SECURITY RISKS IN IoT NETWORKS: A COMPREHENSIVE LITERATURE REVIEW

Kanika Malik
Department of Computer Science & Engineering
Guru Jambheshwar University of Science & Technology
Hisar, India
mkanika86@gmail.com

Deepak Nandal
Department of Computer Science & Engineering
Guru Jambheshwar University of Science & Technology
Hisar, India
gju.dpknandal@gmail.com

Abhishek Verma
Department of Information Technology
Babasaheb Bhimrao Ambedkar University
Lucknow, India
abhiverma866@gmail.com

***Abstract*—The Internet of Things (IoT) is a group of connected gadgets. Sensors, actuators, and embedded devices gather information from their surroundings and communicate online. RPL protocol is used to implement routing in network which operates over low power wireless IoT devices and wireless sensors and networks. There is huge amount of data on the cloud so there is high risk of data losses, threats and attacks on the network. Security is the prime major concern for the users in IoT devices. In this paper, we review the study of researchers studying various attacks on low power and lossy devices in IoT networks.**

***Index Terms*—Security, Internet of Things (IoT), Routing Protocol (RPL).**

I. INTRODUCTION

IoT is a network of devices which are connected to each other and have the ability to connect to the internet, collect and share data. It makes our life easier and more comfortable. In the previous years there is high increase in areas of application in the field of IoT. In near future everything we touch or everything we use is connected via internet. We can assume everything is going to be automated and connected to the internet. Where it interacts to the central cloud and all collected data makes our life easier. Data will flow from everything we use and affect us all in both good and bad ways. As data is in very large amount so there can be data losses, delays and attacks hence security is the main concern for IoT devices.In this paper we first introduce what is IoT and what is RPL protocol followed by a literature study summarizing security risks on IOT devices with summary of literature review done by various researchers based on different aspects. The different security methods techniques can be compared in the table.

II. INTERNET OF THINGS

Internet of Things (IoT) is a network of those objects that are connected to each other via Internet. The objects are smart devices for example heart monitor, remote or automobile with the built in sensors. Each object is having an IP address and is capable of collecting and transferring data in network[9].

III. IoT LAYERS

Three layers make up the IoT architecture. The application layer, network layer, and perception layer are the three layers. A layer of applications The application layer's primary goal is to offer its users services. A layer of the network The network layer is particularly vulnerable to assaults because it collects data from existing infrastructures and sends it to other layers. The authentication and integrity of the data that is being transmitted are the main security concerns.The Perception Layer is the lowest layer of the Internet of Things architecture and acts as the structure's central nervous system. The physical layer is it. On this layer, there are sensors and other sensing apparatus. It also goes by the name "sensors layer."

Table: Network layer protocols and usage

PROTOCOL	USAGE
6LoWPAN	6LoWPAN is intended to operate with a variety of network topologies, including mesh and star networks, low bandwidth, scalable networks, mobility, and cheap cost.
RPL	The RPL (Routing Protocol for Low-Power and Lossy Networks) protocol is compatible with the data link protocol.
6TiSCH	To enable IPv6 to travel through the Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e data connections, the IETF's 6TiSCH working group is creating standards.

IV. RPL ROUTING PROTOCOL

"Routing Protocol for Low Power and Lossy Network" is known as RPL. It creates a DODAG, or destination-oriented directed acyclic graph. Each leaf node in DODAG only has one path to the root, and the root is the final destination for all communication.

A node in the network sends a DODAG Information Object (DIO) to identify themselves as the root, and any time a new node trying and attempts to join, it sends a DODAG Information Solicitation (DIS) request. The root answers back with a DAO Acknowledgment (DAO-ACK) to the node in the network, confirming the node's joining the network[8].

V. 6TISCH

6TiSCH works for wireless sensor networks and in the area of applications such as industrial internet, health and smart grids.

Wireless sensor networks have sensors that work wirelessly and send all data to a central unit in a network. Using IPv6 addressing with Time Slotted Channel Hopping (TSCH) MAC, 6TiSCH enables deterministic, low-power wireless sensor networks. Low power devices uses TSCH to communicate over wireless links and designed for networks with low power and loss to provide a reliable media access control layer. It is a combination of Time Division Multiple Access and Frequency Division Multiple Access and uses time diversity and frequency to provide reliability in upper network layer[10].

