Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 6, June 2022, pg.34 – 45

Secured Clustered Internet of Things Wireless Sensor Network

Prabhjot Kaur; Rupinder Singh; Rachhpal Singh
Khalsa College, Amritsar
E-mail: prabhjot25762@gmail.com
DOI: https://doi.org/10.47760/ijcsmc.2022.v11i06.003

Abstract- The Internet of Things (IoT) is a swiftly evolving technology that will have a significant impact in the future. The Internet of Things (IoT) is a huge collection of interconnected networks, such as the Wireless Sensor Network (WSN), that make use of fast evolving devices and technologies. The risk of confidentiality of information and protection has increased as a result of the indefinite interconnection of a variety of applied sciences in IoT. WSN employs Low Energy Adaptive Clustering Hierarchy (LEACH) to create an energy-efficacious network that is vulnerable to a wide range of assaults, including the HELLO flood. This work employs AS-LEACH (Abundant Secure LEACH) as an extension to the LEACH protocol to protect cluster heads from Hello flood attacks. For the purpose of validating a sensor node as CH, AS-LEACH employs RBG color cube numbers, a distinct Abundant number, and each sensor node has its own unique ID. The NS2 network simulator is utilized to implement AS-LEACH and verify its efficiency in this proposed work.

Keywords: Abundant number, RBG color cube, IOT, WSN, LEACH, Cluster head, Hello flood attack.

1. INTRODUCTION

The Internet of Things (IoT) is a kind of network of physical objects that provides various technological capabilities for exchanging information with other devices over the internet. The integration of wireless sensor network (WSN) with Big Data and Cloud Computing results in wide expansion field of information technology. Figure 1 shows WSN-IOT integration. This extensive interrelation of distinct technologies will be used in future for collecting information needed using several sensor nodes. This will support data collection in remote locations where appropriate connectivity and infrastructure facilities are lacking. The integration of Internet of Things (IoT) with other technologies will impart a wide range of applications including water and waste management, smart pollution control, smart farming, patient tracking, smart cities, medicine, traffic management, environmental surveillance, locations of active volcanoes, highly radioactive vulnerable places etc. The most critical factor in WSN-IOT integration is data confidentiality.

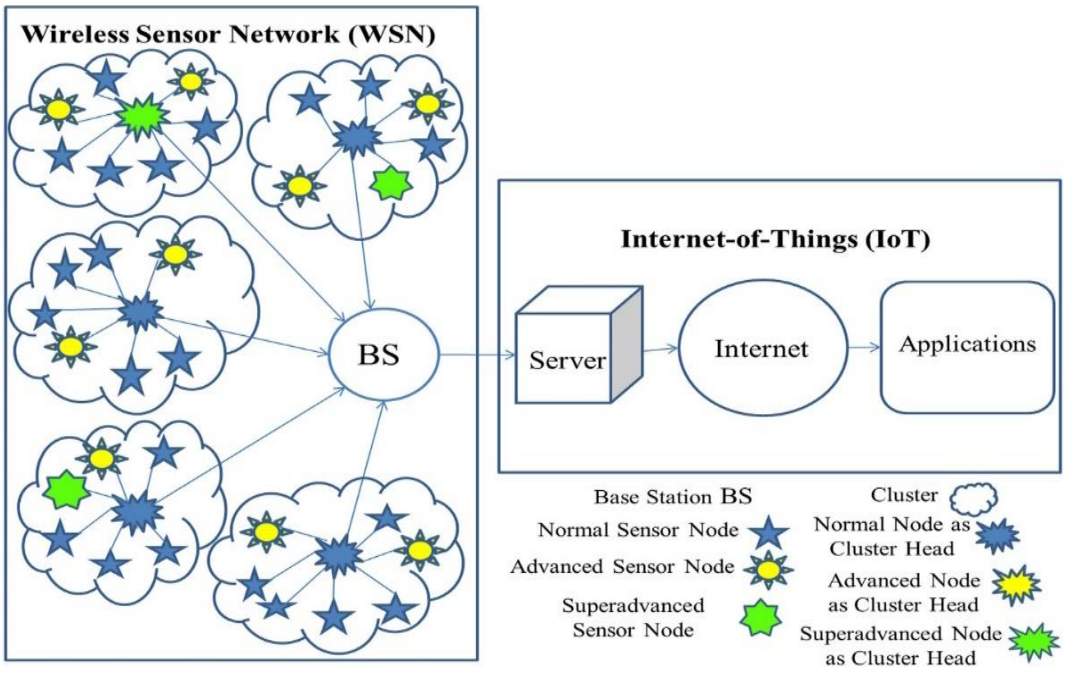

Figure 1: WSN-IoT Integration

When WSN is integrated with IoT, a protocol for detecting HELLO flood attacks efficiently is proposed in this research work. The proposed protocol is a variant of Low Energy Adaptive Clustering Hierarchy (LEACH), which exploits clustering in tandem with Received Signal Strength (RSS) to elect Cluster Heads dynamically (CHs). The HELLO flood attack, which intends to create malevolent nodes CH, is one of the assaults that LEACH is vulnerable to.

