Threshold Based Dynamic Approach for the Isolation of the Version Number Attack in IoT

Mr. Debasish Hati
Department of Computer Science and Technology
Technique Polytechnic Institute
Hooghly,India
debasishhati2013@gmail.com

Mr. Sohan Goswami
Department of Computer Science and Technology
Technique Polytechnic Institute
Hooghly,India
sohangoswami@gmail.com

Ms. Soumali Roy
Department of Computer Science and Technology
Technique Polytechnic Institute
Hooghly,India
roysoumali21@gmail.com

Abstract— **The Internet of Things is the self-configuring type of network in which various nodes can join or leave the network when they want. Due to such nature of the network, various malicious nodes can join or leave the network. The version number attack is the active type of attack which affects network performance. In this research work, technique of threshold is proposed for the detection and isolation of malicious nodes from the network. The proposed technique is implemented in network simulator version 2 and results are analyzed in terms of packet loss, delay and throughput.**

Keywords—**Version number attack, DODAG, Threshold Technique**

I. Introduction

IoT (internet of things) can be defined as a technology that connects multiple sensors, smart nodes, and objects together for establishing communication among them without any manual intervention. The autonomous functioning of entities or things depends on the connectivity amid them. The nodes in IoT carry out different types of tasks. These tasks include analysis of gathered data for decision making, giving lightweight data and data extraction by getting the excess of the cloud-based resources. The connection between clients, services, sensors and objects is established extremely closely via IoT. There are various application fields that make use of IoTs in extensive manner. These application fields include smart grid healthcare, its (intelligent support system). IoT is highly beneficial from business prospective also as it provides large number of intelligent tools and services [1]. The connectedness of IoT devices on the cloud system is the main reason behind the development of cloud-based iot networks. This makes possible the transmission of data to serve different purposes. In particular, ip based web and iot applications provide transferring using tcp and udp. On the other hand, few commonly used message distribution functions occur amongst the majority of IoT applications. Different applications apply these tasks in interoperable standard manners. The designing of a publish/subscribe protocol framework, extremely analogous to the client/server protocol, is carried out. This is referred as MQTT (Message Queue Telemetry Transport). MQTT protocol becomes highly important because of its uncomplicated structure and capability to prevent the extreme use of CPU and memory. AMQP (Advanced Message Queuing Protocol) is the one more protocol developed for the financial industry. The main motive behind using TLS/SSL protocols is security management. The use of less power and memory embedded devices can be ensured by using CoAP for the communication purpose.

Up to now, several network layer protocols have been designed as well. Among these protocols, IEEE 802.15.4 is the most frequently used IoT standard for MAC protocol [7]. This protocol defines a frame set-up. In this set-up, the address of source and destination is defined in headers along with way through which node can interact with each other. In recent times, the implementation of Low power multi-hop networking is carried out in IoT due to its unsuitability of using frame formats implemented earlier in the conventional networks. They increase the system's overhead. In general, channel hoping and time synchronization are employed to ensure high consistency, inexpensiveness and to satisfy the communication requirements of internet of things. The IPv6 Routing Protocol is a standardized remote vector routing protocol. This protocol is specially designed for RPL network which is lossy and includes low energy. This protocol does not include any cycle, and therefore does not have loop. This occurs due to the way in devices are linked to each other. DODAG with the border routers avoids cycles. These routers are linked to the internet. All devices linked to DODAG are connected online via this border router. The protocol prevents loops when it measures the location of node corresponding to the root node [9]. This position regarding the root node is referred as the rank and the rank increases with the motion away from the border router. Messages from a child node which is going down are ignored to prevent loops. A node contains a parent, which transfers data from the nodes to the border router and may have various children. The node sends the children's packages to the border router.

- *Version Number Attack*

The root node makes use of version number to ensure that the global repair process of rpl is under control and updating of all the nodes existing in dodag is carried out based on their routing location. The occurrence of version number attacks in iot can decrease its service time. The intruder can launch this intrusion with extremely low overhead and the use of global repair scheme included as an immune system of protocol can overload the global repair scheme network. The root starts a global repair in the occurrence of numerous network irregularities. The vn (version number) of dodag is incremented to rebuild the entire dodag. DIO (Dodag Information Object) refers to the control message that carries this version number. Every receiving node compares the earlier version number and the one obtained from its parent. The existing rank information is overlooked, the trickle timers are reset and a novel process to join the DODAG is started in case of higher received version. This global repair guarantees a loop free topology despite of its too much expensiveness. It is important to notice that the node did not transit to the novel dodag version if dio messages advertize its earlier version. It is essential for the other nodes to not choose such a node as preferred parent. Two versions of dodag may occur simultaneously during global repair. On the other hand, data packets existing in old version can migrate in fresh version to prevent loops. The earlier version is not regarded as dodag. Also, the accessibility of loop free topologies cannot be guaranteed as the network is still away from the convergence state.

