The Scientific Temper (2023) Vol. 14 (4): 1412-1418
Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.52
E-ISSN: 2231-6396, ISSN: 0976-8653
https://scientifictemper.com/

REVIEW ARTICLE

Detecting denial of sleep attacks by analysis of wireless sensor networks and the internet of things

R. R. Jenifer*, **V. S. J. Prakash**

Abstract

The internet of things (IoT) amalgamates a large number of physical objects that are distinctively identified, ubiquitously interconnected and accessible through the Internet. IoT endeavors to renovate any object in the real world into a computing device that has sensing, communicating, computing and control capabilities. There are a budding number of IoT devices and applications and this escort to an increase in the number and complexity of malicious attacks. It is important to defend IoT systems against malicious attacks, especially to prevent attackers from acquiring control over the devices. Energy utilization is significant for battery-enabled devices in the IoT and wireless sensor networks which are operated long time period. The denial-of-sleep attack is an explicit type of denial-of-service attack that beleaguered a battery-powered device's power supply that results in the exhaustion of this critical resource. This paper focuses on the survey on denial-of-sleep attacks in Wireless Sensor networks and the IoT.

Keywords: Denial of service, Denial of sleep, Internet of things, Wake-up radio, Network security, Wireless sensor networks, AODV protocol.

Introduction

Sensor nodes are diminutive and economical devices designed to run on battery-powered devices which has some precincts in terms of possessions such as storage, computational and communication competence. Sensors are used in the field of environmental monitoring, health care applications, traffic control and home applications. The wireless sensor network is a network that consists of a collection of self-governing sensors for sensing. The sensors in WSN are energized by batteries.

These sensor nodes congregate data and collaborate with each other and send the deliberated data via wireless communications to the sink. The sink acquires data from sensor nodes, analyses and synthesizes them and serves as the rationale of the interface for the outside world. Using the GSM or internet, the sink is usually linked to the end user. There are usually hundreds, even thousands of sensor nodes, which communicate with the sink in one sensor network. Sensor node has very limited resources such as battery power supply and processing ability. Denial-of-Sleep (DoS) is a special category of denial of service that prevents the battery-powered sensor nodes from going into sleep mode, which affects the performance of the network, Figure 1 represents a DoS attack. In this method, a distributed cooperation-based hierarchical framework (Bhattasali, T., Chaki, R., & Sanyal, S.,2012) is used to perceive the refutation of sleep attacks in WSNs. This technique granted a competent heterogeneous wireless sensor network with an unswerving performance by detecting anomalies in two stages, for minimizing the probability of improper intrusions. To condense the risk of attack, this study secluded the networks from malicious nodes to rebuff receiving fake packets. The compact hierarchical model (Bhattasali, T., & Chaki, R., 2011) is used in heterogeneous wireless sensor networks which is used to notice sleepless nodes exaggerated by the attack. In this method, five layers of hierarchical architecture is created by cluster based on effective energy for increasing its scalability and longevity. In this approach, minimized active sensors achieved energy efficiency. Moreover, the sudden death of sensor nodes is protected by the designed dynamic model. This model has an intrusion detection system through power analysis meticulously used for detecting the intrusion

Department of Computer Science, Cauvery College for Women (Autonomous), (Affiliated to Bharathidasan University), Tiruchirappalli, Tamil Nadu, India.

***Corresponding Author:** R.R. Jenifer, Department of Computer Science, Cauvery College for Women (Autonomous), (Affiliated to Bharathidasan University), Tiruchirappalli, Tamil Nadu, India, E-Mail: ritajenifer.cs@cauverycollege.ac.in

How to cite this article: Jenifer, R.R., Prakash, V.S.J. (2023). Detecting denial of sleep attacks by analysis of wireless sensor networks and the Internet of Things. The Scientific Temper, **14**(4):1412-1418.

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.52

Source of support: Nil

Conflict of interest: None.