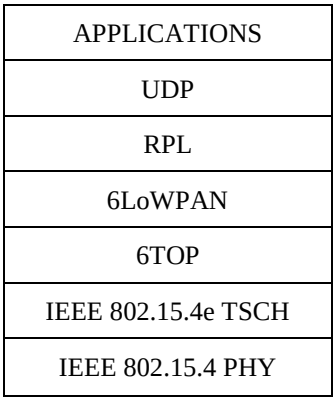

Fig. 6TiSCH protocol stack

The network stack structure of 6LoWPAN performs header compression, link step fragmentation, and reassembly mechanisms for transmitting IPv6 packets to IEEE 802.15.4 frames, as well as a destination-oriented directed acyclic graph (DODAG) in a wireless sensor network environment. 6TiSCH uses IEEE 802.15.4 PHY and IEEE 802.15.4e TSCH MAC protocols.

VI.IoT NETWORK LAYER ATTACKS

The network layer handles the network's data packet routing. Any malicious node can prevent the network from operating normally and start assaults.The user can benefit greatly from a variety of applications provided by the Internet of Things, but it also presents a number of security risks and difficulties that have never before been faced. The fact that IoT networked devices exchange information and have a degree of confidence in one another without running malware scans is a major source of this threat.

Table: Network Layer Protocol Attacks

PROTOCOL	ATTACKS
6LoWPAN	Authentication attack, Eavesdropping attack, man in the middle attack,Spoofing attack, Fragmentation attack
RPL	Sybil attack, Wormhole attack,Selective forwarding attack, Rank attack
6TiSCH	Denial of sleep attack, Flooding attack, Jamming attack, Replay attack, Overloading attack

VII. LITERATURE STUDY

The security of IoT networks is a growing concern as IoT devices increasing continuously in numbers. The literature review of relevant studies and articles on the topic of security in 6TiSCH in IoT has been conducted to gain a comprehensive understanding of the security challenges and solutions in this area.

Alakesh Kalita and Manas Khatua(2022):This paper concludes that 6TiSCH provides low latency and dependability for IoT applications. The 6TiSCH-MC standard using the IPv6 routing protocol in lossy and low-power networks and aids in resource allocation optimisation during network construction. While malevolent nodes send several DIS requests to obtain the network's routing information, new nodes and joining nodes in RPL send DODAG Information Solicitation (DIS) requests. This report used modelling and experimentation on actual devices to study and analyse how the DIS attack has affected the development of the 6TiSCH network. This study demonstrates that an attacker doesn't need to access sensitive network data, have expensive resources, or carry out DIS attacks on the network. The energy usage during the creation of the 6TiSCH network is hampered by DIS attack as well as the connecting time of network nodes. The DIS attack also lengthens the time it takes for pledges to synchronise and join, and it uses more energy per node in the network. on the future, a dataset for executing a variety of routing attacks on actual IoT networks can be created. Additionally, an effective machine learning technique can be used to detect network attacks[1].

Alakesh Kalita and Manas Khatua (2022): This paper concludes that as to avoid interference and multi-path fading on the channels, the TSCH protocol allows nodes to switch their physical channel after each transmission. However, this results in high energy consumption and inefficient data transmission, making the communication unstable.The 6TiSCH network, however, provides reliable communication in the IIoT. Therefore, this is a crucial issue for the quick creation of the 6TiSCH network. To better understand network development and evaluate performance, theoretical analysis, testbed tests, and simulation are all carried out. In order to increase the lifetime of the network and improve the efficiency of data packet transmission, many researchers have suggested a variety of methods and advancements to shorten the pledges' network joining time. The work that has already been done on the creation of TSCH and 6TiSCH networks is surveyed in this

study. This article also lists a few unresolved problems in the construction of the 6TiSCH network[2].

