Available Online at www.ijcsmc.com

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. 10, Issue. 1, January 2021, pg.49 – 60

Securing Cluster Head in Wireless Sensor Network for Internet of Things

Rupinder Singh; Rachhpal Singh; Prabhjot Kaur
Khalsa College, Amritsar, E-mail: rupi_singh76@yahoo.com
DOI: 10.47760/ijcsmc.2021.v10i01.005

Abstract- Internet of Things (IoT) is a rapidly growing technology and will be of great importance in the future consisting of a vast number of interconnected networks. One of the important networks that will be part of future IoT is Wireless Sensor Network (WSN) connected with the help of rapidly emerging devices and technologies. Due to the unlimited interconnection of various technologies in IoT, the threat to confidentiality and security of data has also increased. WSN uses Low Energy Adaptive Clustering Hierarchy (LEACH) for constructing an energy-efficient network that is prone to a vast number of attacks and one of them is HELLO flood. This paper makes use of HFS-LEACH (Hello Flood Secure LEACH) as an extension to LEACH protocol for the purpose of protecting cluster head from Hello flood attack. HFS-LEACH makes use of RBG color cube numbers, a unique Automorphic number, and a unique ID for each sensor node for the purpose of authenticating a sensor node as CH. The HFS-LEACH is implemented with the help of NS2 for verifying its efficiency.

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

I. INTRODUCTION

Internet of Things (IoT) is a type of universal network architecture that provides facilities of the physical world by making use of data analyses and its processing. A wireless sensor network (WSN) is a collection of small sensor nodes that can be integrated with cloud computing, Big Data, etc. for the huge expansion in the field of IT. Figure 1 shows WSN integration with IoT. This enormous association of different technologies will be future in which several sensor nodes will be used for collecting information needed. This will help in data collection at faraway places where suitable communication and infrastructures are not available. The IoT and its integration with different technologies are going to provide a large number of applications including industrial toxic

vapors, patient tracking, medicine, environment monitoring, radioactive sensitive areas, active volcanoes sites, etc. The most important concern of IoT and WSN integration is to provide data confidentiality.

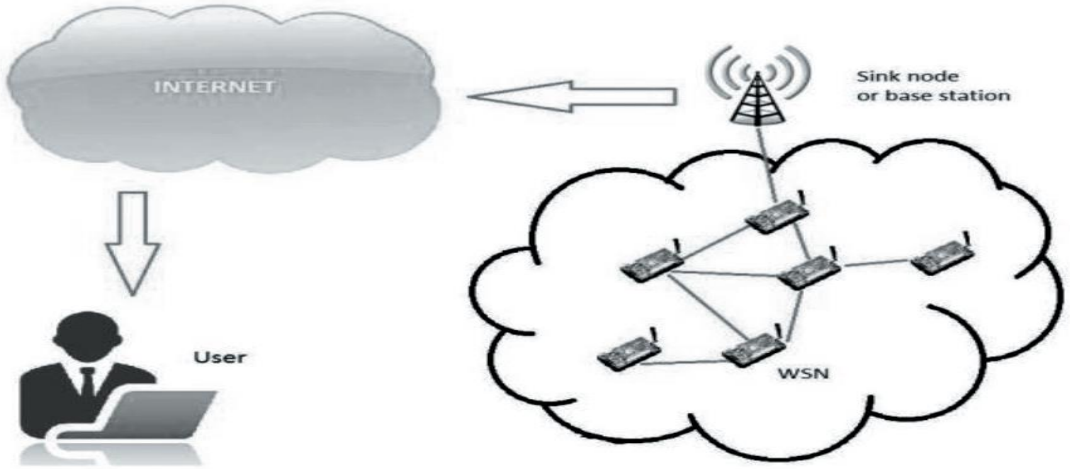

Figure 1: WSN integration with IoT

In this research work, a protocol for the detection of HELLO flood attack in an efficient manner is proposed when WSN is integrated with IoT. The proposed protocol is an extension to Low Energy Adaptive Clustering Hierarchy (LEACH) that makes use of clustering along with Received Signal Strength (RSS) so as to dynamically select Cluster Heads (CHs). LEACH is vulnerable to a large number of attacks and one of them is HELLO flood attack launched to make malicious node CH.

