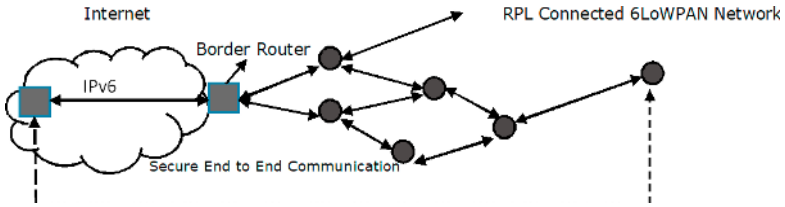

Figure 1: IoT Environment for Interconnection of IPv6 and RPL Network

These kinds of real IoT applications require secure communications [12] and that is difficult due to heterogeneous devices in which some of them are resource-constrained and the other may be powerful hosts. The confidentiality and integrity between the IoT devices should also be maintained and source and destination devices should be secured by end-to-end encryption. An intrusion detection system can efficiently utilize this architecture for placement of processing-intensive intrusion detection module for anomaly detection in the border router and other lightweight modules for rule-based detection in the resource-constrained sensor nodes. Putting IDS in constrained nodes requires more storage and processing resources while placing IDS in the border router requires more overhead in terms of communication between resources constrained nodes and border router. The intrusion detection module in the border router has the advantage of stopping intrusion attempts from the internet. They are also capable of blocking intrusion attempts from the insider nodes. It is because of physical access to a border router in WSN than typical internet hosts.

In the event of an attack, attackers hold control of the input data (Figure 2) that is transferred to the node from the IoT environment [13]. This input data may include data captured by the sensors or data obtained from the user interfaces. If the incoming data has not checked at the sensor nodes attackers can manipulate the IoT environment and may produce spurious sensor data or may launch a buffer overflow attack which leading the nodes to denial of service or improper behavior. Since the nodes are connected to the internet the misbehaving nodes can be used to attack other nodes in the RPL network. the nodes are connected to the internet the misbehaving nodes can be used to attack other nodes in the RPL network.

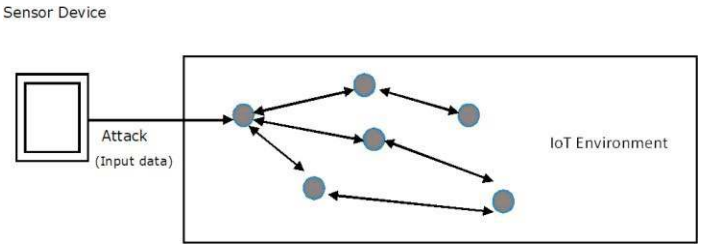

Figure 2: Attack Model (control over the input data by attackers)

2. Routing in RPL

Routing in RPL can be categorized in 2 main phases i.e. routing upward [2] and routing downward. Destination Oriented Directed Acyclic Graph (DODAG) is used to maintain topology. The DODAG contains paths from leaves to root. For upward routing RPL only uses the information in DODAG. The DODAG helps in the selection of preferred parents of the node while sending the packets to the root so the preferred parent node helps in sending the data to the root node. For loop avoidance, DODAG uses the rank to determine the position of a node in DODAG. Objective function computes the rank of a node. RPL populates DODAG with the parent node information. Control packets such as DODAG information object (DIO) and DODAG information solicitation (DIS) used for conveying the messages. An RPL instance is denoted by RPL instance ID containing many DODAG's denoted by DODAGID. DAO messages are used to update the routing table which helps in downward traffic.

2.1 Routing Metrics

RPL implementations mainly use two routing metrics i.e. hop count and ETX (Expected Transmission Count) [4]. Routing metrics helps to find the cost of a path and making the routing decision [3] if there are several routes available. Routing metrics in LLN is a scalar value helps in finding the best path and determines the routing strategy. Routing metrics used for quick delivery of packets using the shortest path and also for encrypted communication and avoiding non-encrypted links through the path. Routing metrics also help in selecting the path which has minimum energy constraints and it is done by selecting a path with the minimum number of battery- operated nodes as compared to the alternate paths. Hop count routing metric selects such a path in which participating nodes over the route are minimum which also minimizes the energy required for packet routing. ETX used for [4] packet retransmission and to minimize the overall transmission required for data transfer but it causes unequal energy distribution among the nodes. Energy-based routing metric is used to maximize the minimum remaining energy of the nodes between the pair. The benefit of using this metric is to favor all the paths which traverse the nodes with higher energy.