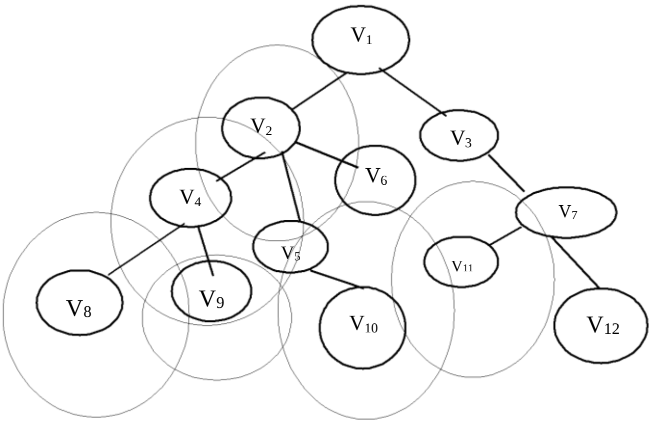

Figure 1: Illustration of a version number attack

In order to prevent any possible irregularities of the network, the version number must be transmitted unaltered across DODAG. RPL does not include ant method to ensure the reliability of version number occurring in the received DIO messages. An attempt made by the malicious node to change this value in its own DIO messages can cause harm to the network. If a malevolent DIO is received with a fresh version number, the trickle timer is reset, the version is updated and the fresh version is promoted to the neighbors by DIO messages. Figure 1 shows the propagation of the illegal version number via the network. In this situation, the genuine network nodes broadcast their increased version number started by malevolent node V_5 in the automatic manner.

II. Literature Review

Ahmet Aris *et al.* [16], presented two new lightweight mitigation schemes for RPL-VNA (Version Number Attacks). These intrusions severely affected the efficiency of IPv6-connected LLNs (Low Power and Lossy Networks). In these intrusions, an intruder cause changes in the version number of the network spitefully. The main aim of the attacker here was to increase the latency and control message overhead. These types of intrusions reduced the service time of network and PDR (Packet Delivery Ratio). This work presented simple at the same time efficient mitigation methods to significantly improve the efficiency of attack affected RPL network. The new schemes reduced the attack caused delay, average power consumption and control message overhead up to 87%, 63%, and 71%. These schemes also showed 86% of increase in the PDR (Packets Delivery Ratio). The new schemes exchanged the mitigation efficiency against the resource outlays while permitting the ordinary RPL function. Hence, these schemes allowed network manager to select the appropriate technique for their RPL network.

Amit Dvir *et al.* [17], presented a novel routing protocol to remove the problems of LLNs (Low power and Lossy networks). This protocol was referred as IPv6 routing protocol. The new protocol made its contribution in the performance of LLNs (Low power and Lossy Networks). RPL provided multiple routes by generating and handling the DAGs (Directed Acyclic Graphs) via single or multiple gateways. Therefore, an adversary deploying a single node close to the gateway could divert a bigger part of the network traffic independently. This work made use of an improve version called DODAG to reconstruct the routing topology. It was also essential to carefully prevent an internal attacker from publishing the reduced rank level that caused a bigger portion of the DODAG for establishing connection to the DODAG root through the intruder and made it enable to listen to a bigger portion of the network traffic forward on its own. Hence, this new security approach was capable enough to prevent the illegal boost in the version number.

Anthea Mayzaud *et al.* [18], proposed a detection technique derived from a distributed monitoring framework with dedicated algorithms. The main aim of this technique was to detect VNAs (version number attacks) in RPL-based networks using a distributed monitoring framework. The new technque successfully identified the malevolent nodes that launched these types of intrusions in RPL networks. A lot of tests were conducted in this work to evaluate the efficiency of the proposed technique. This work considered a monitoring node placement scheme to quantify the scalability of the new technique. The future work would be focused on conducting corresponding tests in real-time architectures with more types of devices applying the RPL protocol. In future, the proposed technique could be evaluated and extended to the case of intruder alliance. It refers to the condition when various adversary nodes occur in the network simultaneously.

