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. 4, April 2022, pg.49 – 60

Clustering and Securing IoT Wireless Sensor Network

Rupinder Singh; Rachhpal Singh; Prabhjot Kaur
Khalsa College, Amritsar
E-mail: rupi_singh76@yahoo.com

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i04.007

*Abstract– One of the future rising technologies is Internet of Things (IoT) that will play a significant role in linking the world. IoT is a group of a huge number of interrelated networks including Wireless Sensor Network (WSN). IoT makes use of speedily developing devices and technologies. A large number of unlimited interconnections of numerous technologies in IoT makes privacy and safety of data as a matter of concern. WSN makes use of Low Energy Adaptive Clustering Hierarchy (LEACH) for the purpose of construction of sensor networks that are energy-efficient. These networks are likely to a huge number of attacks including HELLO flood attack. This paper presents a novel protocol named CS-LEACH (*Cyclic *Secure LEACH) for securing cluster head from Hello flood attack as an extension to LEACH protocol. CS-LEACH makes use a unique Cyclic number, an exclusive ID and RBG color cube numbers for each sensor node so as to authenticate one of the nodes as CH. The CS-LEACH is executed by making use of NS2 simulator for the purpose of proving its efficiency.*

Keywords: LEACH, Cyclic number, Internet of Things, Cluster head, Wireless sensor network, RBG color cube, Hello flood attack.

I. INTRODUCTION

Internet of Things (IoT) a worldwide system connection style offers services of the real world by usage of information investigation with its further processing. A WSN (wireless sensor network) is a group of minor sensor nodes that may be united with big data, Cloud computing, robotics etc. for the vast development in the field of Information Technology. Figure 1 illustrations how WSN can be integrated with IoT. This huge association of diverse technologies will be upcoming in which

numerous sensors will be applied for gathering information to be needed. As a result of this it helps in assisting to collect data at distant places where appropriate way of data communication and organizations are not available. Combination of IoT with diverse technologies is going to offer a great quantity of implementations with manufacturing poisonous smokes, patient following, drug, environment monitoring, active volcano's locations, radioactive sensitive areas, etc. The greatest significant worry of integrating IoT with WSN is to deliver information secrecy.