Received: 12/10/2023 **Accepted:** 17/11/2023 **Published**:27/12/2023

that occurred in devices. The abnormality of the detection method is engaged in approaches to avoid intrusion detection. In this method (Chen, J. L., Ma, Y. W., Wang, X., Huang, Y. M., & Lai, Y. F.,2011) The DoS attack is identified and rectified by time-division secret key protocol and the simulation results are inveterate that the Cipher function was flawless for WSN. Further, the network lifetime was increased by the detection jamming scheme. The denial-of-sleep attack is detected by a swarm-based defensive technique which is used to determine the traffic impact among sensor nodes (Ghildiyal, S., Mishra, A. K., Gupta, A., & Garg, N.,2014). Oscillation and communication frequency are collected by the ant factors which acted as swarm information. According to the frequency of oscillation, the faulty channel is detected. Data flooding and denial of sleep attacks were reduced by the storm control mechanism. The node humiliates the base station and its wireless receiver, when the frequencies of the packets are received by the system and when the projected frequency configuration is exceeded (Rughiniş, R., & Gheorghe, L., 2010). Table 1 shows the different attacks in wireless sensor networks and the internet of things (Periyanayagi, S., & Sumat, 2013). Table 2 shows the various techniques and protocols used to prevent the DoS attack (Akila, K, Evanjaline, D.J,2019).

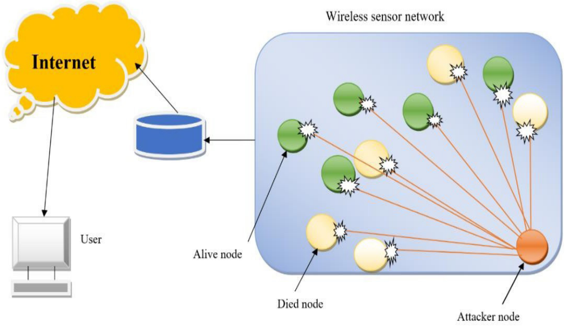

Figure 1: DoS Attack in WSN

Table 1: DoS attacks based on layers

Attacks	*Description*
Physical layer jamming	At constant interference, the data is emitted at regular interval of time.
constant interferences	At Random deceptive, Flooding attack occurred when the attacker acted like a lawful node within the network and constantly sent data. Also when the attacker perceived data transfer within the network then emitted jam signal. Instead of unremittingly sending out a radio signal, the alternation happened between sleeping and jamming by random jammer. Specifically, after jamming for a while, it revolved off its radio and entered a "sleeping" mode.
Random deceptive	Another kind of jammer is a deceptive jammer. It sent a stable stream of bytes into the network to make it look like legitimate traffic. A reactive jammer stayed hushed when the channel is idle, but initiated the transmission of a radio signal as soon as it sensed the activity on the channel.
Reactive functions	At Inference, large amounts of network traffic in the form of radio waves are generated by the attacker, periodically or constantly in order to obstruct with the functioning of a network.
Inference	It transpired when the attacker gained physical access to the node and hindered its functioning or gains access to its memory with the aim to change the information that secured proper functioning.
Node destruction	When two nodes try to send the packets at the same time at the same frequency.
Data link layer	It occurs in the case of constant collisions, which leads to a complete congestion of the channel.
Collision	It occurs with Illegal use of the connection layer that impedes regular activities.
Exhaustion	The malicious node acted as numerous individualities to supplementary nodes in the network that convinced Sybil attack. During the Sybil attack, routing protocols are attacked; the malicious node takes the identity of multiple nodes which leads to conveying multiple routes through it.
Unfairness	The malicious node rejects some of the received packets and forwards to others.
Network layer	During the sinkhole, the malicious node is positioned in such way that all data traffic of an assured area is routed through it, and its role is to reject all received packets. The malicious node is identified by surrounding nodes as the most efficient node to send data through. The node accomplishes this by reducing the number of jumps to the sink using a strong transmitter. The longer the malicious node operates within the network, the more rapidly the number of nodes that send data through it increases.
Sybil attack	During this attack, the attacker sends a broadcast message using strong emission power. A large number of nodes received the broadcast message in that each node decided that the surrounding node was the attacker. Even though the real attacker is usually distanced from the node and actually is out of their range.
Selective forwarding	Legitimate nodes send messages toward the attacker, and in case the attacker receives these messages he rejects or abuses them in other ways. In case messages are not delivered to the attacker node, their content is lost. Namely, a large number of protocols require the broadcast sending of a "hello" message by every single node.
Sinkhole	The attacker tunnels data traffic between one part of the network and the other, using a direct slow-speed connection. In this attack, two malicious nodes are used.
Hello flooding	In Flooding, the attacker sends a large number of requests to establish the connection.
Wormhole attack	It refers to the disconnection of an established connection. Constant sending of establishing connection requests from one or both nodes is required by malicious nodes. so the additional power is wasted.
Transport layer	The attacker tries to surplus the node by stimulating sensors, which originate forwarding of a large amount of data traffic towards the sink. This attack overloads the bandwidth and wastes the node's power.
Flooding	The attacker injects replayed packets as a flood between end-to-end communications. Every node in the path toward the base station forwards the packet, and if large numbers of fake packets are sent all of these become busy. Network bandwidth and energy of the nodes are consumed by this attack.