HFS-LEACH (Hello Flood Secure LEACH) an extension to LEACH protocol is proposed in this paper for preventing mean from being selected as CH. Wireless Sensor Network (WSN) is a collection of small sensor nodes that work together and pass collected data to a central place Base Station (BS) so as to distribute it at many locations via IoT. The complexity of security algorithms makes it very difficult for their implementation due to the limited battery power provides to small sensor nodes.

Hello packets are used by sensor nodes for the purpose of discovering neighbor nodes in the WSN, but they can be used by an attacker node with high transmission power to launch a hello flood attack. The countermeasures use for preventing hello flood attack are discussed in [1] as previous work. HFS-LEACH makes use of RBG color cube number, Automorphic number, and unique ID, so as to authenticate CH. The remaining paper is structured as: In section II, WSN hello flood attack is discussed, section III explains the unique WSN formation of clusters, section IV discusses HS- LEACH, section V describes NS2 simulation results.

II. HELLO FLOOD ATTACK

Hello flood attack is used in WSN by the mean node for sending Hello packets to other sensor nodes with the power of wireless transmission. Due to this strong power transmission malicious node is easily selected as CH by other sensor nodes in the network. The malicious node by implementing this technique makes the impression that it is a nearby node of sensor nodes in WSN and uses it for trouble making essential routing protocol for the purpose of launching further

attacks. The attacker after becoming the parent node in WSN controls the sensor node clusters as per the scenario shown in figure 2. The mean node regulates all the data transfer in the cluster that is routed via this CH for the purpose of increasing communication delay in the WSN. The attacker transmits hello messages to a large range of areas in WSN and almost forces and influences remaining sensor nodes that attacker node is very close to them. The cluster sensor nodes waste limited power available in replying to the attacker HELLO message by creating a non-clear state in the network. Hello flood attack used in the WSN is represented in Figures 3 and 4. In the figure triangle, rectangle, and circles represent attacker, base station, and sensor nodes respectively.

For initiation of WSN hello flood attack, hello messages are aired by the attacker by catching a sensor node for declaring as their neighbor. The sensor nodes in WSN after receiving this hello message start interacting with the attacker node and by making an entry in the routing table as a neighbor. All the sensor nodes in WSN transfer data to the base station with the help of this CH. The nodes in WSN accept the attacker as the neighbor node as the message is with the shortest path from the CH. Due to this illusion, they start communicates with the mean node. The attacker after having complete control of sensor nodes in the WSN manipulates the data collected by the sensor node as per the desire as the contact of these nodes is totally cut from BS.

Figure 2: Hello Flood Attack

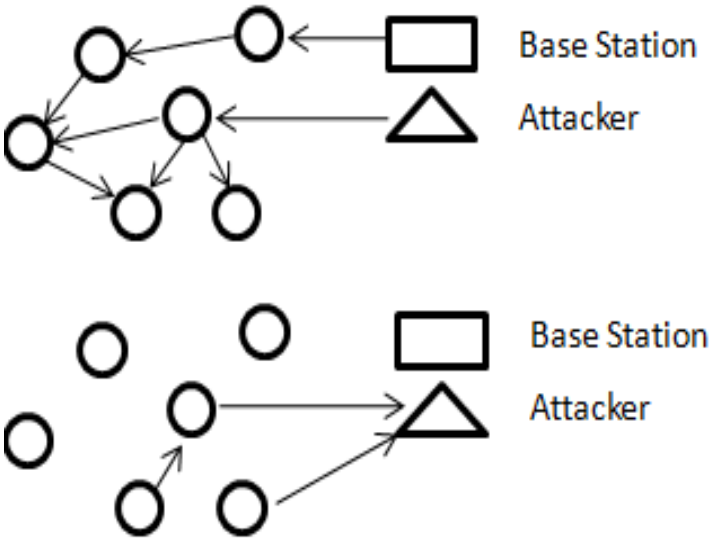

Figure 3: Hello packets broadcast by an attacker with high transmission power.
Figure 4: Sensor nodes selecting attacker as a neighbor.

III. WSN CLUSTERING

Almost every application used in WSN integrated with IoT works in an environment that is unattended and harsh. In such environments, human monitoring is not always possible. The organization of sensors is finished by controlling methods in an exceptionally huge region with the goal that specially appointed system arrangement is feasible. A huge number (hundreds or thousands) of sensors are required to cover such an enormous area and these nodes are very vitality compelled. The power delivering batteries cannot be consistently revived. Hence, it necessitates that uniquely planned vitality productive steering conventions ought to be actualized in WSN for protecting sensor organize lifetime.