Alakesh Kalita and Manas Khatua (2021):This paper concludes that a standard named as 6TiSCH Minimal Configuration (6TiSCH-MC) allots only a minimal cell, or per slot frame, one shared cell, to send all different kinds of control packets. The performance of the 6TiSCH network is significantly impacted by a few network parameters because the congestion in minimum cells increases as the network's nodes grow in number. By easing congestion in the smallest cells, we can enhance network performance. Trickle algorithm and a slot frame window based adaptive method are presented to lessen congestion, and Contiki-NG is used to implement both. Nodes are required to transmit control packets often. The findings demonstrate that the suggested strategy reduces joining time and energy usage while giving network nodes a fair chance to transmit control packets[3].

Alakesh Kalita and Manas Khatua (2021):This paper concludes that when building a network for the IIoT, 6TiSCH assists in achieving reliable and timely data delivery and minimal resource allocation. High network congestion reduces the efficiency of network development in terms of combining time and effort use. Faster network construction utilising fewer resources is still a research topic that has to be addressed. Network bootstrapping traffic can only use one cell every slot frame, or a minimal cell, which leads in there is a lack of channel resource use and longer network construction times. To enhance the effectiveness of network development, this research developed an autonomous allocation and scheduling of minimum cell (TACTILE). The proposed technique, TACTILE, is evaluated in this work using both real testbed experiments and theoretical analysis. The results demonstrate that TACTILE improvements in joining time and energy consumption are made[4].

Alakesh Kalita and Manas Khatua (2020):This paper concludes that as a result of beacon frames havinghas precedence over all other control packets and providing nothing in the way of routing information during network construction, as well as joined nodes being unable to broadcast control packets due to extreme congestion in shared slots, and the effectiveness of 6TiSCH-based IIoT networks suffers over time. Opportunistic priority alternation and rate control (OPR) and opportunistic channel access (OCA) schemes, which enable nodes with urgent packets to transmit them in less time with faster association of nodes, are proposed as solutions to these issues. OPR provides adequate routing information and modifies the priority of control packets during network bootstrapping. Theoretical study and network simulation demonstrate that the 6TiSCH network is performing better regarding the fusion of time and effort usage[5].

Alakesh Kalita and Manas Khatua (2020):This paper concludes that The theoretical analysis of the 6TiSCH network formation protocol leads to the conclusion that when a pledge or new node joins the network, performance suffers because the transmission of beacon messages, which are required to understand the topology, causes channel congestion. And a channel condition based dynamic beacon interval (C2DBI) is suggested as a solution to this problem and for speedier connection of nodes in the 6TiSCH network. A theoretical analysis is conducted to demonstrate how the performance of network creation is enhanced in the suggested scheme when compared to constant beacon interval methods. Because Cooja's simulator is being used to simulate and evaluate the suggested approach and the outcomes are compared, the simulation will also be carried out utilising real testbed experiments. The findings indicate that C2DBI is more efficient in terms of energy use but not in terms of network formation time. Therefore, C2DBI is appropriate for networks when network construction time and energy usage are significant constraints[6].

Summary of some literature reviews done by various researchers based on different aspects are shown in Table. The different security methods and techniques can be compared in the table.

Table: Summary of some significant studies based on different aspects of IoT

S.No	Paper Title	Author Name	Technique OR Methodology	Data Set	Experimental Result	Proposed Work	Research Gap	Reference
1	Effect of DIS Attack on 6TiSCH Network Formation	Alakesh Kalita; Alessandro Brighente; Manas Khatua; Mauro Conti	6TiSCH-MC (6TiSCH minimal configuration) standard for 6TiSCH network bootstrapping	Real devices and testbed experiments	When compared to normal operation during the creation of the 6TiSCH network, DIS attack dramatically worsens the	By executing several routing attacks on a live IoT network and using an effective machine learning	To synchronise with the network and have an impact on network performance, malicious nodes do not need a lot of	IEEE Communications Letters Volume: 26, Issue: 5, May 2022,10.1109/LCOMM.2022.3155992, 02 March 2022 [1]

