Elaborative Investigation of Denial of Services on Wireless Sensor Networks

Sovon Chakraborty (ID 22366023)

Abstract

Wireless sensor networks are the new emerging technologies that are the combination of wireless devices, small, effective sensors and special embedded system design with them. Basically WSN gathers data from very sensitive and harsh environments. Then after processing,they transmit all the information to base station or user application for their further use. But in their design,there is some design constraints like less memory,power or less secured system. For this they have faced lots of attacks . Denial of service (DOS) is one of the most crucial of them which attacks the whole network system on each layer separately and makes the whole network paralysed and jeopardized. In this review paper, all the attacks of DOS are discussed and their countermeasures are also discussed here attack wise.

Keywords: Denial of Service (DOS), Detection, Wireless Sensor Networks (WSN)

Introduction:

Wireless sensor networks are getting much attention and popularity day by day because of its vast application on different parts of human life. It is basically making life easier by getting the updated information from its combination of wireless technology, tiny sensors and embedded systems and devices. WSN can work in any environment like rain , sunlight, cold breeze and also in harsh environment. So it also has to face some attack on it . Denial of service (DOS) is one of those attacks . Because of its design constraints , it is much weaker against those attacks. So in order to get the proper feedback from the sensor nodes of WSN proper counter measures should be taken against those attacks. Wireless sensor networks are basically a sensory system which sense the different parts of environment and gather needed information . It is used in different sectors like monitoring of traffics, to diagnosis of healthcare problems, nuclear plantation, military network communication,weather update and information collection, ensuring security of a system etc. Wireless sensor networks must deliver security, integrity and correct output. But because of low power consumption, their tiny body structure and limitations of memory, DOS attack easily takes place and security vulnerability increases . Wireless sensor networks are much easier to implement in any situation and environment ,it is also very cost effective super fast than any other sensory device. tacks .

So the use of WSN is increasing rapidly. Also the attack generation is much more easier so proper countermeasures should be taken against it. Basically different network layers have to face different types of attacks . So in this paper, DOS attacks on different network layers are discussed properly and the available countermeasures are also available in this paper for ensuring the security, non repudiation and integrity of different layers.

Background Study

Properties of wireless sensor networks and its constraints

A wireless sensor network is basically an embedded system which has 3 parts. First, it has some sensor which will sense the parameters.Then it is embedded tiny body where these sensors and other equipment like flash memory, batteries for power, etc and a medium by which it transfers, the collected data to end point application. Sensor plays the most vital role by sensing the environment, gather the proper information and transmitingt this data to the user applications for further use. The sensor is consists of 4 major works:

a) **Sensing the environment :**sensors gather the information and there is an ADC (analogue to digital converter)inside it which converts the collected analogue data into digital signal.

b) **Processing the sensed data:** then this digitized data is processed by a processor after that it remains in storage memory of it. But the capacity of both the processor and memory is very low and short span.

c) **Transmission and receiving these processed data:** transfer and receiving of this data is done by a single transceiver module.

d) **Power supply:** Solar cells, batteries are the best options for power supplies. There is something alarming in the design of wireless sensor networks and that is their limited capacity of storage and also limited capacity of processing. These two constraints put them in danger and make a way for the intruder and hackers people to attack using these lacking. As wireless sensor networks give first priority to decreasing the costs,they make a huge lacking on other sides like increasing their capabilities or giving strong secured sensor system. So the main constraints of WSN are:

- There is only one flash memory and one RAM flash memory, so after installing all the application and operating system programs there remains only few spaces that is not sufficient.

- There is no segmentation in the messages and the message size of WSN is very small.

- In WSN, same data and information can be collected by more than one nodes or many nodes. So unnecessary data redundancy occurs.

- As it has low capacity processor, it's low computational capability is found and very low bandwidth and radio frequency are very high.

- There can be hundred of nodes or more than that in one WSN .So identifying each node with separate global address is quite challenging and impossible.

- Location management for the nodes of harsh and unmanageable environment is much difficult.

Wireless Sensor Networks Design issues :

Development of wireless sensor networks are not easy task as it has to contain a lot of sensors and circuits including external hardware in their tiny embedded system. It has to must ensure some parameters for working appropriately. Like :

Fault Tolerance : Sensor nodes can fail anytime anywhere because of its physical damage or other attack issues. So it must be implemented in their design protocol to identify this sensor failure as soon as possible and inform the other part any other connected sensor.