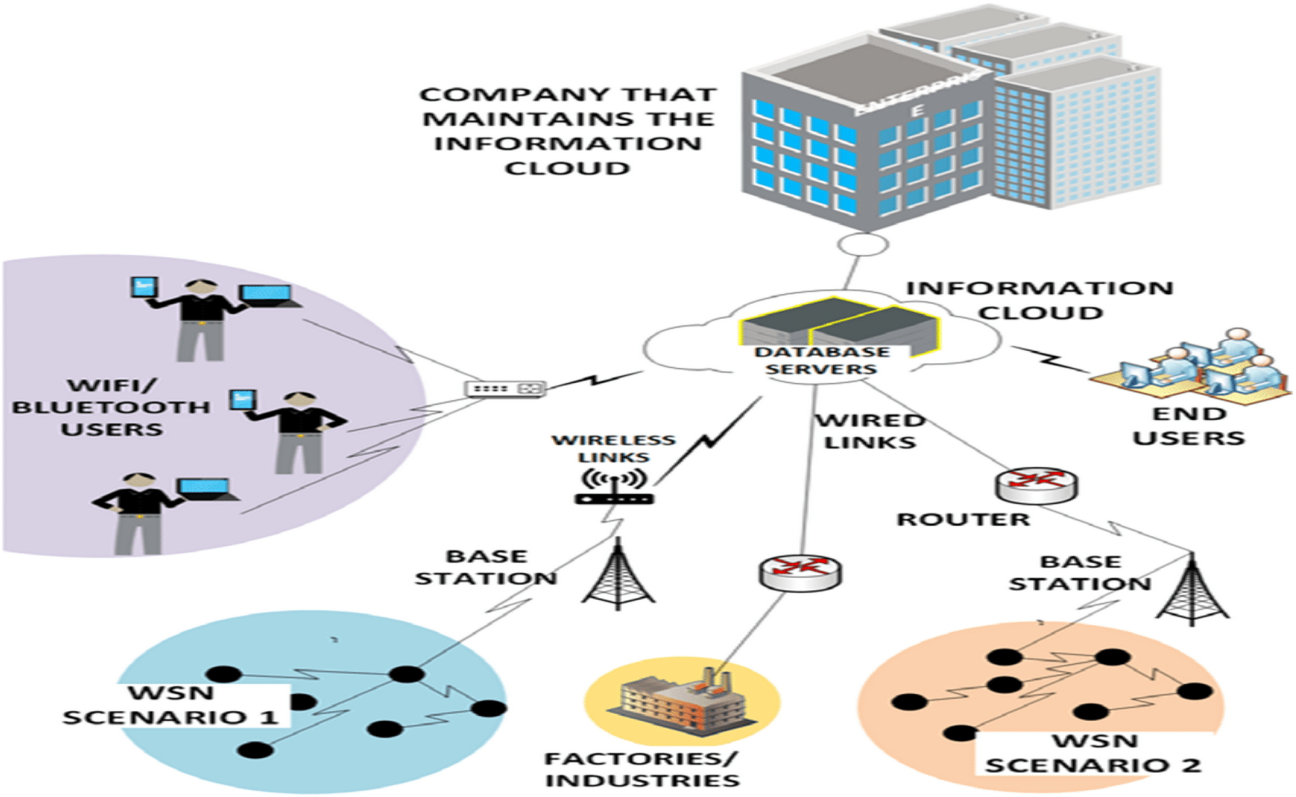

Figure 1: WSN with IoT

The work done in this paper focus on a procedure for the recognition of HELLO flood attack in a well-organized means and can be used for WSN and IoT integration. The projected procedure is basically extension of LEACH (Low Energy Adaptive Clustering Hierarchy) that styles practice of gathering along with RSS (Received Signal Strength), which is further used for dynamic selection of CHs (Cluster Heads). LEACH susceptible to a huge amount of attacks including HELLO flood launched for making mean node CH.

CS-LEACH (Cyclic Secure LEACH) as one of the versions of LEACH protocol is projected in this research paper for avoiding malicious node from actuality becoming CH. WSN is a group of minor sensor nodes that labor together and forward composed information to a vital place BS (Base Station) to dispense it at many positions through IoT. The difficulty of safety procedures makes it very hard for their execution due to the partial battery-operated energy power delivers to small sensor nodes.

Hello packets specially designed packets are used by sensor nodes for determining WSN neighbor nodes, and these packets are used by attacker having high broadcast signal power to create hello flood attack. The measures to counter this hello flood attack are provided and discussed in [2] as our previous work. CS-LEACH uses a unique ID, RBG color cube number, and Cyclic number so

as to validate CH. The rest of the paper is organized as: In the II section of paper, hello flood attack for WSN is discussed, section III provides how exclusive WSN foundation of clusters is used, section IV the research work CS-LEACH, section V defines NS2 simulation outcomes.

II. HELLO FLOOD ATTACK

WSN use Hello flood attack with the help of a special node that sends Hello packets to remaining sensor nodes by making use of powerful wireless transmission. With the help of this powerful strong transmission signal the malicious node is selected as CH easily by other sensor nodes in the wireless sensor network. The mean node by transmitting this powerful signal impress other nodes in the wireless sensor network that it is a nearby node so that it can be used by other node as part of routing protocol. Once this mean node becomes the part of protocol it can be used for initiating further attacks. The attacker node due to strong signal becomes the parent node in the sensor network and controls the other sensor node clusters. This is depicted in figure 2. This malicious node controls all the transfer of data in the clusters of wireless sensor network routed via this Cluster Head for the purpose of enhancing communication delay in the WSN. The attacker node spreads hello messages to a huge variety of areas in WSN and nearly forces and effects remaining sensor nodes that attacker mean node is actually close to them. The nodes in the cluster waste their limited power remaining to them for the purpose of replying to the HELLO message of attacker resulting in making an unclear state. Hello flood attack that can be launched for WSN is denoted in Figures 3 and 4.