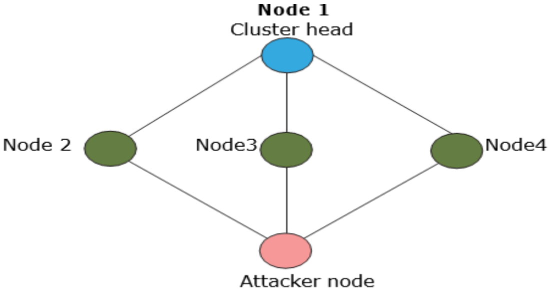

Figure 2: Denial of sleep attack

Existing Methods

Genetic algorithm-based DoS attack detection in WSN (GA-DoSLD)

This paper (Gunasekaran, M., & Periakaruppan, S., 2017) focuses on the misbehaviors of the nodes that are analyzed by a GA-DoSLD algorithm. The generation and distribution of key pairs among the sensor nodes are achieved by the algorithm of a modified RSA (MRSA) in the base station (BS). Before the establishment of sending/receiving the packets, the optimal route is established between the sensor nodes are strongminded by the AODV protocol and then ensure the fidelity of the relay node using the fitness calculation. The crossover and mutation operations are used to find and analyze the methods of the attackers and use them for implementing the attack. During the time of the fortitude attacker node, the BS conveyed the blocked information to all the other sensor nodes in the network. The simulation results confirmed that the recommended algorithm is optimal and coupled to the existing algorithms such as X-MAC, ZKP, and TE$_2$P schemes.

To analyze the misbehaviors of the sensor nodes, there are five key steps involved in GA-DoSLD algorithm.

- WSN initialization
- Population generation and BS configuration
- Generation and distribution of key pair (MRSA Algorithm)
- Route discovery
- Behavior monitoring

The loading of two-hop neighbor information to the base station is initiated by the population generation algorithm; then for every member in the neighbor list, the population is considered as the next neighbor. WSN environment is initialized during this session. At the same time Base station initiated the process to analyze the behavior of the nodes in WSN. MSRA algorithm creates a public key for BS and a private key for sensor nodes for blocking the attacker node at the initial level. A sensor node determines the optimal route using the AODV protocol. Using the optimal path, the sensor node forwards the packets and suspects the other malicious behaviors based on fitness values of flooding of packets and packet size which exceed the data capacity of the sensor node. Figure 2 denotes the DoS attacker node, using the fitness values the sensor node identifies whether the communicated neighbor node is a normal node or an attacker node.

A Secure SWARD algorithm against the denial of service attack

the energy of active IoT nodes and control of sleep mode is achieved by wake-up radios. In this proposed method (Montoya, M., Bacles-Min, S., Molnos, A., & Fournier, J. J., 2018) provided a new way of generating capricious wake-up tokens using recursion calculation which depended on the previous tokens and messages already traded with the main