Scalability : The sensor node and other chips must be scalable for any other neighbouring networks so that it can work on different levels of sensing the parameters.

Hardware Constraints : In every wireless sensor network, there must be four components : a power supply system, a unit for transmission, a separate unit for the sensors but not the least a processing unit for processing rest of the 3 parts. Despite having this, additional equipments or devices can be added or subtracted from the system.

Production Cost : Above , we must keep that in mind that the whole system have to be cost effective and budget friendly for people of all clasees who want to afford it.

Network topology of sensors : We have to design such a system, where network topology can be maintained properly by reducing the wasting energy. There are basically 4 pure topologies like : bus , star, mesh and ring.

Transmission media : We need to choose such a medium where the loss will be minimum, which will be robust free and can transmit fluently without any pause or breaking.

Wireless Sensor Networks Types:

Mobile WSN
Multimedia WSN
Terrestrial WSN
Underground WSN
Underwater WSN

Application of wireless sensor networks:

Machine health monitoring
Data logging
Earth/Environmental sensing
Monitoring Air Pollution
Landslide detection
Forest Fire Detection
Monitoring water quality
Natural disaster prevention
Water waste monitoring
Producing wine

Security Requirements :

Security requirements basically ensure that the transmitted data over the medium will be secured and no one will alter or delete any important information of it. Each and every node will be authorized by authorities and only they can take part in data exchange and passing. No trusted nodes can be masquerade by any malicious node. There must be integrity, non repudiation , confidentiality and security in every message passing.

Threat Model

Threats can be generated by the intruders or the outsiders of the network. When an insider attacks the system, then it is called native attack and it is much dangerous and harmful for the system than the outside attacks as the attacker knows many confidential and hidden information of that system network. Also it is very challenging to find out the insider. Also when an attacker attacks the system and change or alters the information of the message, it is called active attack. But in passive attack, no alterations can be done by the attacker.

Denial of service attacks and its effects:

When the attacker makes the system or the network inaccessible and uncontrollable , it is called denial of service attacks. DOS attack can be found in the network like software bug, complicated accessing of application, exhaustion of resources etc. Basically DOS attack is generated intentionally and it hampers the total system capabilities and stop the regular functionality of the system steps. In most of the situations, attacker creates DOS attack to disturb, interrupt or destroy the whole network. After this DOS takes place, some situation arise. That are :

- Sensors can transfer abnormally more data packets by gaining energy
- Intermediate and sender/ receiver nodes are not working - Clusters are not uniformly distributed
- There remains a chance of high loss of the transmitted packets
- An attacker can create a jam in the medium by remaining there and can send malicious traffic
- Attacker can create false message by taking the control of any nodes in WSN
- Attackers can target to do the power drainage of the sensors by
- Attacker can also create a unfavorable situation to prevent DOS attack also as they have much resources and techniques.
- They can loss energy of sensor nodes by creating false communication and keeping the nodes busy.

Denial of service attack format:

Basically DOS attacks don't need any special program or place for generating the attack. It only targets the lacking or the vulnerability of the network communication and attack. DOS attacks mainly continuously stream some fake requests and send them to the server. Then the server usually responses with real answers . But after this, when attacker continuously streams repeated values, the server get confused and shut down.That's how the attacker successfully paralyses the system and prevents it from working. Denial of service attack creates an immense loss on organizations , office, financial sectors, confidential data and many more. We can detect denial of service attacks symptoms by following some steps.

1. Using traffic analytic tools to detect any DOS symptoms.
2. If an individual single IP range or IP address is generating a numerous amount of traffific, then it is suspicious.
3. If a single behavioral profile like a user/ web browser/ geo location is sending a flood of traffic then it is a symptom of DOS attack.
4. A request from an unexplained surge to become an endpoint.
5. Odd traffic patterns like the pattern does not look natural or it is giving spikes in the odd hours of working.