For commencement of hello flood attack in WSN, hello data is transmitted in the air by the attacker so that this signal is cached by sensor nodes. The attacker declares itself as the neighbor of other nodes. The sensor nodes in different clusters of WSN start interacting with the attacker node after the receipt of this hello message. The sensor nodes make an entry about the attacker in the routing table as a neighbor. Every sensor node is forced in WSN to transmission data to BS by making use of CH. The nodes with lower transmission power in WSN admit the attacker as the neighbor node because the communication to be transmitted with the direct pathway from the CH. Because of this illusion, they start links with the attacker node. The attacker once has complete control over the sensor nodes in the WSN starts manipulating the data composed by the sensor node as per the wish as the interaction of these nodes is completely cut from BS.

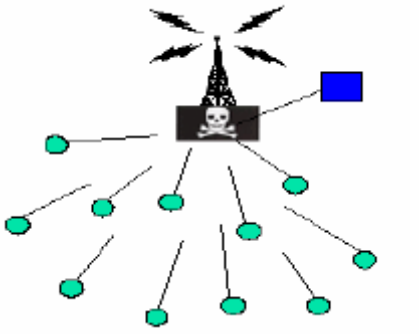

Figure 2: Hello Flood Attack

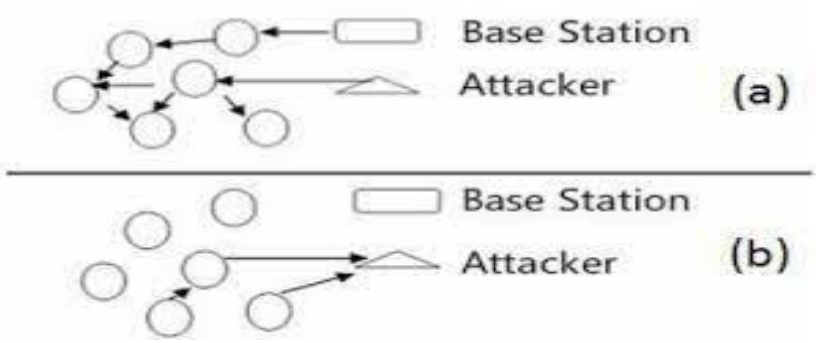

Figure 3: High power attacker Hello packets broadcast.
Figure 4: Attacker selected as neighbor.

III. CLUSTERING WSN

Most of the application used for integrated WSN and IoT make use of harsh unattended environment. In such situations, human control and monitoring is not constantly possible. The specifically chosen organization planning is achievable. A vast quantity of sensors is essential to represent such a huge part and these nodes are very strength bound. The power distributing batteries cannot be steadily recharged. therefore, it imposes that exclusively strategic vitality creative navigation agreements must be realized in WSN for defending sensor organize time period.

So, it is wanted that nodes in the network should be assembled into groups. This is essential for sufficient aim of scalability along with high energy efficiency in WSN so that the network occurs in huge scale surroundings. In grouped classified assembly, each of the groups has a static quantity of participant sensor nodes. One of the member sensor nodes that regulate the whole cluster is CH. The duty of union along with combination is accomplished by CH. The gathering of sensor nodes arrangements a two-level order with CH on an advanced and other at lower level. The cluster followers communicate data to the WSN over corresponding CH. These CH's convey data composed from sensor nodes to the Base station (BS) either straightway or using some midway communication. The CH transmits composed information to extended distances so they have to devote complex energy rates. In direction to stabilize the energy usage of each sensor nodes, the CH is frequently re-elected between nodes. Figure 5, represent WSN with clustered nodes, CH and BS.

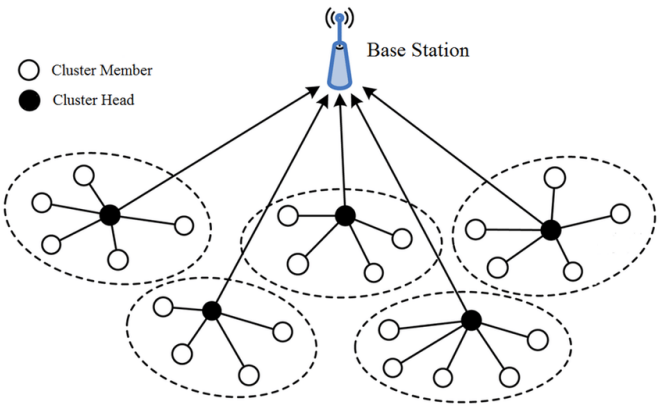

Figure 5: WSN Clustering

IV. GENUINE CH SELECTION

After the setup of WSN, a number of sensor nodes are interconnected in clustered form, the early step is to form groups for encouraging energy productive communication. After the planning of the group, the system task is distributed into rounds. Each round works in three phases as shown in Figure 6.