Table 2: List of protocols and techniques to prevent DOS attacks

Name of the technique	*Protocol*	*Parameter*	*Malicious behavior*
A bayesian game approach	S-Leach	Number of packets dropped, throughput	Reputation
Game theoretic approach	Utility based dynamic source routing (USDR)	Mean no of packets dropped	Reputation
Enforcing security using economical modeling	Secure auction based routing (SAR)	Mean no of packets dropped	Reputation
Frequent game theory approach	Repeated game theory based on DSR	Number of hops for received packets, Throughput	Reputation
Strength based detection and prevention	AODV routing protocol	Packet Delivery Ratio	Reply of Hello Message
An ant based framework	Ant-based routing algorithm	Flooding	The number of packets traveled simultaneously
Protection using KDS	Hybrid energy-efficient distributed clustering (HEED) protocol	Network Lifetime	Node duplication
Message observation mechanism	Message observation mechanism	The loss rate of packets	Content and frequency attack
Cooperative game theoretic approach	Fuzzy-Q learning algorithm	Accurate Defence rate and Energy consumption	Reputation

radio. The SWARD communication protocol engendered an impulsive new wake-up token at every wake-up token conception stage of an IoT node. The token computation is a recursive model that requires only local mode information which is a previous token and securely exchanged messages on the main radio. It integrated a protocol to keep nodes synchronized and to compute tokens when no messages are exchanged.

Securing WSNs against DoS attacks using RSA cryptography algorithm and interlock protocol (ASDA-RSA)

In this method (Fotohi, R., Firoozi Bari, S., & Yusefi, M.,2020) there is two phases in the abnormal sensor detection accuracy (ASDA-RSA) method. During the first phase, the proper cluster head is formed based on energy and distance. The second phase provided the interlock protocol based on the RSA algorithm used to prevent DoS attacks. The member node is selected based on the global positioning system. This node has more energy-efficient among the selected nodes, which is contiguous to the base station that is appropriate for the cluster head. The nodes with the most remaining energy and the slightest distance to the sink are elected to be cluster head nodes.

After the formation of the cluster head along with member nodes, the ADSA-RSA algorithm is formed to prevent the nodes from denial of sleep attacks. This proposed method provides the interlock protocol formed based on the RSA algorithm. RSA is used to perform key exchange along with the node authentication method. AES algorithm is used to perform the encryption of keys. Keys are prone to attacks. The interlocking protocol is used to protect the keys against such attacks. The size of the key employed in the AES code resolved the number of repetition cycles in the conversion, which encoded the input (plain text) to the output (encoded text). Several processing steps in the iteration depended on the encryption key. On the receiving side, aset of reverse cycles are used to translate the encoded text to the original text using a similar encryption key.

The locked key is divided into two parts in the interlocking protocol. The transmitter has sent the first ingredient of the key at the beginning of the process. The second part, however, is transmitted when a response is received by the receiving node. In this proposed method, the AES algorithm divided the encryption key into two parts. In sensor networks, the S-MAC protocol is used to set the sleep periods. In these protocols, the clocks of the nodes are adjusted by the synchronization signals. In these protocols, a large number of control messages, such as RTS and CTS, are utilized, which are referred to as synchronization packages (SYN). Denial of Sleep attack sends repeated control packets such as RTS messages, which are used to prevent the nodes from entering into a sleep mode, leading to energy consumption. Node authentication is at the cluster level. The reason to use the RSA algorithm is that in all symmetric key encryption algorithms, the sender and receiver of the message should be acquainted with the encryption key. The message from the sender used a unique and secret key for encryption, and the message of the receiver side used the same key for decryption, revealing a key from one of the message recipients that imperils everyone's security. The RSA algorithm is a public key method. RSA algorithm is used to validate the nodes using the public and private keys

Securing WSN from DoS by isolating nodes: (SWSNDoSIN)

This paper recommended feasible clarification to decipher the problem of denial of sleep attacks by isolating the nodes using hierarchical clustering. The main intention of this research work is to increase the lifetime of a node by saving energy which to be infatuated by the denial of sleep. In this paper, the LEACH protocol is used which created a hierarchical cluster with no particular cluster head with different energy levels. Sensor node has schedule time which contains node's active and sleep schedule time. A node can sense the data and transmit the data in an active schedule and goes to sleep mode to conserve energy (Kaur, S., & Ataullah, M., 2014)