This paper proposes AS-LEACH (Abundant Secure LEACH), a LEACH protocol enhancement that prevents mean from being chosen as CH. A Wireless Sensor Network (WSN) is a grouping of small sensor nodes that collect data collectively and send it to a central Base Station (BS) for distribution across multiple locations through the Internet of Things. Due to the restricted battery power available sensor nodes that are small, the complexity of security algorithms makes implementation extremely difficult.
Hello packets are being used by sensor nodes to discover neighbour nodes in the WSN, but they can also be used to launch a hello flood attack by a high-data-transmission-rate attacker node. The countermeasures used to deter hello flood attack are discussed in [1] as previous work. To authenticate CH, AS-LEACH uses the RBG color cube number, Abundant number, and unique ID. The rest of the paper is organised as follows: Section 2- discusses the Wireless Sensor Network hello flood attack, Section 3- discusses the formation of a unique WSN cluster, Section 4- discusses AS- LEACH, and Section 5- discusses NS2 simulation output.

2. HELLO FLOOD ATTACK

In a WSN, the mean node uses the Hello flood attack to transmit Hello packets to other sensor nodes via wireless transmission. Because of its high power of transmission, the other sensor nodes in the network quickly identify the malevolent node as the CH. With using this technique, the malicious node gives the impression that it is the neighboring node of sensor node in the WSN and uses it to cause trouble with the pertinent routing protocol in order to launch further attacks. As shown in Figure 2, the attacker takes control of the sensor node clusters after being the parent node

in the WSN. For the intention of increasing the time it takes to communicate in the WSN, the mean node oversees all data transmission that is routed in the cluster through this CH. The attacker sends hello messages to a wide range of WSN areas, almost inducing and influencing remaining sensor nodes to imply that the attacker is really close by. By responding to the attacker's HELLO message with limited power, the cluster sensor nodes create a non-clear state in the network. Figures 3 and 4 depict the Hello flood attack employed in the WSN. The base station, attacker, and sensor nodes are represented in the diagram by triangle, rectangle, and circles, respectively.

Hello messages are simulcast by intercepting a sensor node by the attacker and declaring it as their neighbor to initiate a WSN hello flood attack. The sensor nodes in the WSN begin communicating with the attacker node after receiving this hello message, and a neighbor entry is created in the routing table. This CH is used by all of the sensor nodes in the WSN to transmit data to the base station. Since the message has the shortest path from the CH, the WSN nodes consider the attacker as a neighbor node. After acquiring full control of the sensor nodes in the WSN, the attacker manipulates the data obtained by the sensor nodes as desired, as the communication between these nodes is completely discontinue from BS.

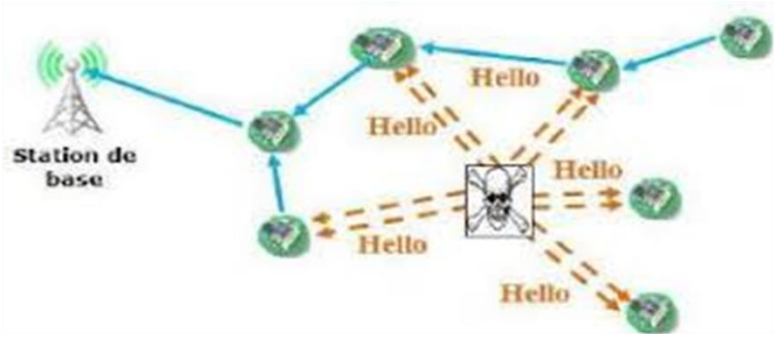

Figure 2: Hello Flood Attack

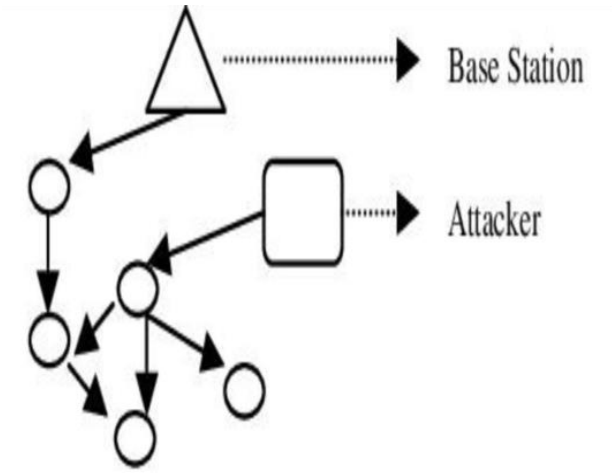

Figure 3: An attacker with a high transmission power broadcast hello packets.

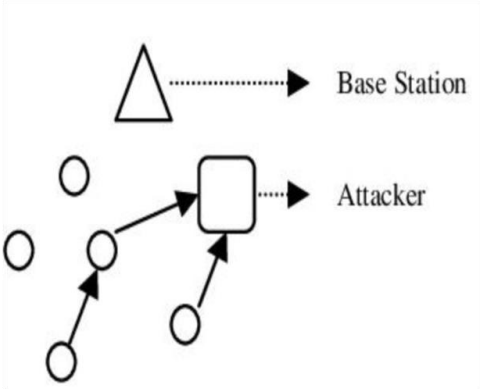

Figure 4: The attacker is chosen as a neighbor by the sensor nodes.