The stages used for the building of WSN are Synchronization, Genuine CH Election, Data Combination, and Forward. This working is dedicated just around Authenticated CH Election stage. A CH WSN choice outline must fulfil the following conditions:

- Non-manipulability: the choice for outcomes of CH selection is non-flexible.
- Unpredictability: uniformity about CH selection should be unusual by a sensor node.
- Agreement property: every sensor node gets the similar choice outcomes in WSN.

The battle for selection of CH is assumed to be initiated on a typical non-regular worth. First of all, this regular random worth is formed and all cluster individuals need to agree with a typical worth CH. All cluster entities add to constructing random worth which is regular with the way toward circulating uneven approximations of their own. A malicious sensor hub can evaluate the elementary assets formed by other sensor hubs by accepting its arbitrary worth with the aim that others can spread their wine. The attacker hub can delay non-manipulability situations by getting gone transmission, for example, the attacker hub sustains a planned distance from the irregular worth transmission, in direction to alternate the CH race consequence since of changes in like way esteem. Typical sensor hub broadcast lay on lot distance transversely between collected sensor hubs. By dropping broadcast switch a harmful hub can make numerous basic qualities by to abandoning the thoughtful property of choice outcomes.

The choice of CH for most of part relies upon the superiority of the signal, which is used by the sensor hubs for the transmission of hello message. The sensor node with high-capacity battery can produce all the more leading signal and is trusted upon to move toward becoming CH. The malicious element is characteristically filled with a massive power reinforcement, so it can be used for exploiting an unbelievable hello message for the purpose of getting to be CH. The CH decision is based on both uneven qualities and signs unity to stay missing from a malevolent sensor node from selected as CH. At the same time, the odds are that attacker sensor node control the above-forced situations. Along these scenario's, there is a necessity for a hard CH confirmation method. Under in the next passage, a safe WSN CH determination method is talked about.

The RBG shading outline as shown in figure 7 characterizes each shading by the measure of creation of red, green, and blue shading. For the most of the part, computerized information utilizes 0-255 whole numbers for the purpose of indicating these measures. RGB shading with 3D square is applied to display these types flat advances. It makes use of 8 bits for each part and a sum of 256*256*256 possible number of kinds can be utilized. A special type of number called cyclic number contains m digits and when it is multiplied by 1, 2, ..., m it produces the number which is same but the order is different. Such as 42857, this number is cyclic: 142857 × 2 = 285714; 142857 × 3 = 428571; 142857 × 4 = 571428; 142857 × 5 = 714285; 142857 × 6 = 857142, and so on. The BS allot an exceptional ID, cyclic number, and a RBG shading 3D shape number to each sensor hub in the process of arranging groups and record this information in the table. When a sensor node is picked as CH, it requests to take permission before working from the BS. The BS is responsible for verifying the authenticity of CH after confirming data from the enrolment table and examining the

rest of the vitality level. Figure 8 stream diagram summaries the proposed validation system of safe determination of CH.

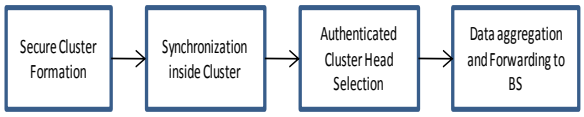

Figure 6: operations of Sensor network

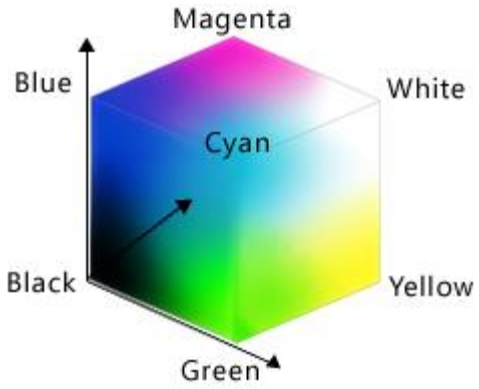

Figure 7: RBG cube

V. RESULTS OF SIMULATION

Result and simulation portion of paper delivers effectiveness of proposed protocol CS-LEACH so as to confirm its validity. NS 2.35 is used along with given below parameters.