2.2 Intrusion Detection Methods

Intrusion detection techniques are divided into four types depending [20] upon detection mechanism used in the system namely anomaly based, signature-based, and specification-based and hybrid intrusion detection. Signature based method analyze the network behaviour and compare it with an attack [5] signature stored in the IDS internal database. If the behaviour matches with a stored signature then an alert is sent to the network administrator. This technique is very effective to detect the known threats and the mechanism of this technique is also easy to understand. But this method ineffective to detect the new threats since the signature of unknown threats is not available for comparison in the internal database of IDS. This technique is purely based on pattern detection for known threats.

Anomaly based Intrusion detection method observes [6] the activities of a system at any instance against a normal behaviour, if any deviation has occurred which exceeds a threshold from the normal behaviour then alerts will be generated. For constructing the normal behaviour profiles machine learning algorithms [10] are used. This method is useful for detecting new attacks. But this technique considers anything intrusion which does not match with the normal behaviour. For machine learning algorithms also it is a difficult task to learn the entire scope of normal behaviour.

In specification based Intrusion detection methods a set of rules or specifications [7] for the expected behaviour of the network components are defined by the human experts. This technique then compares the network behaviour with the specified rules, if any deviation occurs an alert will be generated to a network administrator. Specification based IDS need not the training or learning phase cause after defining the certain rules or specifications IDS can

start work immediately [11]. But it is inefficient in situations when manually defined rules do not match with the real environment and time consuming also.

In hybrid approaches, the above concepts of signature, anomaly, and specification based are used to obtain maximum advantage of all the methods and reduce the drawback of these methods. Several techniques for security attack detection (Figure 3) and prevention have been presented which are based on hybrid cryptography, key chain, and public keys. We cannot rely on a single method as it may be broken by attackers in one way or another. To deploy an effective attack prevention mechanism, it should be capable of locate and remove the attacker from the IoT environment. Different strategy is used to detect different attacks like location spoofing is detected by analyzing the communication delay between the nodes, malware attacks can be detected by analyzing the relationship of cause and timing of happenings of different events. Incoming data packet can help in the detection of attack. If the packets are arriving too frequently and with slow speed data packets are rejected to accept. If the arrival time delay of data packets is very high then it is not accepted. Data packets with time arrival within a specified threshold are accepted. A physical layer attack can be detected by the analysis of radio channel information.

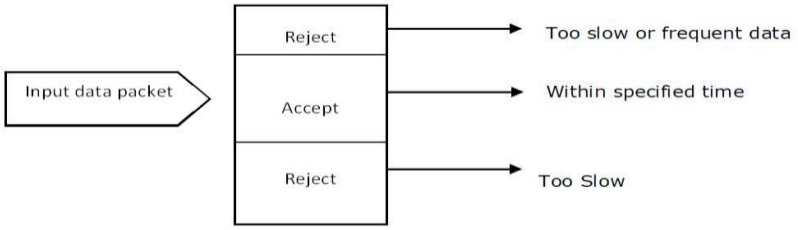

Figure 3: Detection of attack Through IDS

For deployment of an intrusion detection system in RPL based network the approaches for detecting the internal threats [8] must be clear. One of the IDS approach for detecting the internal threat is anomaly intrusion detection. The philosophy for anomaly based detection is to define the standard behaviour of the node and the threshold for deviation from the legitimate behaviour, when any node crossing the threshold identified as the malicious node. Anomaly based intrusion detection is used at the primary or initial stages of IDS [9]. IDS using for securing the RPL collect and analyze the data obtained from various sources. Information received from all nodes and their neighbours at the DODAG root are analyzed viz. the node's parent ID, rank and timestamp. The rank consistency and the legitimacy of the rank are to be analysed for recognizing any deviation. Another approach for intrusion detection is based on identifying a particular behaviour of the routing protocol. It is more effective when attackers attack on the topology. This approach identifies the malicious nodes which breaking the protocol rules.