					nodes joining time and energy consumption , increasing them by 34% and 16%, respectively	technique to detect the assaults, a dataset can be created	energy or private information	
2	6TiSCH – IPv6 Enabled Open Stack IoT Network Formation: A Review	Alakesh Kalita and Manas Khatua	Survey of theoretical investigation of the creation of the 6TiSCH network	Real testbed experiments	Several open research questions in 6TiSCH network formation are presented, along with a brief summary of the elements that influence 6TiSCH network formation	Study to make network network reliable and how nodes connect more quickly in 6TiSCH network	Only focus on work from 2014 to 2021 and only theoretical and experimental results are considered	*ACM Trans. Internet Things* 3, 3, Article 24 (July 2022), 36 pages. https://doi.org/10.1145/3536166, 2022 [2]
3	Adaptive Control Packet Broadcasting Scheme for Faster 6TiSCH Network Bootstrapping	Alakesh Kalita and Manas Khatua	Both a dynamic trickling technique and an adaptive approach based on software windows (SW) are offered	Testbed for Contiki-NG's FIT IOT-LAB	Both of the approaches give network nodes an equal chance to transmit control packets. Together, the two programmes reduce the amount of time and energy commitments take to join	To lessen the congestion, a dynamic trickle algorithm is suggested. The nodes are need to transmit their control packets more often due to the slotframe window	The creation of the 6TiSCH network under DIO transmission rate was not taken into account in previous research	DOI 10.1109/JIOT.2021.3080735, IEEE Internet of Things Journal, 2021 [3]
4	Autonomous Allocation and Scheduling of Minimal Cell in 6TiSCH Network	Alakesh Kalita and Manas Khatua	TACTILE is proposed	Combined with Markov chain based theoretical analysis an evaluation of TACTILE is done on	In terms of joining time and average energy usage, TACTILE can outperform 6TiSCH-MC by 87% and 42%, respectively	Compare TACTILE with other existing benchmark schemes and proper scheduling should be done	Proper scheduling is necessary to provide synchronization among each pair of nodes	DOI 10.1109/JIOT.2021.3062115, IEEE Internet of Things Journal, 2021 [4]

				the FIT IOT-LAB real testbed				
5	Opportunistic Transmission of Control Packets for Faster Formation of 6TiSCH Network	Alakesh Kalita and Manas Khatua	Opportunistic priority alteration and rate control (OPR) and opportunistic channel access (OPA) are used to form opportunistic transmission of control packets (OTCP)	6TiSCH network low power and lossy devices and simulation on real testbed (FIT IOT-LAB) and benchmark 6TiSCH-MC and BS schemes	Results demonstrate a significant performance gain in terms of joining time and energy usage for the 6TiSCH network as well as network joining time	Offer an OCA method to allow nodes in urgent packets to directly access the shared slot	The proposed schemes' simulation and real testbed (FIT IOT-LAB) results are contrasted with those of the benchmark schemes 6TiSCH-MC and BS	ACM Trans. Internet Things 2, 1, Article 5 (December 2020), 29 pages. https://doi.org/10.1145/3430380, 2020 [5]
6	Channel Condition Based Dynamic Beacon Interval for Faster Formation of 6TiSCH Network	Alakesh Kalita and Manas Khatua	In order to account for channel congestion during network construction, a dynamic beacon interval (C2DBI) technique dependent on channel state is presented	Simulation and real testbed results	Compared to all previous works, C2DBI is superior. When network formation time and energy usage are major constraints, the C2DBI approach can be more appropriate	C2DBI is compared with other existing work and combined with the best suited	C2DBI outperforms all already available works, but not DRA in many ways	DOI 10.1109/TMC.2020.2980828, IEEE, 2020 [6]
7	Opportunistic Priority Alternation Scheme for Faster Formation of 6TiSCH	Alakesh Kalita and Manas Khatua	It is suggested to use Opportunistic priority alteration scheme (OPAS)	Real testbed experiment and simulation on COOJA simulator	The proposed approach improves network joining time and converges more quickly than the benchmark	OPAS can be implemented with while resetting the TRICKLE algorithm	Simulation is used to validate the proposed system, and the results are contrasted with those obtained using the	21st International Conference on Distributed Computing and Networking (ICDCN 2020), January 4–7, 2020, Kolkata, India. ACM, New York,