3. CLUSTERING OF WSN

Almost every WSN integrated with IoT application operates in an unattended and harsh environment. Human oversight is not always feasible in such situations. Sensors are arranged using control methods over a wide area, allowing for specially made system arrangement is feasible. To cover such a large area, a large number of sensors (hundreds or thousands) are needed, and these nodes must be very critical. The power-delivery batteries can't be revived on a regular basis. As a result, specially built energy-efficient steering conventions must be introduced in WSN in order to preserve sensor device lifetime.

As a result, the sensor nodes in the WSN must be clustered together. This is needed to achieve the WSN's extensibility and high energy efficiency goals, allowing the network to operate in wide-ranging environments. In a clustered hierarch WSN system, each cluster has a set number of member sensor nodes. One of the member sensor nodes, CH, is in charge of the entire cluster. CH is in charge of both fusion and aggregation. The sensor node clustering is divided into two levels, with CH at the top and member nodes at the bottom. The cluster members send data to the WSN via the associated CH. These CHs either deliver data directly to the BS or send data from sensor nodes to the BS via midway communication. Because the CH must send acquired data over large distances, they must actually spend high energy rates. In order to control the energy utilisation of all sensor nodes, the CH is re-elected among cluster sensor nodes on a regular basis. WSN single-hop intra-cluster communication and multi-hop inter-cluster communication are represented in Figure 5.

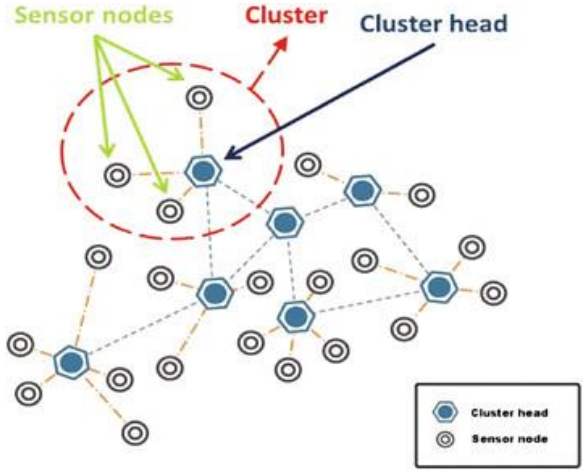

Figure 5: WSN CLUSTERS

4. AUTHENTICAL CH SELECTION

After the WSN has been formed with a large number of sensor nodes, the first step is to form groups to encourage vitality effective communication. The system task is divided into rounds when the group has been arranged. Figure 6 shows how each round proceeds in three parts.

Synchronization, Authenticated CH Election, Data Aggregation, and Forward are the stages used in the construction of WSN. The focus of this work is on the Authenticated CH Election stage. The following conditions must be met by a WSN CH choice framework:

- Unpredictability: A sensor node's constancy about CH should be ludicrous.
- Non-manipulability: The outcomes of CH choice are inflexible.
- The Agreement property: each sensor node in a WSN obtains the same decision outcomes.

The race of a CH is expected to be determined by a common erratic worth. To begin, a fundamental arbitrary worth is established, and all group members must agree on a standard worth CH. Every member of the cluster contributes to the formation of arbitrary worth, which is common on the route to circulating their own irregular estimations. A malevolent sensor hub can evaluate fundamental characteristics created by other sensor hubs by procrastinating its arbitrary worth in order for others to disseminate their wine. The assailant hub may obstruct non-manipulability instances by disconnecting transmission. For example, the assailant hub may retain a strategic distance from the irregular worth transmission in order to change the CH race result as a consequence of analogous esteem alterations. The distance between groups of sensor hubs is frequently used to determine sensor hub transmission. A noxious hub can generate numerous basic qualities by reducing transmission control and disregarding the understanding property of decision results.

For the most part, the CH is determined by the quality of the signal used by the sensor hubs for hello message telecommunication. The sensor hub can produce a better signal and be counted on to progress toward being CH with more battery reinforcement. In exchange for becoming CH, the malevolent node is usually equipped with a significant power reinforcement, which it can utilise to send an incredible hello message. Both irregular aspects and signals of solidarity influence the CH decision to stay away from a malicious hub. However, assailant hub has a good chance of controlling the above-mentioned imposed conditions. A rigorous CH verification technique is required in this regard. A secure WSN CH determination technique is discussed further down over the next passage.

Figure 7 shows how the RBG shading scheme categorises each shade based on the amount of red, green, and blue shading produced. To indicate these measurements, the bulk of computerised records use 0-255 whole integers. The RGB shading 3D square is used to depict the seamless progression of these hues. It employs 8 bits for each segment, giving it a total of 256*256*256 hues to choose from.

An abundant number is one that is smaller than the sum of its aliquot parts (proper divisors).The proper divisors of 24 are, for example, 1, 2, 3, 4, 6, 8, and 12, whose summation is 36. The number 24 is abundant because 36 is greater than 24. So Its abundance is 36-24=12. During the grouping process, the BS assigns a unique ID, abundant number, and RBG shading 3D shape number to each sensor hub, which is then recorded in the table. When a sensor hub is selected as the CH, it must first obtain permission from the BS before it can begin working. After confirming data from the enrolling table and evaluating the rest of the vitality level, the BS verifies the CH. The proposed confirmation system for secure CH determination is represented in Figure 8 stream diagram.