Table 1: Simulation parameters

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

An important parameter for measuring performance is throughput and is used for isolated sensor positions. Throughput defined as number of packets received at destination in some predefined unit time.

The formula is:
Throughput = (Packets received in totality)/ (simulation time)
Figure 9 specifies throughput without Hello flood, with Hello flood, and with CS-LEACH.

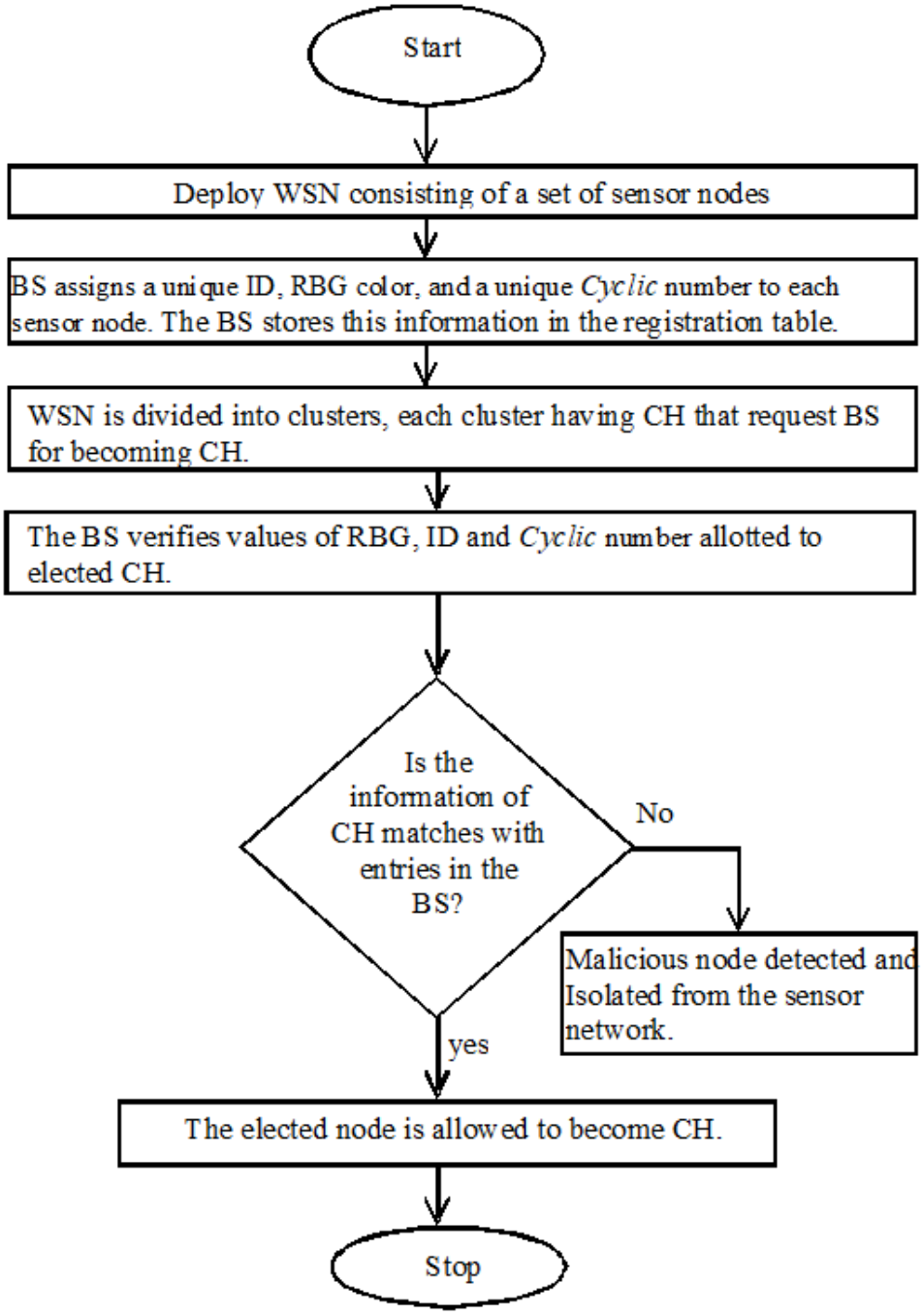

Figure 8: flow chart of CS-LEACH.

B. Packet delivery ratio (PDR)
Packet delivery ratio is defined as ratio data packets that are received at destination i.e. (Packets got/packets produced) * 100
Figure 10 is the result of simulation for with Hello flood, without attack and CS-LEACH.