	Networ k				protocol		benchmark protocol 6TiSCH-MC	NY, USA, 5 pages [7]

Alakesh Kalita and Manas Khatua (2020): This paper concludes that In IoT networks, 6TiSCH offers dependability, prompt data delivery, interoperability, and network bootstrapping. The network formation's performance of 6TiSCH declines when more nodes are added and are uninformed of the needs for routing information and the highest priority of beacon messages in the network. This study addresses these difficulties. In order to hasten the affiliation of nodes and the development of the network of 6TiSCH, an opportunistic priority alteration scheme (OPAS) was presented in this research. This technique involves accelerating the transport of packets with routing information.The cause is that EB frames are given first priority during network construction, while already-established nodes in the network continue to send DIO at the same rate. In order to get around these restrictions, the OPAS method reset the Trickle algorithm's DIO transmission rate by giving highest priority to joined nodes. If the network adheres to the suggested strategy, the acquired results demonstrate a significant improvement with respect to network joining time[7].

VIII. COOJA SIMULATOR

A simulator for the Contiki operating system is called Cooja. It is written in Java and has a plugin structure for user expansion. Using Java Native Interface (JNI), it is feasible to run native C programmes in the Cooja emulator. The Cooja simulator, in particular, allows for the full execution of the Contiki and Contiki-NG operating systems, ensuring that the software used in simulations and the software used in actual deployments are quite similar. The poor performance of the hardware-emulated devices renders them useless for networks with 100 or more nodes, so this great level of detail comes at a cost. Cooja is only appropriate for networks with up to a few hundred nodes, even when the hardware emulation capability is not employed.

IX. CONCULSION

Internet of Things is the network of devices which are connected with each other via internet or wireless network. Various protocols are there on different layers of IoT. Some of the protocols are RPL, CoRPL, CARPL etc. Routing Protocol for low power and lossy devices is used on the Network layer of IoT. Since, low power devices run on battery so they are prone to security attacks on the network. We study literature and study various aspects of security issues in the network of IoT. There are various attacks like DIS attack, Rank attack, Denial of Service attack, Synchronization attack, Traffic Dispersion, Overloading attack etc. When new nodes join network there is no technique to find the node is malicious or not and check the joining time, energy consumption, latency, packet loss, delay in network formation and stability in a network. Faster network construction with the least amount of resources is still a topic of active research. We need to find alternative solutions for various attacks that are less complex and less time consuming. The security protocols proposed in future security solutions should be adaptable enough to provide security across all network tiers without compromising the network's effectiveness or raising its power consumption. We also look at the problems with end nodes that could disconnect or become unreachable for various causes like battery discharge since low power devices runs on battery, network interference or the issues like packet collision. We will also study all the aspects of security against various attacks in a network in real time scenarios. There are still many issues need to propose and find possible solutions against attacks and also there is a scope to apply Machine Learning to find solutions.

REFERENCES

[1] Kalita, A., Brighente, A., Khatua, M. and Conti, M., 2022. Effect of DIS attack on 6TiSCH network formation. *IEEE Communications Letters*, *26*(5), pp.1190-1193.

[2] Kalita, A. and Khatua, M., 2022. 6TiSCH–IPv6 enabled open stack IoT network formation: A review. *ACM Transactions on Internet of Things*, *3*(3), pp.1-36.

[3] Kalita, A. and Khatua, M., 2021. Adaptive control packet broadcasting scheme for faster 6TiSCH network bootstrapping. *IEEE Internet of Things Journal*, *8*(24), pp.17395-17402.

[4] Kalita, A. and Khatua, M., 2021. Autonomous allocation and scheduling of minimal cell in 6TiSCH network. *IEEE Internet of Things Journal*, *8*(15), pp.12242-12250.

[5] Kalita, A. and Khatua, M., 2021. Opportunistic transmission of control packets for faster formation of 6TiSCH network. *ACM Transactions on Internet of Things*, *2*(1), pp.1-29.

[6] Kalita, A. and Khatua, M., 2020. Channel condition based dynamic beacon interval for faster formation of 6TiSCH network. *IEEE Transactions on Mobile Computing*, *20*(7), pp.2326-2337.