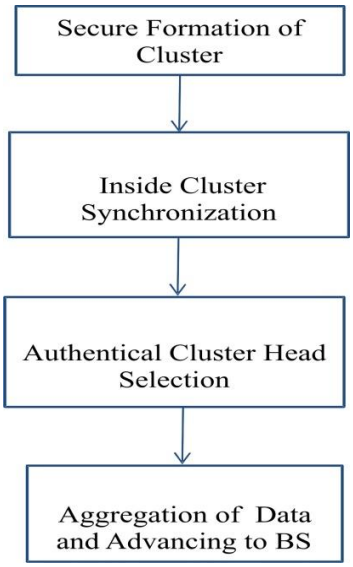

Figure 6: The sensor network operation

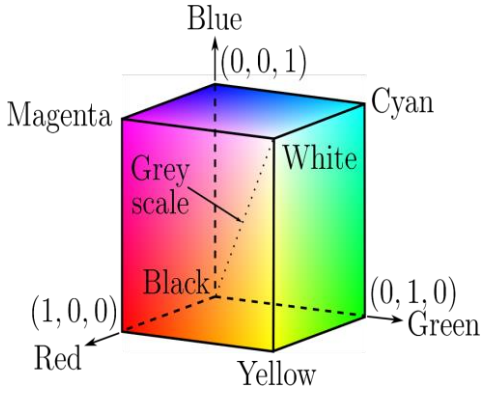

Figure 7: RBG color cube

5. SIMULATION RESULTS

The simulation results for the AS-LEACH protocol are presented in this section of the paper to illustrate the effectiveness of the proposed work. With the following parameters, the simulation is performed in NS 2.35.

Table 1: Parameters of Simulation

Parameter	Value
Simulator	NS 2.35
Area	800X800
No. of nodes	42
Protocol for routing	LEACH
Channel type	Wireless
Packet size	512 bytes
Mobility model	Two ray ground propagation model

a) Throughput

The throughput of a system is a significant factor in determining remote sensor arrangements execution. The normal rate of parcels (packets) conveyed effectively is referred to as throughput. The total number of bundles delivered to the goal per unit time is known as throughput. The term "throughput" is defined as:

Throughput = (Total number of packets delivered to their final destination) / (simulation time)

Figure 9 shows the throughput of the reproduced WSN with, without, and after using AS-LEACH. The figure demonstrates that AS-LEACH builds throughput after the disengagement of the Hello flood assault.