Therefore, it is needed that the sensor nodes in the WSN should be grouped into clusters. This is required for satisfying the objective of scalability and high energy efficiency condition in WSN so that the network exists in large scale environments. In clustered hierarchical WSN structure, each of the clusters has a fixed number of member sensor nodes. One of the member sensor nodes that control the entire cluster is called CH. The task of fusion along with aggregation is performed by CH. The clustering of sensor nodes forms a two-level hierarchy with CH on a higher level and member nodes on a lower level. The cluster members transmit data to the WSN through corresponding CH. These CH's transmit data collected from sensor nodes to the BS directly or using midway communication. The CH sends collected data to long distances so they have to spend higher energy rates. In order to balance the energy consumption of all the sensor nodes, the CH is regularly re-elected among cluster sensor nodes. Figure 5, represent WSN single-hop intra-cluster communication and multi-hop inter-cluster communication.

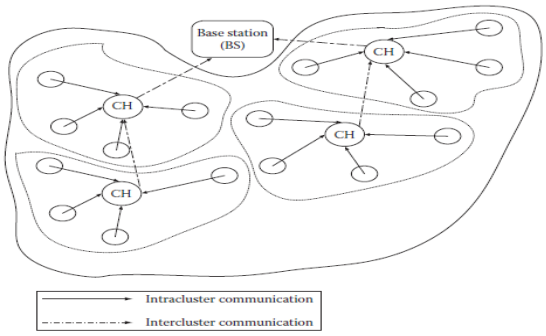

Figure 5: Clustered WSN

IV. AUTHENTICATED CH SELECTION

After WSN is set with numerous sensor nodes, the initial step is to shape groups for encouraging vitality productive correspondence. After the arrangement of the group, the system task is dispersed into rounds. Each round works in three stages as appeared in Figure 6.

These stages use for the construction of WSN are Synchronization stage, Authenticated CH Election stage, Data Aggregation, and Forward stage. This work center just around Authenticated CH Election stage. A WSN CH choice framework must fulfill the accompanying conditions:

- Unpredictability: consistency about CH should be outlandish by a sensor node.
- Non-manipulability: CH choice outcomes are non-flexible.
- Agreement property: each sensor node in WSN gets the same decision results.

The race of a CH is thought to be founded on a typical irregular worth. First, this normal arbitrary worth is produced and all group individuals need to concur with a typical worth CH. All cluster individuals add to producing arbitrary worth which is normal with the way toward circulating irregular estimations of their own. A malevolent sensor hub can appraise the basic qualities created by other sensor hubs by deferring its arbitrary worth with the goal that others can disseminate their wine. The assailant hub can hinder non-manipulability conditions by getting away transmission, for example, the assailant hub maintains a strategic distance from the irregular worth transmission, in order to change the CH race result because of changes in like manner esteem. Typical sensor hub transmission lay on bunch distance across between-group sensor hubs. By diminishing transmission control a noxious hub can create various basic qualities by to disregard the understanding property of decision results.

The CH choice for the most part relies upon the quality of the signal, which is utilized by the sensor hubs for the telecom of hello message. The sensor hub having more battery reinforcement can produce an all the more dominant signal and is relied upon to move toward becoming CH. The pernicious node is typically fitted with a gigantic power reinforcement, so it can exploit this to communicate an incredible hello message for getting to be CH. The CH decision is chosen by both irregular qualities and signs solidarity to stay away from a malevolent hub from chose as CH. Yet at the same time, the odds are that assailant hub can control the above-forced conditions. Along these lines, there is a requirement for a solid CH verification technique. Beneath in the following passage, a protected WSN CH determination technique is talked about.

The RBG shading framework as appeared in figure 7 characterizes each shading by the measure of creation of red, green, and blue shading. For the most part, computerized records utilize 0-255 whole numbers in order to indicate these measures. RGB shading 3D square is utilized to show these hues smooth advances. It utilizes 8 bits for each segment and a sum of 256*256*256 conceivable number of hues can be utilized. An automorphic number is a number that is available in the last digit(s) of its square. Model: 25 is an automorphic number as its square is 625 and 25 is available as the last digits. The BS dispense an exceptional ID, automorphic number, and RBG shading 3D shape number to every sensor hub during the arrangement of groups and record this in the enlistment table. At the point when a sensor hub is picked as CH, it needs to take consent from the BS before begins working. The BS verifies the CH after confirmation of data from the enrolment table and checking the rest of the vitality level. Figure 8 stream diagram outlines the proposed confirmation system of secure determination of CH.