Related Work

In this section,basically different papers are discussed with their method,pros and cons of detecting DOS attacks on wireless sensor [1-5] networks. In [6] and [7], Denial of Service Attacks are categorized . In [6], these are basically the layers where the attack occurs. The layers are : Physical layer DOS attacks, Link layer DOS attacks, Network layer DOS attacks and Transport layer DOS attack. There are primary and secondary security goals for preventing security attacks in WSNs which should be supported by the security mechanisms. Confidentiality,Availability Authentication and Integrity are the four primary goals on the other hand Secure Localization,Time Synchronization, Self-Organization, and Data Freshness are the four secondary goals for WSNs. Two subcategories of security attacks for WSNs can be categorized, Passive attacks and Active attacks. The well-known counter measures and security mechanisms of all the attacks are also mentioned in this article. In [2],this article contains custom dataset of intelligent underwater wireless sensor network which can be divided into four categories of DoS attacks (gray hole, black hole, scheduling attacks and flooding).Method used to train datasets is Artificial Neural Networks to classify them into different DoS attacks. The experimental work carried out here has a high classification rate and accuracy, which is worth mentioning attack with the suggested dataset.To create the structure of an intrusion detection system to resist DoS attacks at an affordable cost is the main goal of this paper.The results considered have been successfully classified as a DoS attack with higher detection rate. In [8], The purpose of this research is to design WSN DoS attack detection system with energy consumption, optimized cost,security and complexity.The data set is structured as the DoS attacks are divided into four types: gray holes, black holes,scheduling and flooding. For testing performance of DoS detection on WSN dataset decision tree and support vector Machine learning [9-13] algorithms are used. Experimental results shows that decision tree technology has achieved higher True positive rate and lower false positive rate achieved by Support vector machines. The rate of percentage : 99.86 percentage vs 99.62 percentage and 0.05 percentage vs 0.09 percentage respectively.In [14], DoS attacks and various Countermeasures have been discussed in this report. Some of the defense mechanism provided also has some limitations and can defeated by the attacker’s counterattack.Most threat types can be overcome by Authentication and anti-replay mechanism. Other methods can also avoid or detect and recover from attacks, but these solutions can also be defeated by some counter mechanisms. This is why we need to find some specific remedies and research them to protect DoS. In [15], A hierarchical clustering system (HCS) is proposed to improve accuracy to prevent DoS attacks and extend network life. In the proposed mechanism,Hierarchical Cluster System (HCS) without any specific cluster head is formed based on the energy level of the sensor node. any abnormal packages through detection can be detected by nodes with super energy.Refusal of sleep attacks is a serious difficulty in wireless sensor networks.The result of solving this difficulty was implemented. HCS protocol is very suitable for largescale The internet. The protocol described above can also manage the denial of sleep attacks in the following ways Find the detection and in [16],This article reviews denial of service attacks(DoS) in the information system by using citation mapping tools and citation networks analysis (CNA). For implementation a framework is presented for defense mechanism against DoS attacks. Citation network analysis also Shown in the results.To identify important works related to research citation network analysis in Web of Science (WoS) is used. Types of DoS attacks and defense mechanisms for defending security attacks with the help of intelligent systems are proposed in this paper. To Protect information systems Information security policy also plays an important role. In [17] an [18], Different layers of WSN features, constraints and types of various DoS attacks are focused in this paper.In many cases, the attack may overlap each other. Any intentional or unintentional DoS situation in WSN needs to be resolved by powerful mechanism. Always recommend develop and deploy appropriate measures in WSN.in [19],This article examines DoS attacks and Propose a strategy based on clustering technology. This method is compared with other related methods Agreement, the results show that our method can effectively detect and defend against DoS attacks for wireless sensor network.In this article, a unique detection and defense method called DoS attacks in WSN is proposed. Hash function and encryption technology used to ensure the authenticity and integrity of data in the network. DOSAC scheme

generates unique code and hash value to verify transmission data pack. The simulation results show that can effectively detect and defend DoS attacks in WSNs.In [20],The purpose of this survey is to provide up-to-date information on different types of DoS attacks and defense technologies of WSN, the improved changes, according to recent works.Information about attacks and their defense mechanisms, focusing on the different layers of the hybrid layered model have been structured.This method clearly specifies which type of DoS threats will be encountered at which layer, and what is the corresponding defense technology. This survey also makes it easier for people to consider different changes in prevention mechanisms, which can lead to major improvements and safer networks. It also provides key analysis and comparison of these defense technologies for further improvement. In [21],This research work analyzes the performance of professionals constitute Optimized energy-based constraint DoS detection algorithm, which has three different modules, such as energy, bandwidth and attacker detection unit and compare with existing Offloading Denial of Service Attack Detection with Energy Constraint in WSN.The proposed work has been implemented by using a network simulator. From the simulation results it can be seen that the proposed OBES algorithm is efficient because it provides more usable energy
and reduces latency less data packet loss, longer network life. The OBES algorithm can achieve a higher network lifetime before and after the attack detection model. It helps reduce energy consumption, high security and long network life wireless sensor network. In [22],This article covers the basic threats that are threatening WSN is available every day. The main part of this article describes DOS's attack on WSN and solutions suggested by literature used to detect and resolve specific attacks.The attack will cause the WSN to be completely or partially shut down.Therefore, a lot of research is not surprising once a day to protect WSN from different and various DOS attacks. DOS attacks can be divided into multiple categories. The attacks are classified according to the protocol stack layer [23].The most threatening attack is a DOS attack on a physical device layer, on connection layer, at the network layer, transport layer.