Conservation of energy in wireless sensor networks by preventing denial of sleep attack (CEWSNPDoSA)

This proposed method of the zero-knowledge protocol is recommended for corroborating and authenticating of the sensor nodes which passed the sleep synchronization messages. Hashing and interlock protocol is used for exchanging the key between the prover and verifier. Figure 3 demonstrates zero-knowledge mechanism which is used for authenticating the base node. Selective local authentication is used to detect the denial of sleep attacks. RSA algorithm is exploited to create a public and private key for exchanging information securely. The keys are exchanged by using the interlock protocol to secure this communication from man-in-middle attack (Naik, S., & Shekokar, N., 2015)

Dos attack prevention technique on wireless sensor networks

In this proposed method, the Co-FAIS technique is used to detect and prevent DoS attacks which uses fuzzy logic to improve the accuracy rate of Dos attack detection and

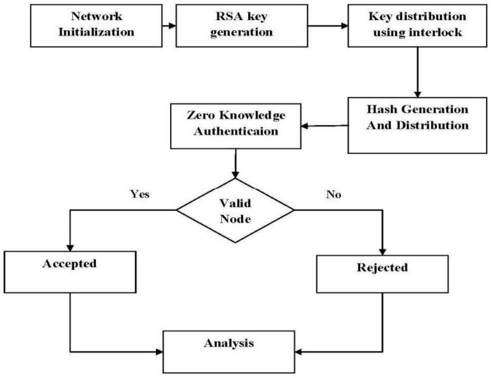
Network Initialization
RSA key generation
Key distribution using interlock
Hash Generation And Distribution
Zero Knowledge Authenticaion
Valid Node
Yes
No
Accepted
Rejected
Analysis

Figure 3: Workflow of zero knowledge mechanism

improve the capabilities of learning. Co-FAIS consisted of six modules which are listed in Table 3.

Threshold-based algorithm for the detection of DDoS attacks in WSN

The proposed research work (Sharma, P., & Sharma, M., 2019) suggested the methodology to detect and isolate the malicious node from the network for improving the lifetime of the node. In this proposed work, key servers are used to register the sensor node itself. When all the nodes are started to transmit the data in the network, the DDoS attack is triggered in the network, the throughput of the network gets reduced to a threshold value then malicious node detection is started. The communicated nodes are considered slave nodes. The technique of monitor mode is applied on the slave node. The slave node with monitor mode is used to detect the malicious node (Patil, S., & Chaudhari, S. 2016). Introduced new methodology for determining the threshold of the low power node and medium, high power nodes. The threshold value is calculated based on the energy of the sensor nodes. Based on the energy level, the member nodes are classified into low-power, medium-power and high-power nodes.

Secure routing against DDoS attack in WSN

This proposed methodology (Nagar, S., Rajput, S. S., Gupta, A. K., & Trivedi, M. C., 2017) introduced a secure routing protocol for wireless sensor networks which is proficient to prevent the network from DDoS attacks. This research work suggested two procedures, which are i) propagating DDoS Attacks on a normal network, ii) conquering the network from attack infection. Intrusion prevention methodology is used to protect the network and nodes act as IPS nodes which are operated in their radio range for the region and examine the neighbor nodes regularly. IPS nodes found any misbehavior node that involved blocking the infected node and informed to the sender to change to another route.

Performance analysis of denial of service and distributed (DoS) attack of the application and network layer of IoT

The proposed research (Alahari, H. P., & Yelavarthi, S. B., 2019) work introduced the distributed denial of service attack algorithm. In this DoS attack, the network traffic arrives from different attacking sides. The solution for this attack is blocking a single IP address making it not probable to thwart the attack. In a typical DDoS attack, the aggressor started by exploiting susceptibility in one system and by creating it the DDoS master. The master attacking system concedes diverse exposed systems and gains management on them either by infecting different systems through bypassing the authentication controls that are by approximation default parole on a widely used device or with malware. A system or a networked device underneath the management of an attacker is understood as a bit or a zombie. Bot master controls a larva net. Botnets will comprise any range of bots; in botnets, there's no higher limit to their size as a result, in present days DoS is also exemplified by the method that the attack uses.