[7] Kalita, A. and Khatua, M., 2020, January. Opportunistic priority alternation scheme for faster formation of 6TiSCH network. In *Proceedings of the 21st International Conference on Distributed Computing and Networking* (pp. 1-5).

[8] https://en.wikipedia.org/wiki/Internet_of_things

[9] https://www.geeksforgeeks.org/rpl-ipv6-routing-protocol/

[10] https://www.geeksforgeeks.org/internet-protocol-version-6-ipv6/

[11] Gallais, A., Hedli, T.H., Loscri, V. and Mitton, N., 2019, April. Denial-of-sleep attacks against IoT networks. In *2019 6th International Conference on Control, Decision and Information Technologies (CoDIT)* (pp. 1025-1030). IEEE.

[12] Micoli, G., Boccadoro, P., Valecce, G., Petitti, A., Colella, R., Milella, A. and Grieco, L.A., 2019, May. ASAP: A decentralized slot reservation policy for dynamic 6TiSCH networks in industrial IoT. In *2019 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 1-6). IEEE.

[13] Smache, M., Olivereau, A., Franco-Rondisson, T. and Assia, T.R.I.A., 2019, October. Autonomous detection of synchronization attacks in the industrial internet of things. In *2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)* (pp. 1-9). IEEE.

[14] Municio, E., Daneels, G., Vučinić, M., Latré, S., Famaey, J., Tanaka, Y., Brun, K., Muraoka, K., Vilajosana, X. and Watteyne, T., 2019. Simulating 6TiSCH networks. *Transactions on Emerging Telecommunications Technologies*, *30*(3), p.e3494.

[15] Shukla, A. and Tripathi, S., 2018, April. Security challenges and issues of internet of things: possible Solutions. In *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)* (pp. 26-27).

[16] Vallati, C., Brienza, S., Anastasi, G. and Das, S.K., 2018. Improving network formation in 6TiSCH networks. *IEEE Transactions on Mobile Computing*, *18*(1), pp.98-110.

[17] Duquennoy, S., Elsts, A., Al Nahas, B. and Oikonomo, G., 2017, June. Tsch and 6tisch for contiki: Challenges, design and evaluation. In *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 11-18). IEEE.

[18] Watteyne, T., Tuset-Peiro, P., Vilajosana, X., Pollin, S. and Krishnamachari, B., 2017. Teaching communication technologies and standards for the industrial IoT? Use 6TiSCH!. *IEEE Communications Magazine*, *55*(5), pp.132-137.

[19] Althubaity, A., Ji, H., Gong, T., Nixon, M., Ammar, R. and Han, S., 2017, September. ARM: A hybrid specification-based intrusion detection system for rank attacks in 6TiSCH networks. In *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1-8). IEEE.

[20] Airehrour, D., Gutierrez, J. and Ray, S.K., 2016. Secure routing for internet of things: A survey. *Journal of Network and Computer Applications*, *66*, pp.198-213.

[21] Dujovne D, Watteyne T, Vilajosana X, Thubert P. 6TiSCH: deterministic IP-enabled industrial internet (of things). IEEE Communications Magazine. 2014 Dec 11;52(12):36-41.

[22] Dujovne, D., Watteyne, T., Vilajosana, X. and Thubert, P., 2014. 6TiSCH: deterministic IP-enabled industrial internet (of things). *IEEE Communications Magazine*, *52*(12), pp.36-41.

[23] Claeys, T., Vučinić, M., Watteyne, T., Rousseau, F. and Tourancheau, B., 2021. Performance of the Transport Layer Security Handshake Over 6TiSCH. *Sensors*, *21*(6), p.2192.

[24] Pokhrel, S., Abbas, R. and Aryal, B., 2021. IoT security: botnet detection in IoT using machine learning. *arXiv preprint arXiv:2104.02231*.

[25] Conti, M., Kaliyar, P. and Lal, C., 2020. A robust multicast communication protocol for Low power and Lossy networks. *Journal of Network and Computer Applications*, *164*, p.102675.

.