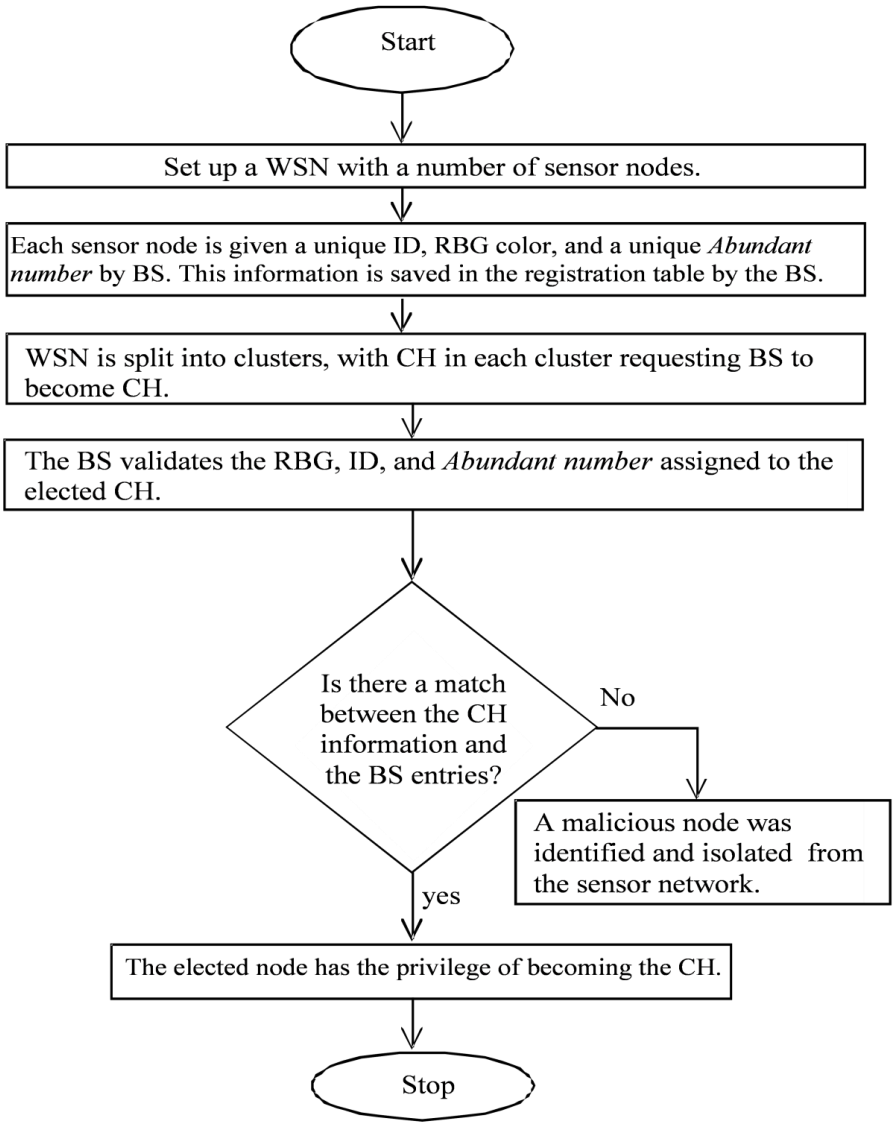

Figure 8: AS-LEACH Flowchart.

b) PDR (Packet delivery ratio)

The packet delivery ratio is the proportion of packets received at the destination to those transmitted from the source. The PDR is defined as (Packets received/Packets produced) * 100.

Figure 10 shows the PDR for AS-LEACH, Hello flood assault, and without assault. The results indicate that PDR has increased.