Various attacks affect the performance of RPL topologies are shown in table 1.

Table 1: Internal threats towards affecting RPL Performance

Attacks	Description	Objective of attack
Sinkhole attack	In this attack, attacker captures the sink's rank and show itself as a sink and communicate accordingly	The consequence of this attack that it can redirect the whole traffic
Rank attack	Attacker does not send the data packets to specified parent	Route can be disrupted and traffic redirected
Neighbor attack	Attacker forward the same DIO message to its neighbor without any change	Resource consumption, false route direction
DIS attack	In this attack DIS message with the fake IP address is sent to other nodes to increase overheads and jamming the routing process	Resource consumption and affects routing process
Repair attack	An attacker request for local repair continuously	Resource consumption and route disruption

2.3 Detection of internal RPL threat

Internal security threat with the RPL based network is topology attack. The intrusion detection system should be capable to detect this topology attack through the collected monitoring data and set of rules which are used straight forward for detecting the protocol behaviour with small overhead and little storage and processing requirement. Internal threats aims to degrade the performance directly by changing node behaviour. Internal attack can follow the protocol regulation yet still affects other performance behaviour like sending, forwarding and controlling the

manipulated messages. Accuracy of Intrusion detection system depends on the robustness of the threat detection algorithm and amount of monitoring data collected by the system need to be extended more. The IDS computation and storage capability can be increased by delegating the IDS work to many other computers in the cloud. This IDS architecture allows using many robust IDS algorithms on large IDS data which is meant for achieving higher accuracy while dealing with the internal threats effectively in the large scale network.

Another strategy used for IDS is focused on monitoring and [14] comparing the network behaviour to detect any suspicious activity. IDS observe any deviation between the monitored data and the regulations and if any deviations more than the threshold value it will raise an alarm. Implemented IDS has the ability to detect new attacks which makes any modification in the network operation. One drawback in this system is that the false alarm rate is also high due to non-differentiation between misbehaviour and malicious activity.

Security requirements in RPL aims at protecting communications [15] in the sensor network which ensures confidentiality, authentication, integrity and freshness for both data and encryption key to ensure no announcement of old messages. The IDS also ensures resiliency to provide a certain level of security even in the case of being captured of some nodes by malicious nodes.

In cryptography techniques authentication ensures through providing the access of right key to decrypt and read the message only to authenticated users. Integrity is achieved by preserving the message content during the transmission. RPL works in WSN and internet so for WSN, public key cryptography mechanism is too heavy to implement due to constrained resources. Exchanging the key is also not feasible due to heavy signaling messages and energy efficiency requirements. Cryptography is helpful in protecting 6LoWPAN from the external attacks mostly. Cryptography mechanism lacks the ability to detect and mitigate the internal attacks due to non-capable of detecting the attacks with legal keys which behaves abnormal. So cryptography alone is not able to secure RPL network and therefore IDS implementation (Figure 4) is required to monitor and protect the network from the malicious behavior. Intrusion detection system is most efficient way for detecting the attacks which bypass the cryptography mechanism. The combination of cryptography mechanism and IDS can be a good option for RPL security and their objective is to monitor the possible threats and raise an alarm for possible threats and regenerate the key for eliminating the attackers. The combination of both these techniques prevents to obtain the suspicious route and ensure to follow optimized route by traffic monitoring through control messages.

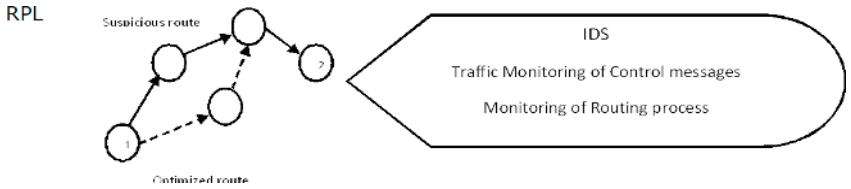

Figure 4: IDS for Securing RPL

3. Proposed Intrusion Detection Approach

While deploying Intrusion detection system [16], initially it is considered that all the nodes are static and no malicious nodes are present in the RPL network. Later on two malicious nodes are introduced by the attackers. These malicious nodes are attracting the traffic from two different part of the network and disturb the routing process. These two nodes can create a channel and controlling the routing process. Later on these nodes can drop the packets as well as can modify the packets. Attackers can analyze the traffic through these nodes by changing the node id, rank and neighbor information. Proposed IDS should be capable of doing several verifications viz. verification of neighbor list of each node, verification of DIO and DIS messages as well as rank information.