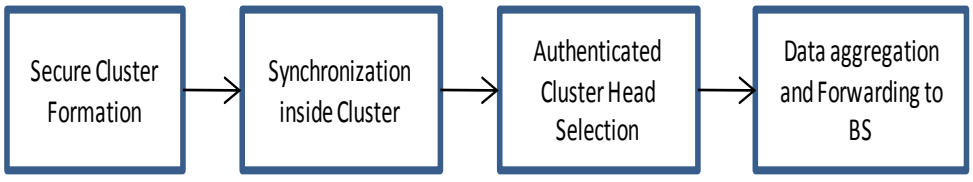

Figure 6: Operation of the sensor network

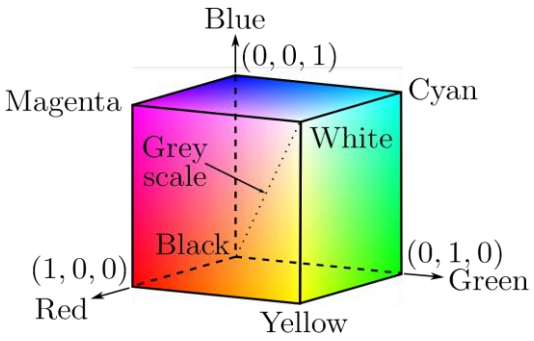

Figure 7: RBG color cube

V. RESULTS OF SIMULATION

This unit of the paper provides results of the simulation for the HFS-LEACH protocol to show that the proposed work is effective. The simulation is performed in NS 2.35 with the following 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

Throughput is a significant system parameter utilized for estimating the execution of remote sensor arranges. Throughput is characterized as the normal pace of parcels (packets) conveyed effectively. Throughput is the complete number of bundles that are gotten at the goal per unit time. Throughput is characterized as:

Throughput = (Total packets delivered at destination)/(time of simulation)

Figure 9 indicates throughput of the reproduced WSN with Hello flood assault, without Hello flood assault, and after usage of HFS-LEACH. The figure demonstrates that HFS-LEACH builds throughput after the disengaging Hello flood assault.