Comparative Study

In TCP-IP model there are five layers these are physical layer, link layer, network layer, transport layer and application layer. Different kinds of layers have different kinds of DOS attacks. In this section, we will show a comparative analysis on different types of DOS attacks and counter measures.

Attacks on application layer

Path based denial of service

In response a network when some packets are inserted into the
leaf nods they travel to base station and waste the energy, bandwidth of that node. For this reason one authenticated become unable to trans fer the data to base station .

Overwhelming sensor node

For application layer it is a very common attack. In these types of attacks some fake nodes can overwhelm the whole system by prompting the sensors. For this big portion of traffific is sent to end points. So bandwidth and power both are unnecessarily wasted.

Attacks on Transport layer

Content Attack

In this type of attack, the attackers change the serial of the message and insert unnecessary or fake contents in it message.

Synchronize flood attack

In this type of attack the attackers send continuous connection request, As a result all the resources become blocked and exhausted. For these requests the system reaches on maximum limit and starts to ignore the legitimate requests.

De-Synchronize attack

In this types of attack fake re-transmission requests are generated for missed contents or frames. It basically drains the energy of end systems by generating spoof messages.

Attacks on Network layer

Hello flooding

Hello flooding is one kind of flooding attack in which huge traffic is generated by unnecessary messages. So it makes all the channel congested. Attackers use RF transmitters to generate these attacks.

Spoofing

Spoofing attack is one of the most serious attacks. In this type of attack the attackers inside the network and cuts off all the communication packets which are sent to it. It is very much difficult to identify because it can pretend as a base station too and can forward packets in different nodes disguised with a fake identity and harms all the transmissions of different nodes. One attacker may have multiple fake identity as well.

Black whole attack

It is one of the most dangerous attacks in network layer. It is a very well known attack all over the world. In this type of attack a false node pretends and becomes a authenticated node.

Attacks on Data Link layer

Denial of sleep

Denial of sleep attack basically targets the MAC layer. A simultaneous fake traffic tries to keep the node always awake. So for these nodes, radio can not go to sleep mode and power sources are heavily drained.

Collision

These types of attacks take place when an equal frequency channel try to access it for continuous transmission. Packet collisions are increased for this. Interrogation attacks basically generate some fake RTS(Request to send) which make the node busy and the real RTS is missed by the node. It is a very well known attack.