The proposed IDS [17] can be divided in three modules viz. first module is responsible for mapping the coverage area of RPL network, second module is responsible for detecting the possible attack and third module is responsible for preventing the attack or protect the whole RPL network as a firewall. In the IoT environment a node may be controlled by attacker and that compromised node is used to send wrong information about the rank of nodes to their neighbors. Incorrect information may be obtained due to lossy links in the IoT environment. It is crucial and necessary to detect incorrect information and also to get the correct information for deploying a successful Intrusion

Detection System.
Module 1 for mapping coverage area is represented by following algorithm. This module is used for setting a coverage area for the participating nodes. The coverage area also calculates the distance between the nodes. It also helps in selection the optimum path for communication and routing between the nodes. If any node is communicating beyond the mapping area or exceeding the threshold distance alarm will be raised and suspicious activity has been rectified.

Module1: Mapping coverage area
DM = Computing the distance for one or two nodes
N= number of elements refers in DM
Function (Mapping of coverage area) = find path & Coverage (Nodes, a, b)
Record SourceID, DISInfo,
DISInfo [SourceId] ++
If DISInfo <= CurrentInfo then Prompt Fake DISInfo
Else
DISInfo = CurrentInfo
IF N= > thresholdcount
Then
Alarm out of Mapping or coverage area
Else
Return
MappingSet, Mappingpath

Module2: Detection of misbehaving node in the network
Variable Th= current threshold value for the degree of the node (for routing path)
Neighbors Th= threshold value for the degree of the neighbour's node
Current _Th= node_Th (i)
If current_Th > neighbors_Th then
Suspecte_node= i
Suspected_node= current_Th
Count=count+1
Endif

Module3: Mitigation of attack
Input: L1 =A list of hosts in RPL DODAG
Input: L2=List of suspected Node with Threshold value
Response = empty List For nodes in nodes
Do Check
Node = suspected_node If node = suspected_node Response
Alarm.raise (Removing Suspected node)
Node_remove (Response_source) ENDIF
ENDFOR

Module 2 of IDS is used for detecting inconsistencies in the routing process. For verifying the actual routing path a certain threshold can be define for each node. If the threshold value for a particular node is greater than the defined threshold value then it is assumed that the node is far from the current node and it is trying to attract the traffic towards it. This node may be introduced by the attacker. The threshold value may be the h-index of any node mentioning the neighbor of the node. If this value has high then the node may be suspicious or trying to hijack the maximum number of nodes by the attacker. Degrees of neighborhood estimate the capability of nodes from different perspective. It tells the impact of linkage quantity and clustering behavior of the network. H-index value of the node provides the information to us that maximum integer h of the node has at least h neighbor. If the number goes beyond this value node would be considered as suspicious.

Module 3 is used to remove the suspected node from routing process to mitigate the impact of attacks. Another strategy used for IDS is focused on monitoring and comparing the network behavior to detect any suspicious activity. An ID observes any deviation between the monitored data and the regulations and if any deviations more than the threshold value it will raise an alarm. Implemented IDS has the ability to detect new attacks which makes any modification in the network operation. This module prevents to capture the nodes by the attacker and remove the suspicious node.

4. Implementation

In our experiments we use Contiki operating system for the simulation and validation process of proposed intrusion detection technique to secure RPL routing. Within Contiki network simulator which is known as Cooja allows many of the network topologies to be simulated. Cooja simulator is used to show the communication in radio environment and the nodes of real time traffic. It is also possible to export the radio message to export for further analysis through protocol analyzer Wireshark. IoT is similar to WSNs as IoT network inherit attacks from both WSNs and traditional internet network. We focus on routing attacks that RPL susceptible to attacks inherited from WSNs and attacks on RPL vulnerability. These attacks belong to all categories of attacks. Attacks mitigation [18] is done through the IDSs mechanism which deals with the specific attacks for detection and mitigation. For mitigation of attacks IDS needs collaboration between the nodes.