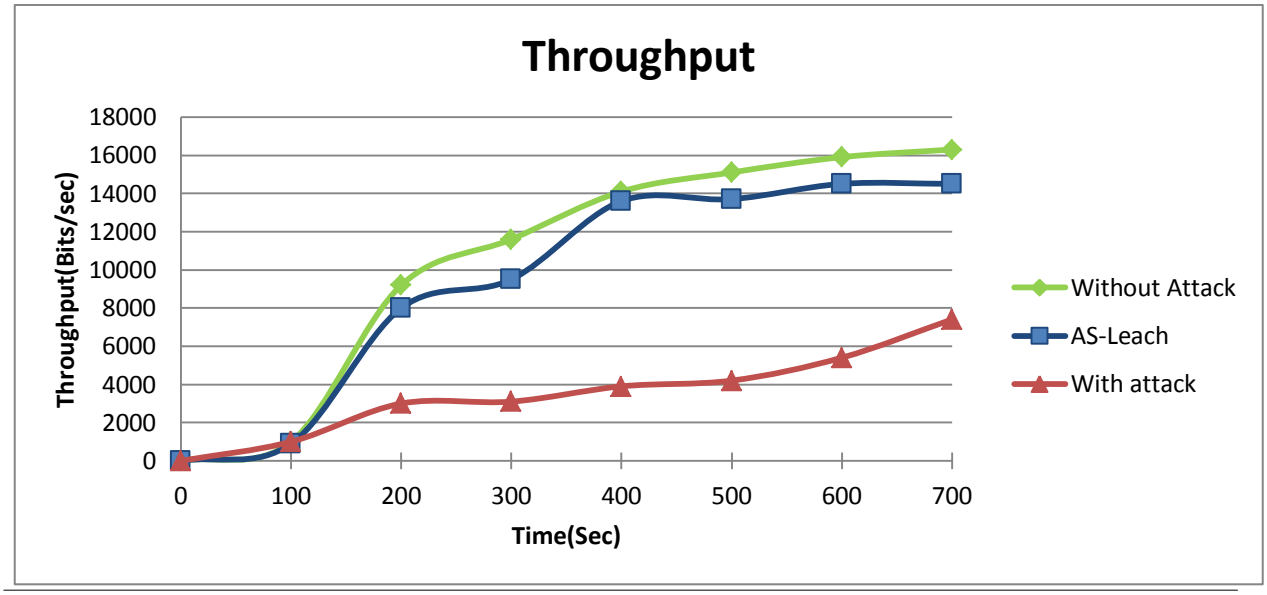

Figure 9: Throughput

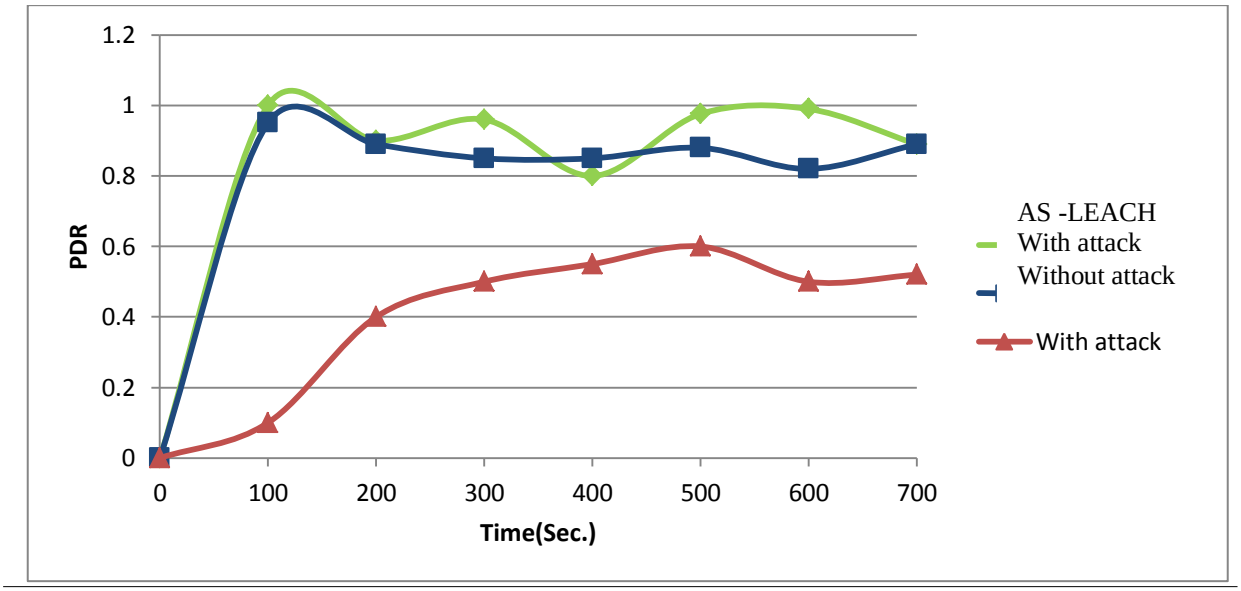

Figure 10: PDR

c) Delay

The delay is the time it takes for a bundle to get at its destination, as well as the time it takes to reveal the course and transmit the information parcels (packets). Delay is defined as follows:

Delay = ∑ (received time – send time) / ∑ (No. of connections)

Figure 11 shows the AS-LEACH postponement with and without assault.

d) Overhead

The amount of time it takes to transport packets to their final destination is known as overhead. As the CH develops overhead in WSN, hello flood shoved. The overhead is the evaluation of WSN directed bundles. Figure 12 illustrates AS-LEACH overhead, without assault and invasion. AS-LEACH reduced the WSN organisation overhead after removing a malevolent hub.

e) Energy consumption

At the start of recreation, each sensor hub is given 10 joules of precursive vitality. This vitality worth is transferred as information dissension, and a sensor hub transmits and accepts each bundle using an unmistakable measure of vitality. The level of vitality usage is calculated as follows: Energy consumption = Initial energy - Current energy