Zeeshan Ali Khan *et al*. [19], designed and evaluated some IDS schemes for IoT Networks. These schemes were suitable for the minute devices. These schemes made use of trust management method. This method allowed devices to handle reputation information of their neighbors. This approach efficiently distinguished spitefully behaving elements in a processing and energy-efficient manner. This procedure was carried out in an energy based system. The trust management subjective logic was focused on to recognize the adversary nodes existing in the network. Three variables were presented. These variables were based on negative and positive trust ratings; belief (b), disbelief (d) and uncertainty (u).

$$b = \frac{\mathrm{p}}{\mathrm{p+n+k}} \quad d = \frac{\mathrm{n}}{\mathrm{p+n+k}} \quad u = \frac{k}{p+n+k}$$

The adversary node after being detected got immediately eliminated from the network. The new scheme performed better against the three sorts of intrusions launched on RPL protocol. It was possible to use the new scheme against the other sorts of attacks as well. The future work would be focused on developing a test bed containing Z1 elements to validate the simulation results of MATLAB tool. This work made a discussion on a variety of algorithms to manage the reputation. These algorithms included NBTD (Neighbor Based Trust Dissemination), CNTD (Clustered Neighbor Based Trust Dissemination) and TTD (Tree Based Trust Dissemination).

H. Abdo *et al.* [20], presented a new technique based on both safety as well security during for analyzing the risk in industrial applications. This technique combined bowtie analysis with a fresh improved adaptation of attack tree analysis. The use of bowtie analysis was quite popular to analyze the security while the second approach was presented to analyze the safety of ICS (Industrial Control Systems). The bowtie and attack tree when merged together comprehensively represented the risk conditions by considering safety and security. Afterward, this work presented a technique to evaluate the risk level on the basis of two-folded possibility portions. The first portion was used for the safety while the other one was for the security. This work analyzed a real-time risk case in a chemical factory to represent the purpose of this technique.

Ahmet Aris *et al.*[21], deeply studied the RPL version number attacks and presented the analysis of intrusions from different viewpoints. This analysis gave exclusive factors of this work in a real-time network topology. This topology had both stationary and mobile nodes with different multiplicities. This work was inspired from the IETF routing requirement documents. This work also analyzed the way of affecting the energy consumption of the nodes by the VNA (Version Number Attack). This work presented a probabilistic attacking model. In this model, the intruder launched intrusion attacks with a probability of p (e.g., 0, 0.3, 0.5, 0.7, and 1). This work also provided the performance outcomes in terms of different values of probability of p. The simulation results demonstrated that the outcomes of PDR (Packet Delivery Ratio) and the CPO (Control Packet Overhead) were highly related to the intruder's locality.

Hezam Akram Abdul-Ghani *et al.*[22], presented a novel IoT (Internet of Things) suggestion approach based on the construction of blocks strategy. This was mainly a reference model with four layers. This work presented a wide-ranging IT attack model that had four major stages. The first stage presented an IoT asset based attack level made up of four elements. These elements were identified as software, information, protocol wrapping the complete IoT mass and significant things. The next stage provided a description of the IoT security architecture. The third stage classified the IoT attack for all elements. The last stage detected the infringement of security objectives and relation between each intrusion. This stage also presented various strategies to secure every resource. This was the first ever attempt of developing an IoT attack model based on the building block reference model. The achieved outcomes evidently demonstrated the efficiency of the new model.

Anthea Mayzaud *et al.* [23], presented a detection approach to deal with the VNA **(**Version Number Attack) in RPL environment. This work applied a strategy relied on the distributed monitoring architecture to hold a discussion on node resources. The new approach used the relationship amid monitored nodes for the intruder detection. The intruder started the localization process after getting the detection information from all observing nodes. In this work, several tests had been carried out to evaluate the new approach. It was possible to decrease the FPR (False Positive Rate) by placing the monitoring nodes strategically. The future work would be focused on conducting a large number of corresponding tests on the basis of realistic framework with some other types of devices.

III. RESEARCH METHODOLOGY

There are several stages included in the research method. These stages include implementation strategy, projected results and requirements for hardware and software tools.