The method adopted in the IDS depends on sending the messages and receiving acknowledgement to prevent any alteration. In an example where the root node sends echo message to every node and receives acknowledgement back, if the acknowledgement is not received the node is considered as malicious node. But only depending on acknowledgement is not sufficient for protecting RPL routing. Nodes must be observe and monitor the behavior of their neighbors to create a trusted communication between them. This methodology is used to mitigate WSN inherited attacks which may be decreased rank attacks etc. Intrusion detection system uses RPL's specifications like rank and DODAG version for detecting attacks.

The proposed intrusion detection system monitors the traffic of network to record the normal behavior of the network and compare this normal behavior with the possible attack. The proposed IDS is efficient in detecting the attacks. In the proposed IDS either it is resides at the root node or at the dedicated host node and detect attacks though the traffic going through. If it is placed at the root node then IDS is capable to perform extensive security checks. Figure 5 shows the implementation of proposed IDS. RPL protocol is similar as a tree oriented structure. Neighbor discovery is the main process to formation of RPL network [19]. While RPL network is formed it builds the downward and upward paths among the client nodes and root nodes.

5. Evaluation

The metrics for performance analysis is mainly the latency of the radio cycle and power consumption etc. The type of the experimental node is sky mote.

Computational latency is defined as the total time taken for a given number of successful transmissions from client to server node where handover latency is not considered. In our simulations, we computed the latency for 30, 50, and 100 packets. The results are shown in Figure 5 indicates that it takes longer to compute the average signal strength value for a moving node. As a result, additional computational time is required, which degrades the latency performance for the modified RPL algorithm. The overall latency for 30, 50, and 100 successful packet transmissions when handover latency is considered is shown in Figure 6. It is evident that the algorithm outperforms by several folds. Since the standard algorithm delivers a lower PDR, it takes much longer to successfully transmit the same number of packets as compared to that of the modified RPL algorithm. This reflects the consistency in the results obtained from the simulations. When there are 30, 50, and 100 successful transmitted packets, the overall latency improves by 41.1%, 55.8% and 63.3%, respectively. Considering both the computational latency and the overall latency in tandem, we assessed that it is more effective to use the modified RPL algorithm for an IoT environment.

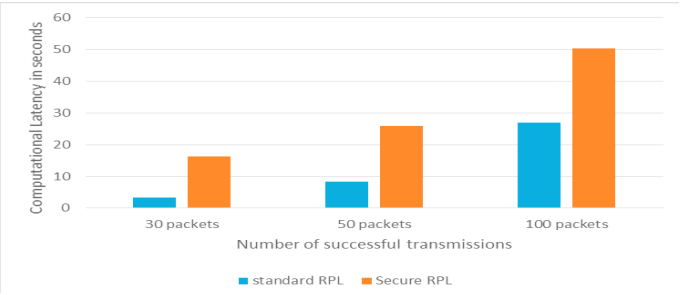

Figure 5: Computational Latency for Successful Transmissions

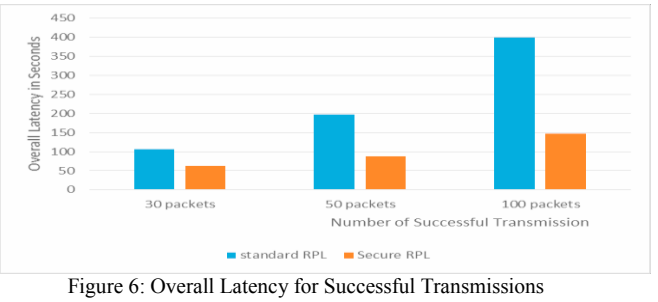

Figure 6: Overall Latency for Successful Transmissions

6. Conclusions

Internet of Things devices or IoT devices is becoming prevalent in many fields. Before we employ these devices for several different and crucial applications such as Health monitoring, military application, area monitoring, etc. an efficient security implementation is required. These implementations should have efficiency considering the resource consumption and enhancing the network security. In this research we analyzed an impact of the proposed IDS or intrusion detection system considering different operating environment and simulation. As we have concluded previously for the results that simulated results are not reliable all the time. We required more research regarding our cyber-attack mitigation algorithm to provide security for these IoT devices and also to provide energy efficient encryption. Hence, there is requirement of an efficient algorithm based on our proposed IDS considering the absence of security implementation and detection mechanisms.