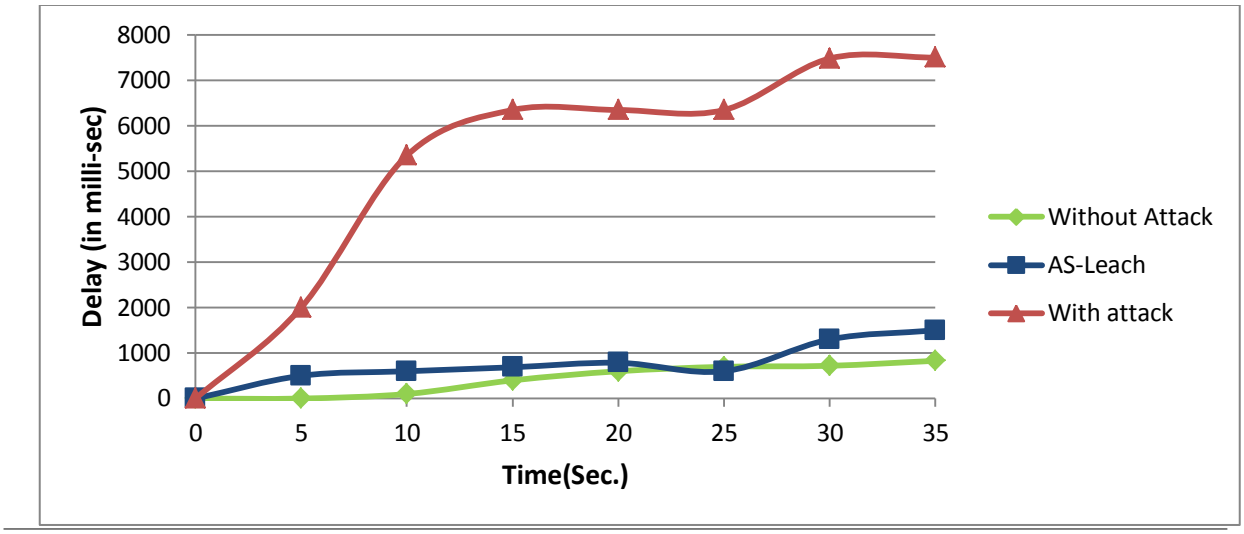

Figure 11: Delay

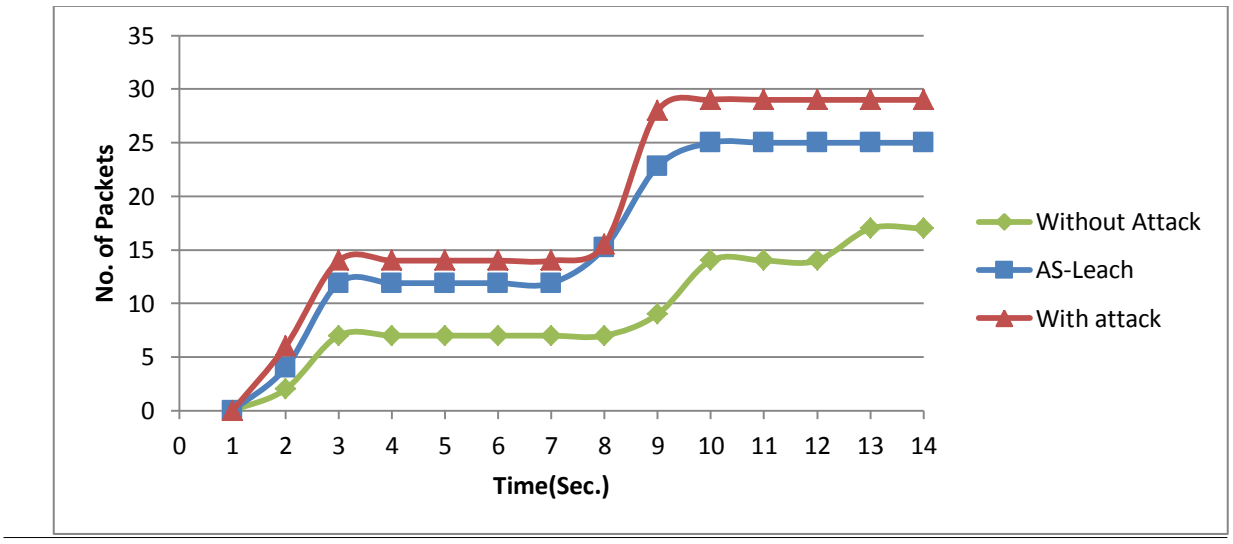

Figure 12: Overhead

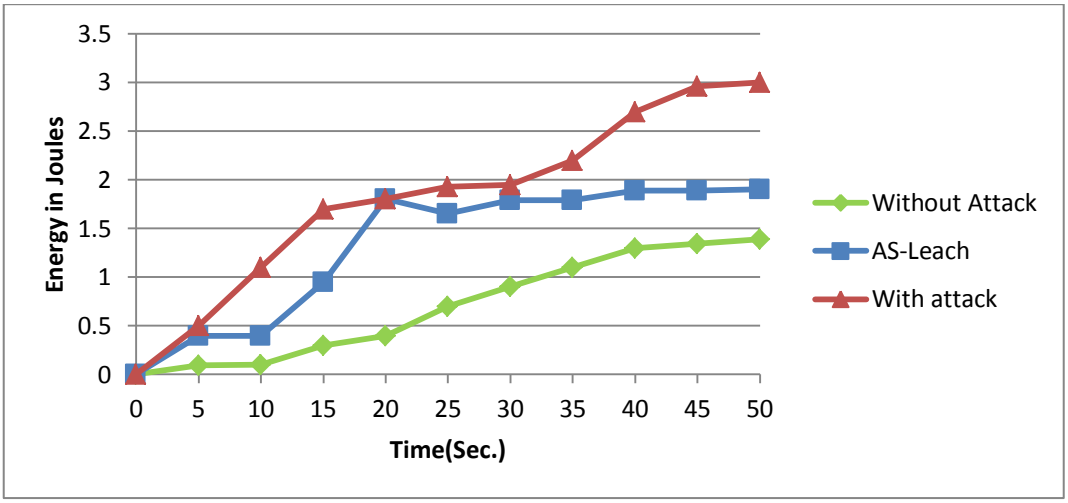

Figure 13: Energy consumption

6. CONCLUSION

The Internet of Things (IoT) is a vast network of networks that connect diverse technologies, such as wireless sensor networks. The Internet of Things makes use of a number of tools to communicate with physical objects and process data collected by sensor nodes in various locations. The internet of things' huge and rapid growth needed effective data communication security tools. This research proposes a approach for selecting cluster heads that is both secure and efficient for use with various wireless sensor networks that are integrated to the internet of things. The cluster head election is essential because it is in responsible of data transfer between the sensor node and the base station. Because all data in a wireless sensor network passes via the cluster head to reach the base station, it must be done securely. In a clustered WSN with high transmission power, the malevolent node uses the Hello flood attack to compromise the cluster head. This paper proposes a novel technique for authenticating cluster head based on unique ID, RBG color cube number, and Abundant number. The proposed work in this research aims to improve WSN performance by detecting malevolent nodes early and actively preventing wireless nodes from forming cluster head associations. This technique facilitates the creation of big clusters. The proposed work results in the evacuation of malicious nodes from clusters, thus enhancing cluster quality and energy efficiency, as demonstrated by the NS2 simulator implementation. For PDR, overhead, delay, throughput, and energy consumption, the proposed work is implemented in NS2. To evaluate the performance of the proposed technique, additional simulations with more sensor nodes will be undertaken in the future.

REFERENCES

[1] Rupinder Singh, Rachhpal Singh, Prabhjot Kaur, "Securing Cluster Head in Wireless Sensor Network for Internet of Things", International Journal of Computer Science and Mobile Computing, Vol. 10, Issue 1, January 2021, pp 49 – 60.

[2] Rupinder Singh, Dr. Jatinder Singh, and Dr. Ravinder Singh, "Hello flood attack Countermeasures in Wireless Sensor Networks", International Journal of Computer Science and Mobile Applications, Vol. 4, Issue 5, April 2016, pp. 1-9.