Attacks on Physical layer

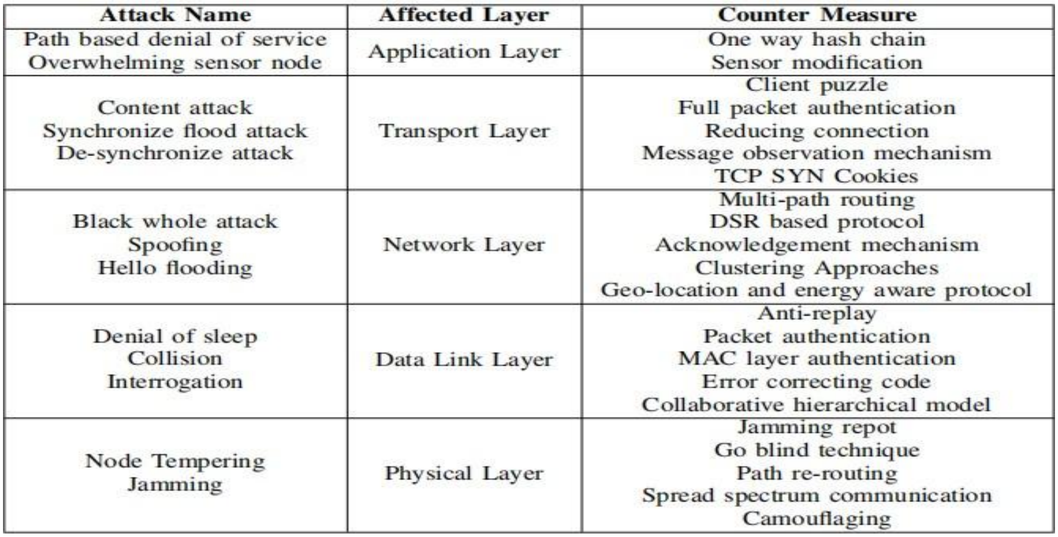
Node Tampering

By these types of attacks nodes are physically tempered. By damaging the node the attacker can retrieve sensitive information(Keys) and communicate in higher level.

Jamming

In physical layer it is the most common type of attack. By generating false traffic the attackers make the network jammed. For this reason the authenticated transmissions cannot be done. There are different kinds of jamming attacks like Reactive, Random, Content or Deceptive.

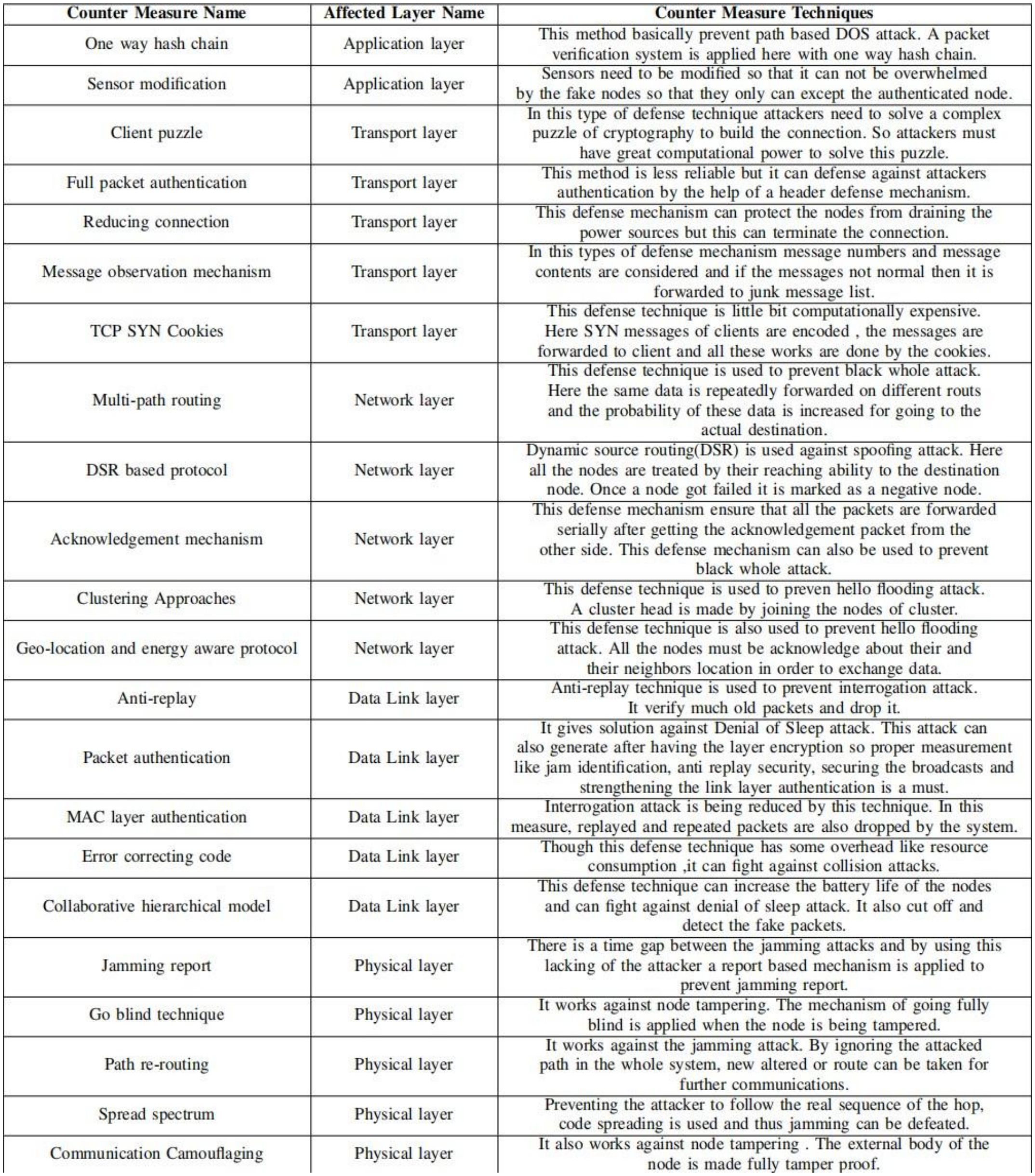
TABLE I
DIFFERENT DOS ATTACKS ON DIFFERENT LAYERS