References

[1] Zarpelao, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

[2] Shreenivas, D., Raza, S., & Voigt, T. (2017, April). Intrusion Detection in the RPL-connected 6LoWPAN Networks. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security (pp. 31-38). ACM.

[3] Kim, H. S., Kim, H., Paek, J., & Bahk, S. (2016). Load balancing under heavy traffic in RPL routing protocol for low power and lossy networks. IEEE Transactions on Mobile Computing, 16(4), 964-979.

[4] Kumar, S., Andersen, M. P., Kim, H. S., & Culler, D. E. (2018, November). Bringing full-scale tcp to low-power networks. In Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems (pp. 386-387). ACM.

[5] Herberg, U., & Clausen, T. (2011, November). A comparative performance study of the routing protocols load and RPL with bi-directional traffic in low-power and lossy networks (lln). In Proceedings of the 8th ACM Symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks (pp. 73-80). ACM.

[6] Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, 152-160.

[7] Amouri, A., Morgera, S., Bencherif, M., & Manthena, R. (2018). A Cross-Layer, Anomaly-Based IDS for WSN and MANET. Sensors, 18(2), 651.

[8] Reddy, R. M., & Neerugatti, V. (2018, February). Anomaly Based Technique for Detection and Prevention of Black Hole Attacks in RPL Based Networks. In International Conference on Universal Computing, Communications and Data Engineering (CCODE-2018).

[9] Jain, A., & Jain, S. (2019). A Survey on Miscellaneous Attacks and Countermeasures for RPL Routing Protocol in IoT. In Emerging Technologies in Data Mining and Information Security (pp. 611-620). Springer, Singapore.

[10] Ashraf, N., Ahmad, W., & Ashraf, R. (2018). A Comparative Study of Data Mining Algorithms for High Detection Rate in Intrusion Detection System. Annals of Emerging Technologies in Computing (AETiC), 2(1).

[11] Kenkre, P. S., Pai, A., & Colaco, L. (2015). Real time intrusion detection and prevention system. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 (pp. 405-411). Springer, Cham.

[12] Abomhara, M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.

[13] Pongle, P., & Chavan, G. (2015, January). A survey: Attacks on RPL and 6LoWPAN in IoT. In 2015 International Conference on Pervasive Computing (ICPC) (pp. 1-6). IEEE.

[14] Le, A., Loo, J., Chai, K., & Aiash, M. (2016). Specification-based IDS for detecting attacks on RPL-based network topology. Information, 7(2), 25.

[15] Le, A., Loo, J., Lasebae, A., Aiash, M., & Luo, Y. (2012). 6lowpan: a study on qos security threats and countermeasures using intrusion detection system approach. International Journal of Communication Systems, 25(9), 1189-1212.

[16] Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. IEEE Communications Surveys & Tutorials, 20(4), 3496-3509.

[17] Zhang, L., Feng, G., & Qin, S. (2015, June). Intrusion detection system for RPL from routing choice intrusion. In 2015 IEEE International Conference on Communication Workshop (ICCW) (pp. 2652-2658). IEEE.

[18] Wallgren, L., Raza, S., & Voigt, T. (2013). Routing Attacks and Countermeasures in the RPL-based Internet of Things. International Journal of Distributed Sensor Networks, 9(8), 794326.

[19] Anuj Sehgal, Anthéa Mayzaud, Rémi Badonnel, Isabelle Chrisment, Jürgen Schönwälder. Addressing DODAG inconsistency attacks in RPL networks. Global Information Infrastructure and Networking Symposium (GIIS), 2014, Sep 2014, Montreal, QC, Canada. pp.1 - 8, ff10.1109/GIIS.2014.6934253ff. Ffhal-01090986f

[20] Sharma, D., Mishra, I., & Jain, S. (2017). A Detailed Classification of Routing Attacks against RPL in Internet of Things. International Journal of Advance Research, Ideas and Innovations in Technology, 3(1), 692-703.