The flow-chart of the implementation is given below:

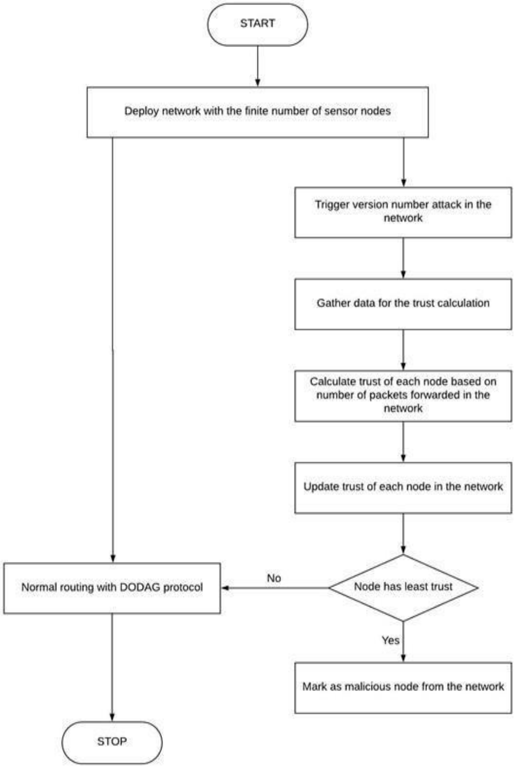
START
Deploy network with the finite number of sensor nodes
Trigger version number attack in the network
Gather data for the trust calculation
Calculate trust of each node based on number of packets forwarded in the network
Update trust of each node in the network
Node has least trust
No
Normal routing with DODAG protocol
Yes
Mark as malicious node from the network
STOP

Figure 2: Flow Chart of the algorithm

Here are the different steps of the implementation strategy:-

- **Deployment of the Network: -** The deployment of network will be carried out with the fixed number of sensor nodes and a sink node. The sensor nodes sense different sorts of physical parameters such as temperature, pressure etc. The sensor devices are heterogeneous in nature. This implies that every sensor node possesses different battery and processing energy. The DODAG protocol will sort out the network into a configuration similar to the tree.
- **Trigger of version number attack: -** The malevolent nodes will be formed in the network. These nodes launch version number intrusion. In the DODAG, malicious nodes cause changes in the version number.

The DODAG protocol will choose the route with high version number. This will result in routes based on loop formation in IoT.

- **Trust Calculation: -** This work presents trust based approach to mitigate the version number intrusion. The trust based scheme will perform in the three stages. These stages include pre-processing, trust measurement and trust updating. The sensor nodes with minimum trust will be marked as malevolent nodes.
- **Analyze network performance: -** The final stage will analyze the efficiency of network in terms of some metrics. These metrics include throughput, packet loss and energy consumption. The efficiency of the new method is evaluated using this metrics.

IV. RESULT AND DISCUSSION

This research work is focused on to isolate version number attack in IoT. The version number attack is launched in the DODAG protocol. This chapter compares the three conditions. The first two conditions include DODAG protocol and the effect of version number attack on the efficiency of DODAG protocol with regard to throughput and packet loss. The third case involves the segregation of version number intrusion in DODAG protocol. As per the analysis, the presented case has minimum packet loss and maximal number of throughput in contrast to attack case presented in the base paper.

Table 1: Simulation Parameters

Parameter	Values
Simulator	Ns2-2.35
Number of nodes	32
Area	800 * 800 meter
Antenna type	Omi-directional
Channel	Wireless channel
Propagation Model	Two ray

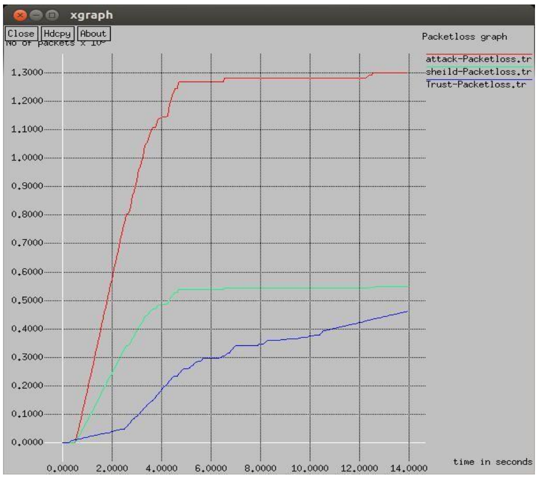

Figure 3: Analysis of packet loss

Figure 3 shows the comparison of attack case, base paper case and proposed case in terms of packet loss. As per the analysis, the presented technique shows minimal number of packet loss in contrast to the other two cases.