Attack Name	Affected Layer	Counter Measure
Path based denial of service Overwhelming sensor node	Application Layer	One way hash chain Sensor modification
Content attack Synchronize flood attack De-synchronize attack	Transport Layer	Client puzzle Full packet authentication Reducing connection Message observation mechanism TCP SYN Cookies
Black whole attack Spoofing Hello flooding	Network Layer	Multi-path routing DSR based protocol Acknowledgement mechanism Clustering Approaches Geo-location and energy aware protocol
Denial of sleep Collision Interrogation	Data Link Layer	Anti-replay Packet authentication MAC layer authentication Error correcting code Collaborative hierarchical model
Node Tempering Jamming	Physical Layer	Jamming repot Go blind technique Path re-routing Spread spectrum communication Camouflaging

Open Issues and Conclusion

Wireless Sensor Networks are nowadays a most picked up and trendy topic for research and development topic. Because of having low cost design and friendly interface for use, it is everywhere for gathering information from sensitive places. But it has many constraints which was discussed in previous sections and for this it has to face many serious attacks. There is a saying that prevention is better than cure and for this case, it is hundred percent applicable. If the proper attack management system and measure can be ready before the attacker can take a chance, then the wireless sensor networks will be much secured and exact. Also the design issues can be changed so that it can consume more memory and can have more battery life to serve more. So future work must be on prevention techniques before the attacks rather than dynamically facing the attack. Recently a work has been imposed to prevent denial of service attacks having the title a work has been imposed to prevent denial of service attacks having the title CO-FAIS (cooperative fuzzy artificial immune system) which can be great research to prevent and cure all types of DoS before it took place. can be a great research to prevent and cure all types. Nowadays wireless sensor networks are gaining much popularity for their simple design structure, less complexity in computation and cost effectiveness. But this simple design led this whole system into danger. For this simple and easy structure, attackers can easily cut off different layers security settings . In this paper, different kinds of DOS attacks in different different layers of TCP/IP model has been showed . Also the countermeasures of each individual attacks are being discussed. But there is no fifixed attack and no fixed solutions for all the attack prevention. So in order to assure the data and transportation security, the design must be upgraded , high encryption and more reliable devices should be introduced and all the nodes must be error less individually.