Denial of sleep attack detection using mobile agent (MA) in wireless sensor networks

In this research work, the algorithm of the sleep attack detection algorithm (Mahalakshmi, G., & Subathra, P., 2018) is introduced to identify the DoS using a mobile agent, trust value, random key pre-distribution, and random password generation. A mobile agent is a self-determining computer program that executes continuously on cross-platforms. In this research, the role of the mobile agent is to monitor the wireless sensor network and show the reaction to the intrusion. The trust value is calculated by the formula of

Initial trust value = 0

Updated trust value=old trust value+1 (between the nodes 1 to 9

Updated trust value = old trust value+(correctly transmitted packets)/10

(Greater than 10 nodes)

In the random key pre-distribution method, a random password generator is used to generate a random password. The source node wants to communicate with the destination node; the mobile agent's role is to compare the id of the source node, trust value, and random password. When

Table 3: Co-FAIS modules and their functionalities

Module	*Functionalities*
Sniffer module	It establishes log file of packets
Fuzzy misuse detector (FMD) module	Fuzzy oriented module. It initiated threat profile with six parameters which are Eu is the energy consumption of sensor node, Tr is the variance of the time difference between two connections, Bs indicates the length of the packets, Co is the no of connections, Tt is denoted as throughput which is number of received packets, Si is the sleep interval
Danger detector module	It calculates the difference between malicious packets and normal packets4
Fuzzy Q-learning vaccination (FQVM) module	It is used to observe factual attacks. In this module, a Fuzzy min-max action selection and reward function with Q-learning is used.
Cooperative decision making module	It combined FMDM and FQVM to analyze the attack
Response module	This module is designed to update the database

Table 4: The existing method's key points and confines

Author *proposed protocol/algorithm*	*Protocol Performance*	*Advantage*	*Issues*
Mahalakshmi Gunasekaran Subathra Periakaruppan AODV Routing Protocol GA-DoSLD Algorithm MRSA Algorithm	MRSA Creates Private and Public Key Provides Optimal Route Monitors the behavior of the sensor nodes	The attacker was identified at the initial level Network parameters are analyzed	It covers a limited number of static nodes It consumes a considerable amount of energy
Maxime Montoya, Simone Bacles-Min, Anca Molnos SWARD Communication Protocol	It provides a Secure and Energy-efficient method to create wake-up tokens	Secure Communication	Network parameters are not analyzed
Reza Fotohi, Somayyeh Firoozi Bari, Mehdi Yusef ADSA-RSA Algorithm S-MAC Protocol	It provides public and private keys to prevent the nodes from attackers	Secure Communication	Network lifetime is not measured
Simerpreet Kaur ,Md.Ataullah LEACH Protocol	It provides an efficient way to consume the energy	Optimized energy utilization	Security is not analyzed
Swapna NaikNaik, Dr.Narendra Shekokar RSA Hashing and Interlock Protocol ZKP	It ensures the security Mechanism to provide the functionality of the key exchange It provides the authentication of the base node	Power Consumption Better Security Concern	Network lifetime is not measured
Shital Patil, Sangita Chaudhari Fuzzy Logic	It consumed six modules to detect and prevent the nodes from DoS attack	It improves the accuracy of the system	Network parameters are not analyzed
Poonam Sharma, Megha Sharma Based on the Threshold Value	The threshold value detects and isolates the malicious node from the network	It improves the throughput and reduces network delay	Network parameters are not analyzed up to 100%
Surendra Nagar, Shyam Singh Rajput, Avadesh Kumar Gupta, Munesh Chandra Trivedi Secure AOMDV routing protocol	i) promulgate DDoS attack on a customary network ii) conquer the network from attack infection	It prevents the network from DDoS attacks by blocking intruder nodes	Throughput is not analyzed
Hanumat Prasad Alahari, Suresh Babu, Yelavarthi Distributed Denial of Service Algorithm	It provides the algorithm to secure the servers	It prevents the server from crashing when it overloaded with many users' data	Network parameters are analyzed
G.Mahalakshmi and Dr.P.Subathra Mobile Agent Trust value Random Key pre-distribution Random Password Generator	It acted as an intermediator between a source node and a destination Trust value calculated for source and destination A random key generator generated the password	-	-

these are matched with the destination, the communication between the source and destination is established. The malicious node detection is informed to the base station and the base station records and alerts the sensor nodes in the network. Table 4 summarizes the key points and confines of the existing methods.