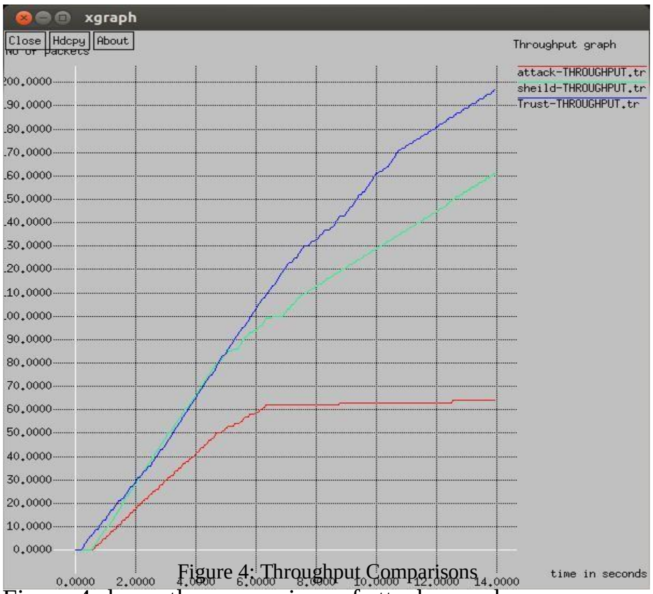

Figure 4: Throughput Comparisons

Figure 4 shows the comparison of attack case, base paper case and proposed case in terms of throughput. As per the analysis, the presented technique shows maximal throughput in contrast to the other two cases.

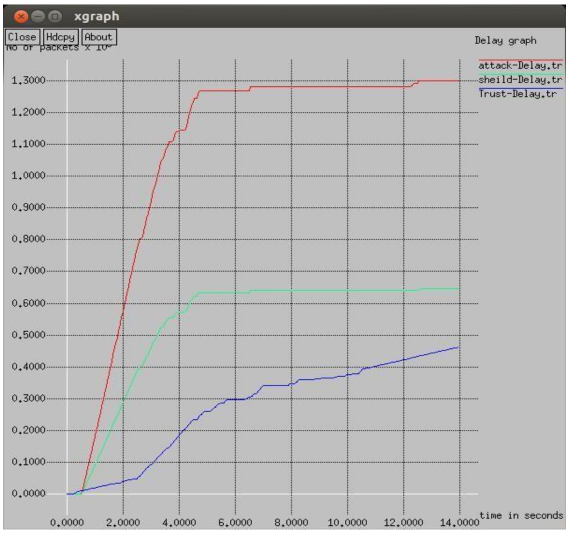

Figure 5: Delay Comparison

Figure 5 shows the comparison of attack case, shield attack and proposed approach in terms of delay. Shield scenario refers to the earlier technique for isolating the version number intrision. As per the analysis, the presented technique shows minimal delay in contrast to the other two cases.

V. CONCLUSION

This work is focused on to mitigate the version number attack in IoT. DODAG is a hierarchical structure. RPL network makes use of this structure for tiny devices where the malevolent nodes increments the version number. In IoT, this results in the formation of path containing loop. This work presents trust based approach to mitigate the version number intrusion from the network, and detecting the malevolent nodes. This approach consumes minimum number of IoT resources. This work makes use of NS2 (network simulator version 2) to implement the presented approach. The analysis of outcomes has been carried out in terms of throughput and packet loss. As per the analysis, the new approach performs better than other two cases in terms of throughput. The packet loss of the presented case is lower than the other two cases.

References

[1] A. Shaddad Abdul-Qawy, P. Pramod, E. Magesh, and T. Srinivasulu, “The Internet of Things (IoT): An Overview”, J. Eng. Res. Appl. , vol. 5, no. 12, pp. 71–82, 2015.

[2] D. Bandyopadhyay and J. Sen, “Internet of things: Applications and challenges in technology and standardization,” Wirel. Pers. Commun., vol. 58, no. 1, pp. 49–69, 2011.

[3] V. Bhuvaneswari and R. Porkodi, “The internet of things (IoT) applications and communication enabling technology standards: An overview,” Proc. - 2014 Int. Conf. Intell. Comput. Appl. ICICA 2014, pp. 324–329, 2014.