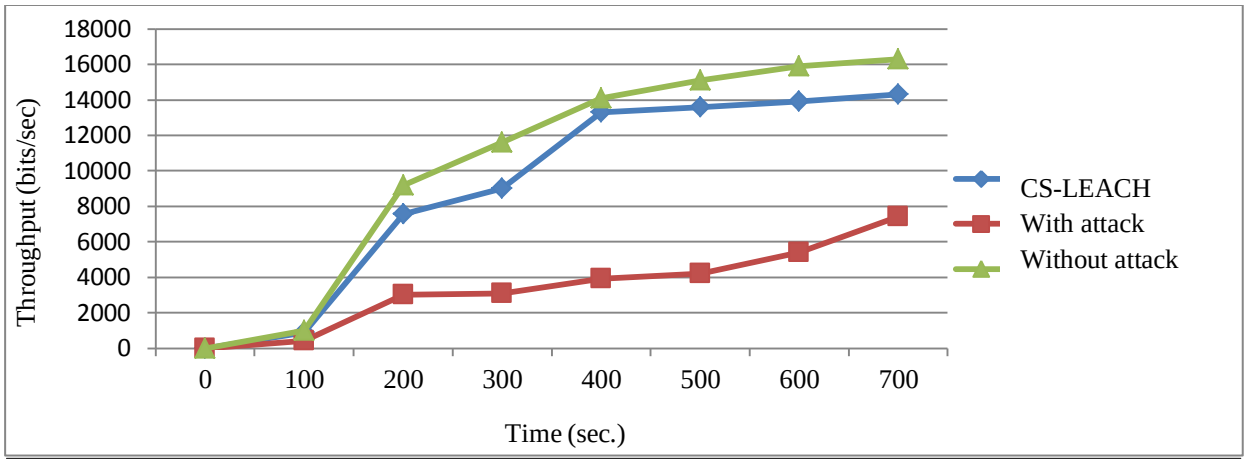

Figure 9: Throughput

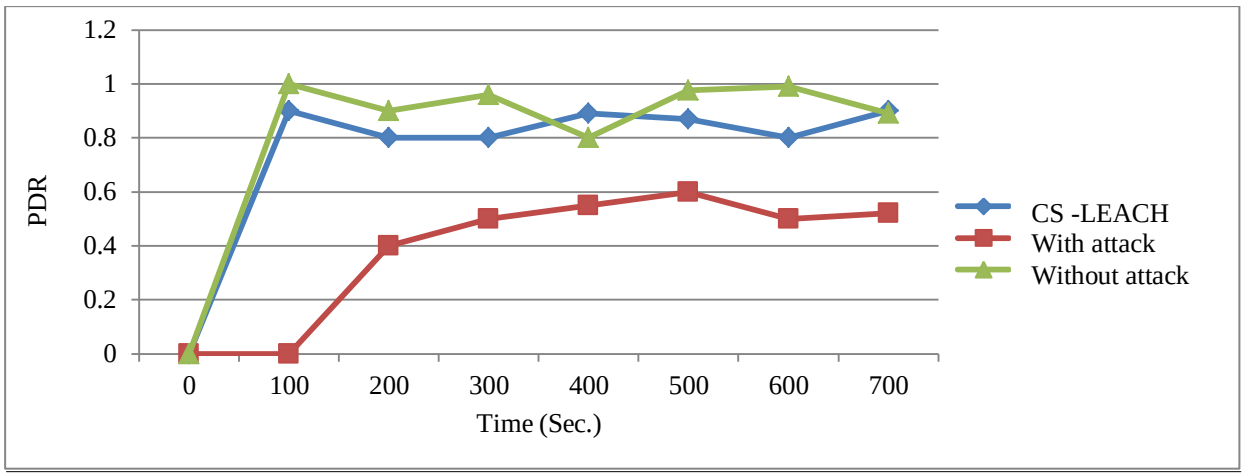

Figure 10: Packet delivery ratio

C. Delay

Delay is defined as the time consumed in transfer of data packets from source to destination i.e.
Delay = ∑ (received time – send time) / ∑ (No. of connections)
Figure 11 is the result of simulation with attack, without attack and CS-LEACH.

D. Overhead

Overhead defined as the extra time for data packets delivery Figure 12 is result of simulation for CS-LEACH, without assault, and with attack.

E. Energy consumption

Initially every node is allotted 10 joules of energy. The consumption is defined as
Energy consumption = Original energy - Existing energy