Counter Measure Name	Affected Layer Name	Counter Measure Techniques
One way hash chain	Application layer	This method basically prevent path based DOS attack. A packet verification system is applied here with one way hash chain.
Sensor modification	Application layer	Sensors need to be modified so that it can not be overwhelmed by the fake nodes so that they only can except the authenticated node.
Client puzzle	Transport layer	In this type of defense technique attackers need to solve a complex puzzle of cryptography to build the connection. So attackers must have great computational power to solve this puzzle.
Full packet authentication	Transport layer	This method is less reliable but it can defense against attackers authentication by the help of a header defense mechanism.
Reducing connection	Transport layer	This defense mechanism can protect the nodes from draining the power sources but this can terminate the connection.
Message observation mechanism	Transport layer	In this types of defense mechanism message numbers and message contents are considered and if the messages not normal then it is forwarded to junk message list.
TCP SYN Cookies	Transport layer	This defense technique is little bit computationally expensive. Here SYN messages of clients are encoded , the messages are forwarded to client and all these works are done by the cookies.
Multi-path routing	Network layer	This defense technique is used to prevent black whole attack. Here the same data is repeatedly forwarded on different routs and the probability of these data is increased for going to the actual destination.
DSR based protocol	Network layer	Dynamic source routing(DSR) is used against spoofing attack. Here all the nodes are treated by their reaching ability to the destination node. Once a node got failed it is marked as a negative node.
Acknowledgement mechanism	Network layer	This defense mechanism ensure that all the packets are forwarded serially after getting the acknowledgement packet from the other side. This defense mechanism can also be used to prevent black whole attack.
Clustering Approaches	Network layer	This defense technique is used to preven hello flooding attack. A cluster head is made by joining the nodes of cluster.
Geo-location and energy aware protocol	Network layer	This defense technique is also used to prevent hello flooding attack. All the nodes must be acknowledge about their and their neighbors location in order to exchange data.
Anti-replay	Data Link layer	Anti-replay technique is used to prevent interrogation attack. It verify much old packets and drop it.
Packet authentication	Data Link layer	It gives solution against Denial of Sleep attack. This attack can also generate after having the layer encryption so proper measurement like jam identification, anti replay security, securing the broadcasts and strengthening the link layer authentication is a must.
MAC layer authentication	Data Link layer	Interrogation attack is being reduced by this technique. In this measure, replayed and repeated packets are also dropped by the system.
Error correcting code	Data Link layer	Though this defense technique has some overhead like resource consumption ,it can fight against collision attacks.
Collaborative hierarchical model	Data Link layer	This defense technique can increase the battery life of the nodes and can fight against denial of sleep attack. It also cut off and detect the fake packets.
Jamming report	Physical layer	There is a time gap between the jamming attacks and by using this lacking of the attacker a report based mechanism is applied to prevent jamming report.
Go blind technique	Physical layer	It works against node tampering. The mechanism of going fully blind is applied when the node is being tampered.
Path re-routing	Physical layer	It works against the jamming attack. By ignoring the attacked path in the whole system, new altered or route can be taken for further communications.
Spread spectrum	Physical layer	Preventing the attacker to follow the real sequence of the hop, code spreading is used and thus jamming can be defeated.
Communication Camouflaging	Physical layer	It also works against node tampering . The external body of the node is made fully tamper proof.

Table 2 COUNTER MEASURES OF DIFFERENT DOS ATTACKS

References

[1] Javed Mehedi Shamrat F.M., Allayear S.M., Alam M.F., Jabiullah M.I., Ahmed R. (2019) A Smart Embedded System Model for the AC Automation with Temperature Prediction. In: Singh M., Gupta P., Tyagi V., Flusser J., Ören T., Kashyap R. (eds) Advances in Computing and Data Sciences. ICACDS 2019. Communications in Computer and Information Science, vol 1046. Springer, Singapore. https://doi.org/10.1007/978-981-13-9942-8_33

[2] F.M. Javed Mehedi Shamrat, Shaikh Muhammad Allayear and Md. Ismail Jabiullah

"Implementation of a Smart AC Automation System with Room Temperature Prediction ", *Journal of the Bangladesh Electronic Society*, Volume 18, Issue 1-2, June-December 2018, ISSN: 1816-1510, pp: 23-32.

[3] F. M. Javed Mehedi Shamrat, Zarrin Tasnim, Naimul Islam Nobel, and Md. Razu Ahmed. 2019. An Automated Embedded Detection and Alarm System for Preventing Accidents of Passengers Vessel due to Overweight. *In Proceedings of the 4th International Conference on Big Data and Internet of Things (BDIoT'19)*. Association for Computing Machinery, New York, NY, USA, Article 35, 1–5. DOI:https://doi.org/10.1145/3372938.3372973.

[4] Shamrat F.M.J.M., Nobel N.I., Tasnim Z., Ahmed R. (2020) Implementation of a Smart Embedded System for Passenger Vessel Safety. In: Saha A., Kar N., Deb S. (eds) *Advances in Computational Intelligence, Security and Internet of Things. ICCISIoT 2019. Communications in Computer and Information Science*, vol 1192. Springer, Singapore. https://doi.org/10.1007/978-981-15-3666-3_29

[5] Javed Mehedi Shamrat F.M., Ghosh P., Mahmud I., Nobel N.I., Dipu Sultan M. (2021) An Intelligent Embedded AC Automation Model with Temperature Prediction and Human Detection. In: Hassanien A.E., Bhattacharyya S., Chakrabati S., Bhattacharya A., Dutta S. (eds) *Emerging Technologies in Data Mining and Information Security. Advances in Intelligent Systems and Computing*, vol 1286. Springer, Singapore. https://doi.org/10.1007/978-981-15- 9927-9_75

[6] E. Unsal and Y. C¸ ebi, "Denial of service attacks in wsn," in *International Symposium on Computing in Science & Engineering. Proceedings*. GEDIZ University, Engineering and Architecture Faculty, 2013, p. 24.