[3] C. Venkata, Mukesh Singhal, James Royalty, and Srilekha Varanasi, "Security in wireless sensor networks", Wireless communications and mobile computing Published online in Wiley Inder Science, 2006

[4] Yaya Shen, Sanyang Liu, Zhaohui Zhang, "Detection of Hello Flood Attack Caused by Malicious Cluster Heads on LEACH Protocol", International Journal of Advancements in Computing Technology (IJACT), Volume 7, Number 2, March 2015.

[5] Gayatri Devi, Rajeeb Sankar Bal, Nibedita Sahoo, "Hello Flood Attack Using BAP in Wireless Sensor Network", International Journal of Advanced Engineering Research and Science, Vol. 2, Issue 1, ISSN: 2349-6495, Jan. 2015.

[6] S. Mayur, H. D. Ranjith, "Security Enhancement on LEACH Protocol from HELLO Flood Attack in WSN Using LDK Scheme", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, ISSN (Online): 2319 – 8753, ISSN (Print): 2347 – 6710, March 2015.

[7] S. Rawan, M. Suhare, A. Manal, "Intrusion Detection of Hello Flood Attack in WSNs Using Location Verification Scheme", International Journal of Computer and Communication Engineering, Volume 4, Number 3. May 2015.

[8] Dilpreet Kaur, Rupinderpal Singh, "Energy level-based Hello Flood attack Mitigation on WSN", International Journal of Embedded Systems and Computer Engineering, ISSN 23213361, July 2015.

[9] Jyoti, Ashu Bansal, "Detection of Hello Flood Attack on Leach Protocol Based on Energy of Attacker Node", International Journal of Innovations & Advancement in Computer Science, Volume 4, ISSN 2347 – 8616, September 2015.

[10] Shikha Magotra, Krishan Kumar, "Detection of HELLO flood Attack on LEACH Protocol", IEEE International Advance Computing Conference (IACC), 2014.

[11] J. Steffi, Agino Priyanka, S. Tephillah, and A. M. Balamurugan, "Attacks and countermeasures in WSN", International Journal of Electronics & Communication, Volume 2, Issue 1, ISSN 23215984, January 2014.

[12] Satwinder Kaur Saini, Mansi Gupta, "Detection of Malicious Cluster Head causing Hello Flood Attack in LEACH Protocol in Wireless Sensor Networks", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 5, ISSN 2319 – 4847, May 2014.

[13] Akhil Dubey, Deepak Meena, Shaili Gaur, "A Survey in Hello Flood Attack in Wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT), Vol. 3, Issue 1, ISSN:2278-0181, January 2014.

[14] Virendra Pal Singh, S. Aishwarya, Anand Ukey, and Sweta Jain, "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks", International Journal of Computer Applications, Volume 62, No.15. January 2013.

[15] Nusrat Fatema, Remus Brad, "Attacks and counterattacks on wireless sensor networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol. 4, No. 6. December 2013.

[16] A. Anup wanjari, Vidya Dhamdhere, "Evading Flooding Attack in MANET Using Node Authentication", International Journal of Science and Research (IJSR), Volume 3, Issue 12, ISSN (Online):2319-7064, December 2014.

[17] Mohammad Sayad Haghighi, Kamal Mohamedpour, Vijay Varadharajan, and Barry G. Quinn, "Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks", IEEE transactions on information forensics and security, Vol. 6, No. 4, December 2011.

[18] Virendra Pal Singh, Sweta Jain, and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", International Journal of Computer Science Issues, Vol. 7, Issue 3, No. 11, ISSN 1694-0814, May 2010.

[19] Mohamed Osama Khozium, "Hello Flood Counter Measure for Wireless Sensor Network", International Journal of Computer Science and Security, Volume 2, Issue 3, May 2008.

[20] A. Hamid, Mamun Rashid, Choong Seon Hong, "Defense against lap-top class attacker in wireless sensor network", The 8th International Conference Advanced Communication Technology, Print ISBN: 89-5519-129-4, IEEE, 2006.

[21] Waldir Ribeiro Pires J´unior Thiago H. de Paula Figueiredo Hao Chi Wong, "Malicious Node Detection in Wireless Sensor Networks",18th International Parallel and Distributed Processing Symposium, Print ISBN:0-7695-2132-0, IEEE, 2004.

[22] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN", International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[23] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", The International Arab Journal of Information Technology, Vol.9, No.3. May 2012.

[24] Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava, "Security in internet of things: Challenges, solutions and future directions," System Sciences (HICSS), 2016 49th Hawaii International Conference on. IEEE, 2016.

[25] Nacer Khalil, Mohamed Riduan Abid, Driss Benhaddou, Michael Gerndt, (2014) "Wireless Sensors Networks for Internet of Things", IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) Symposium on Public IoT.

[26] M. Zorzi, A. Gluhak, S. Lange, A. Bassi, From Today's Intranet of Things to a Future Internet of Things: A Wireless and Mobility-Related View, IEEE Wireless Communication 17 (2010) 43–51.