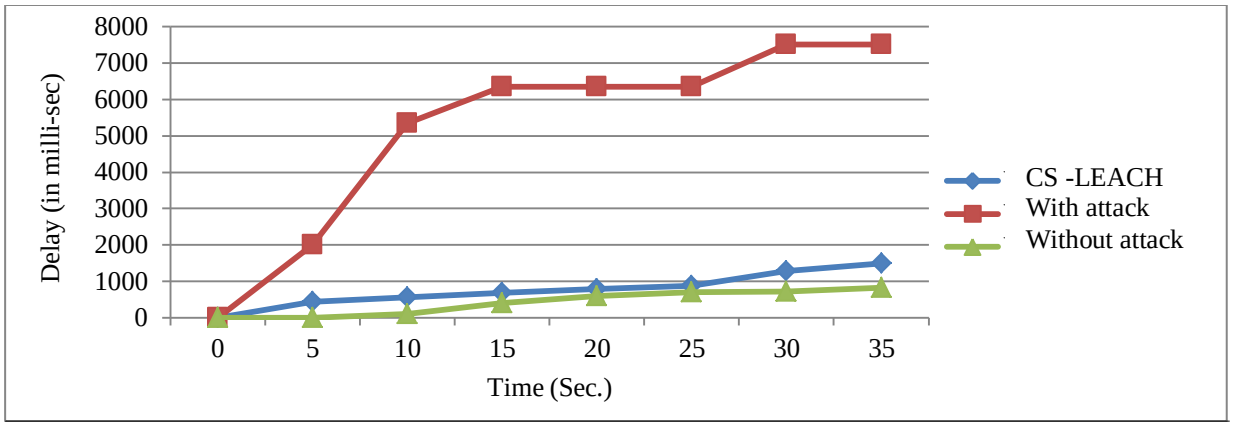

Figure 11: packet Delay

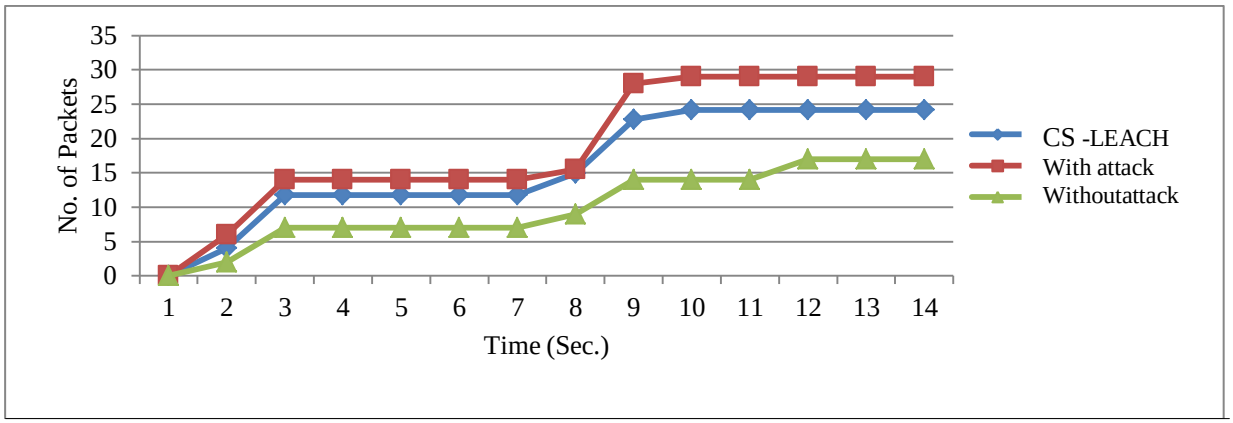

Figure 12: Overhead

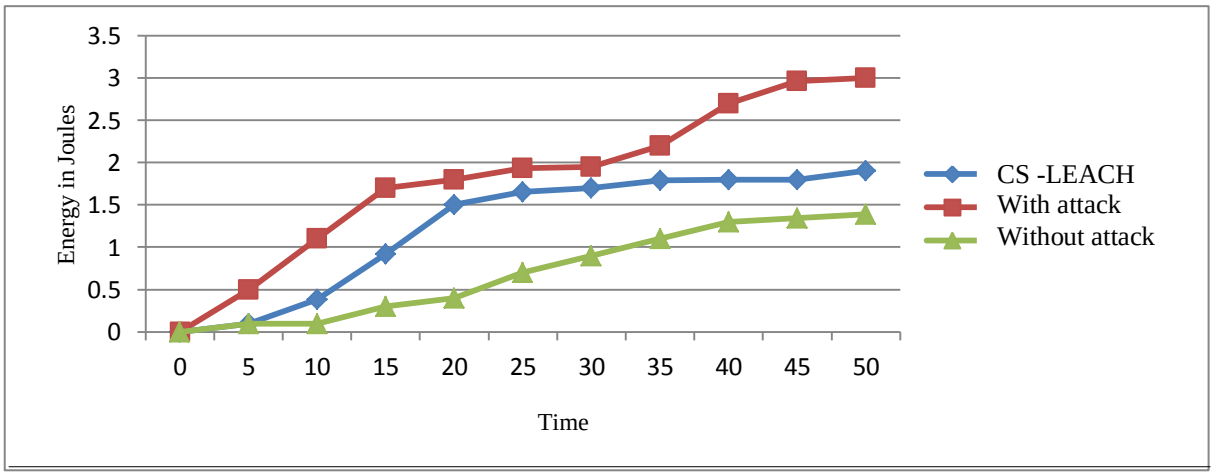

Figure 13: Consumption of energy

VI. CONCLUSION

Internet of things (IoT) an assembly of huge quantity of networks such as wireless sensor networks is formed for the purpose of joining unlike technologies. IoT styles practice of unlike techniques for the transfer of physical items for data processing composed at dissimilar places that are composed by sensors. The enormous and speedy expansion in the field of the IoT requires well-organized safety tools for the transfer of data. This paper presents a safe and effective CH selection technique CS-LEACH that is used with unlike WSNs united with the IoT. The appointment of CH is crucial as the data communication of the sensor node and the base station is done via this cluster head. Data transfer must be completed in a safe method as entirely information in a WSN is transferred over the CH to the BS. The mean node in the WSN gathered execution with large broadcast makes use of Hello flood attack so as to make CH cooperated. This paper suggests an innovative method based on unique Cyclic number, ID, and RBG color cube number authenticating CH. The work planned, makes upgrading in the efficiency of WSN by initial discovery of mean nodes for stopping nodes from the CH. This method benefits in the creation of large-sized collections. NS2 execution illustrates that the research work expels mean nodes in collections for rising cluster superiority and energy effectiveness. The operation of proposed work is done for throughput, energy consumption, delay, overhead, PDR, etc. In upcoming work, extra simulations will be carried out for the other parameters by increasing the number of nodes.

REFERENCES

[1] Rupinder Singh, Rachhpal Singh and 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.