[7] B. Ahmad, W. Jian, R. N. Enam, and A. Abbas, "Classifification of dos attacks in smart underwater wireless sensor network," *Wireless Personal Communications*, pp. 1–15, 2019.

[8] A. I. Al-issa, M. Al-Akhras, M. S. ALsahli, and M. Alawairdhi, "Using machine learning to detect dos attacks in wireless sensor networks," in *2019 IEEE Jordan International Joint Conference on Electrica ngineering and Information Technology (JEEIT)*. IEEE, 2019, pp. 107–112.

[9] S. Chakraborty, F. M. J. M. Shamrat, M. M. Billah, M. A. Jubair, M. Alauddin and R. Ranjan, "Implementation of Deep Learning Methods to Identify Rotten Fruits," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021, pp. 1207-1212, doi: 10.1109/ICOEI51242.2021.9453004.

[10] F. M. J. Mehedi Shamrat, M. A. Jubair, M. M. Billah, S. Chakraborty, M. Alauddin and R. Ranjan, "A Deep Learning Approach for Face Detection using Max Pooling," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021, pp. 760-764, doi: 10.1109/ICOEI51242.2021.9452896.

[11] F. M. J. Mehedi Shamrat, S. Chakraborty, M. M. Billah, P. Das, J. N. Muna and R. Ranjan, "A comprehensive study on pre-pruning and post-pruning methods of decision tree classification algorithm," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021, pp. 1339-1345, doi: 10.1109/ICOEI51242.2021.9452898.

[12] Biswas A., Chakraborty S., Rifat A.N.M.Y., Chowdhury N.F., Uddin J. (2020) Comparative Analysis of Dimension Reduction Techniques Over Classification Algorithms for Speech Emotion Recognition. In: Miraz M.H., Excell P.S., Ware A., Soomro S., Ali M. (eds) Emerging Technologies in Computing. iCETiC 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 332. Springer, Cham. https://doi.org/10.1007/978-3-030-60036-5_12.

[13] F. M. J. Mehedi Shamrat, S. Chakraborty, M. M. Billah, M. A. Jubair, M. S. Islam and R. Ranjan, "Face Mask Detection using Convolutional Neural Network (CNN) to reduce the spread of Covid-19," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021, pp. 1231-1237, doi: 10.1109/ICOEI51242.2021.9452836.

[14] D. Buch and D. Jinwala, "Denial of service attacks in wireless sensor networks," in *International*

conference on current trends in technology, Nuicone, 2010.

[15] N. TAMILARASI, “Neutralization of denial of service attack in wireless sensor networks.”

[16] A. Beena *et al.*, “Defence mechanism for dos attack in digital library (using citation network),” in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*. IEEE, 2019, pp. 1065–1068.

[17] S. Ghildiyal, A. K. Mishra, A. Gupta, and N. Garg, “Analysis of denial of service (dos) attacks in wireless sensor networks,” *IJRET: International Journal of Research in Engineering and Technology*, vol. 3, pp. 2319–1163, 2014.

[18] A. P. Abidoye and E. O. Ochola, “Denial of service attacks in wireless sensor networks with proposed countermeasures,” in *Information Technology-New Generations*. Springer, 2018, pp. 185–191.

[19] M. N. U. Islam, A. Fahmin, M. S. Hossain, and M. Atiquzzaman, “Denial-of-service attacks on wireless sensor network and defense techniques,” *Wireless Personal Communications*, pp. 1–29, 2020.

[20] E. Suryaprabha and N. S. Kumar, “Enhancement of security using optimized dos (denial-of-service) detection algorithm for wireless sensor network,” *Soft Computing*, pp. 1–11, 2019.

[21] Z. Gavric and D. Simic, “Overview of dos attacks on wireless sensor networks and experimental results for simulation of interference attacks,” *Ingenier´ıa e Investigacion*, vol. 38, no. 1, pp. 130–138, 2018.

[22] Rahaman, O. (2017). Data and information security in modern world by using elliptic curve cryptography. Computer Science and Engineering, 7(2), 29-44.

[23] Rahaman, M. O. (2017). Data and Information Security in Modern World. *Computer Science and Engineering*, *7*(1), 12-21.