Conclusion

There are N number of attacks like DoS that can impediment the functioning of wireless sensor networks and the internet of things. Limited battery life has crooked energy utilization is some of the foremost confronts in these networks. There are many algorithms and mechanisms used for network security and it also helps to prevent the above-stated attacks. But those are of no use for WSN due to their constraints. In future works, intend to develop algorithms and methods to prevent the nodes from DoS and sustain the battery life and Energy of the nodes.

References

Akila, K, Evanjaline, D.J(2019) "Strengthening IoT-WSN architecture for environmental monitoring" in International Journal of Innovative Technology and Exploring Engineering,8(11),112278-3075

Alahari, H. P., & Yelavarthi, S. B. (2019, January). Performance analysis of denial of service dos and distributed dos attack of application and network layer of iot. In 2019 Third International Conference on Inventive Systems and Control (ICISC) (pp. 72-81). IEEE.

Bhattasali, T., & Chaki, R. (2011). Lightweight hierarchical model for HWSNET. arXiv preprint arXiv:1111.1933.

Bhattasali, T., Chaki, R., & Sanyal, S. (2012). Sleep deprivation attack detection in wireless sensor network. arXiv preprint arXiv:1203.0231.

Chen, J. L., Ma, Y. W., Wang, X., Huang, Y. M., & Lai, Y. F. (2011). Time-division secret key protocol for wireless sensor networking. IET communications, 5(12), 1720-1726.

Fotohi, R., Firoozi Bari, S., & Yusefi, M. (2020). Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. International Journal of Communication Systems, 33(4), e4234.

Ghildiyal, S., Mishra, A. K., Gupta, A., & Garg, N. (2014). Analysis of denial of service (dos) attacks in wireless sensor networks. IJRET: International Journal of Research in Engineering and Technology, 3, 2319-1163.

Gunasekaran, M., & Periakaruppan, S. (2017). GA-DoSLD: genetic algorithm based denial-of-sleep attack detection in WSN. Security and Communication Networks, 2017.

Kaur, S., & Ataullah, M. (2014). Securing the wireless sensor network from denial of sleep attack by isolating the nodes. International Journal of Computer Applications, 103(1).

Mahalakshmi, G., & Subathra, P. (2018). Denial of sleep attack detection using mobile agent in wireless sensor networks. Int J Res Trends Innov, 3(5), 139-149.

Montoya, M., Bacles-Min, S., Molnos, A., & Fournier, J. J. (2018, June). Sward: a secure wake-up radio against denial-of-service on iot devices. In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (pp. 190-195)

Nagar, S., Rajput, S. S., Gupta, A. K., & Trivedi, M. C. (2017, February). Secure routing against DDoS attack in wireless sensor network. In 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 1-6). IEEE, (IEEE-CICT 2017)

Naik, S., & Shekokar, N. (2015). Conservation of energy in wireless sensor network by preventing denial of sleep attack. Procedia Computer Science, 45, 370-379.

Patil, S., & Chaudhari, S. (2016). DoS attack prevention technique in wireless sensor networks. Procedia Computer Science, 79, 715-721..

Periyanayagi, S., & Sumathy, V. (2013). Swarm based defense technique for denial-of-sleep attacks in wireless sensor networks. Int. Rev. Comput. Softw.(IRECOS), 8(6), 1263-1270.

Rughiniş, R., & Gheorghe, L. (2010, June). Storm control mechanism in wireless sensor networks. In 9th RoEduNet IEEE International Conference (pp. 430-435). IEEE.

Sharma, P., & Sharma, M. (2019). Threshold based algorithm for the detection of DDOS attack in wireless sensor networks. Int. J. Recent Technol. Eng.(IJRTE), 8(4), 1869-1873.