[4] S. V. Pote, “Internet of Things Applications , Challenges and New Technologies,” vol. 67, no. 978, pp. 45–51, 2018.

[5] E. Hopalı and Ö. Vayvay, “Internet of Things (IoT) and its Challenges for Usability in Developing Countries,” vol. 2, no. January, pp. 6–9, 2018.

[6] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, pp. 648–651, 2012.

[7] T. Salman and R. Jain, “Networking protocols and standards for internet of things,” Internet Things Data Anal. Handb., vol. 1, no. 1, pp. 215–238, 2017.

[8] Aniruddha Chakrabarti, “Emerging Open and Standard Protocol Stack for IoT | Aniruddha Chakrabarti | Pulse | LinkedIn,” vol. 1, no. 1, pp. 2–6, 2015.

[9] Internet Engineering Task Force. RPL: IPv6 Routing Protocol for Low-Power and Lossy

[10] Networks.https://tools.ietf.org/pdf/rfc6550.pdf, 2012. [Online; accessed 02-June 2017].

[11] E. Baccelli, M. Philipp, and M. Goyal, “The P2P-RPL Routing Protocol for Ipv6 Sensor Networks: Testbed Experiments,” SoftCOM 2011, 19th Int. Conf. Software, Telecommun. Comput. Networks, Split, vol. 1, pp. 1–6, 2011.

[12] T. Zhang and X. Li, “Evaluating and analyzing the performance of RPL in contiki,” Proc. first Int. Work. Mob. sensing, Comput. Commun. - MSCC ’14, pp. 19–24, 2014.

[13] J. Posegga, T. Eder, D. Nachtmann, D. Parra, and D. Schreckling, “Conference Seminar SS2013 — Real Life Security (5827HS) Trust and Reputation in the Internet of Things Trust and Reputation in the Internet of Things,” pp. 1–19, 2013.

[14] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, “A Trust-based Resilient Routing Mechanism for the Internet of Things,” Proc. 12th Int. Conf. Availability, Reliab. Secur. - ARES ’17, pp. 1–6, 2017.

[15] L. Gu, J. Wang, and B. Sun, “Trust management mechanism for internet of things”, Communi-cations, China, 11:148-156, 02 2014.

[16] J. Guo, I. R. Chen, and J. J. P. Tsai, “A survey of trust computation models for service management in internet of things systems,” Comput. Commun., vol. 97, pp. 1–14, 2017.

[17] A. Arış, S. B. Örs Yalçın, and S. F. Oktuğ, “New lightweight mitigation techniques for RPL version number attacks,” Ad Hoc Networks, vol. 85, pp. 81–91, 2019.

[18] A. Dvir, T. Holczer, and L. Buttyan, “VeRA - Version number and rank authentication in RPL,” Proc. - 8th IEEE Int. Conf. Mob. Ad-hoc Sens. Syst. MASS 2011, pp. 709–714, 2011.

[19] A. Mayzaud, R. Badonnel, and I. Chrisment, “Detecting version number attacks in RPL-based networks using a distributed monitoring architecture,” 2016 12th Int. Conf. Netw. Serv. Manag. CNSM 2016 Work. 3rd Int. Work. Manag. SDN NFV, ManSDN/NFV 2016, Int. Work. Green ICT Smart Networking, GISN 2016, pp. 127–135, 2017.

[20] Z. Khan and P. Herrmann, “A trust based distributed intrusion detection mechanism for internet of things”, in 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), pages 1169-1176, Los Alamitos, CA, USA, mar 2017. IEEE Computer Society.

[21] H. Abdo, M. Kaouk, J.-M. Flaus, and F. Masse, “A safety/security risk analysis approach of industrial control systems: A cyber bowtie combining new version of attack tree with bowtie analysis”, Computers Security, 72, 09 2017.

[22] A. Aris, S. F. Oktug, and S. B. O. Yalcin, “Rpl version number attacks: In-depth study”, NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, pages 776-779, 2016.

[23] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, “A comprehensive iot attacks survey based on a building-blocked reference model”, International Journal of Advanced Computer Science and Applications, 9(3), 2018.

[24] A. Mayzaud, R. Badonnel, and I. Chrisment, “A distributed monitoring strategy for detecting version number attacks in RPL-based networks,” IEEE Trans. Netw. Serv. Manag., vol. 14, no. 2, pp. 472–486, 2017.