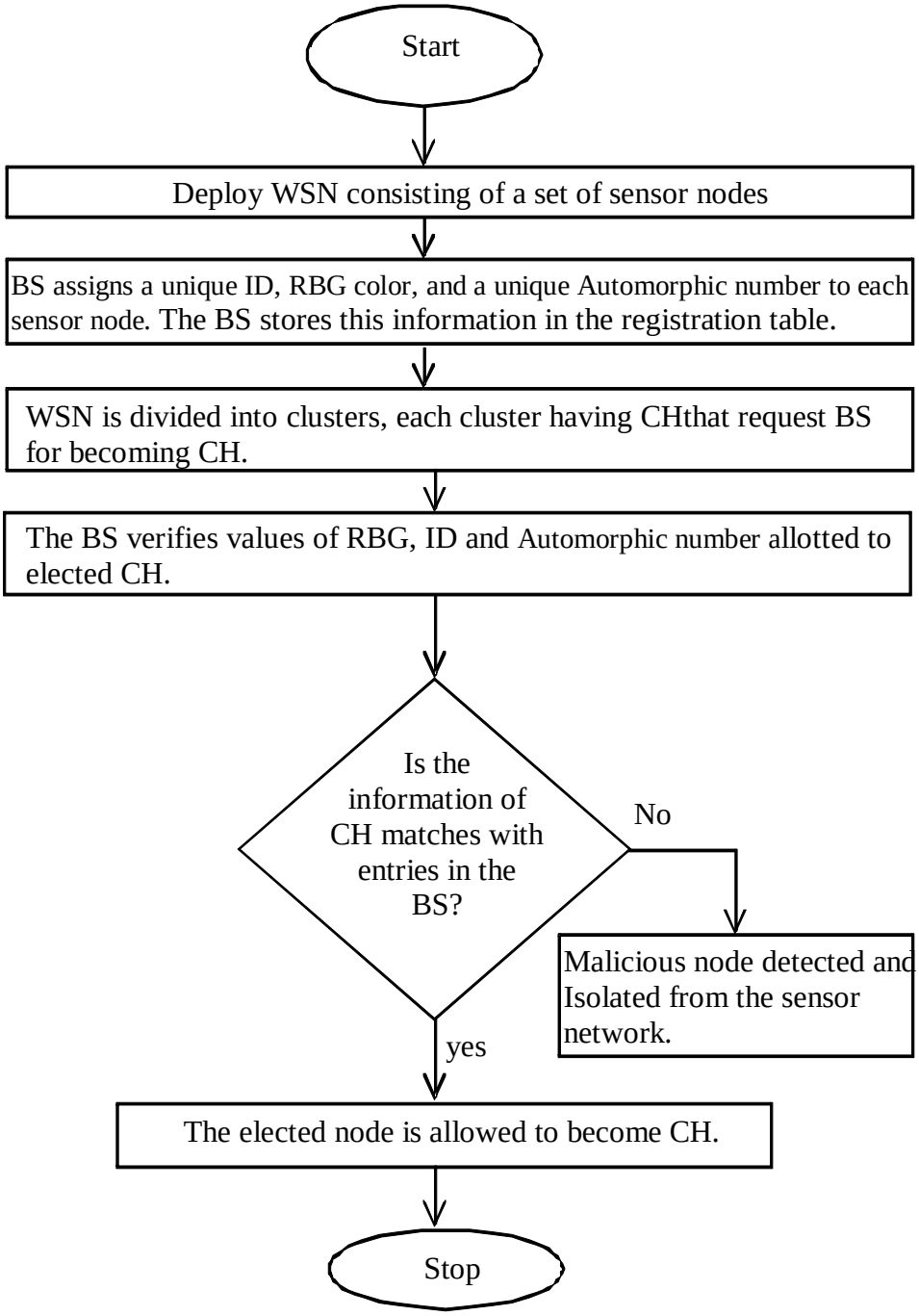

Figure 8: Flow chart of HFS-LEACH.

B. Packet delivery ratio (PDR)

PDR is the proportion of parcels (packets) gotten at the goal to bundles produced at the source. PDR is characterized as (Packets got/packets produced) * 100

Figure 10 gives PDR to HFS-LEACH, Hello flood assault, and without assault. The outcomes show an increment in PDR.

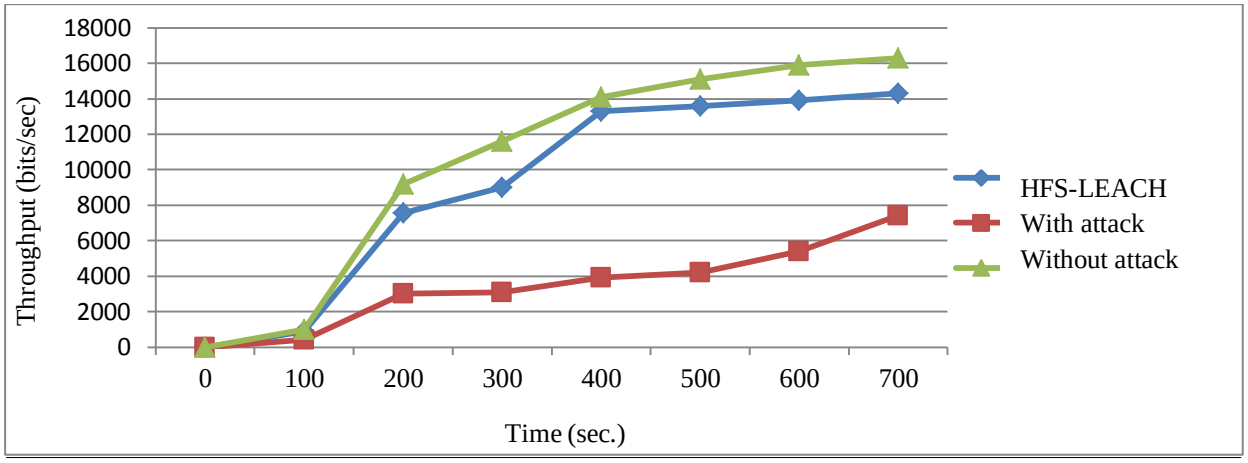

Figure 9: Throughput

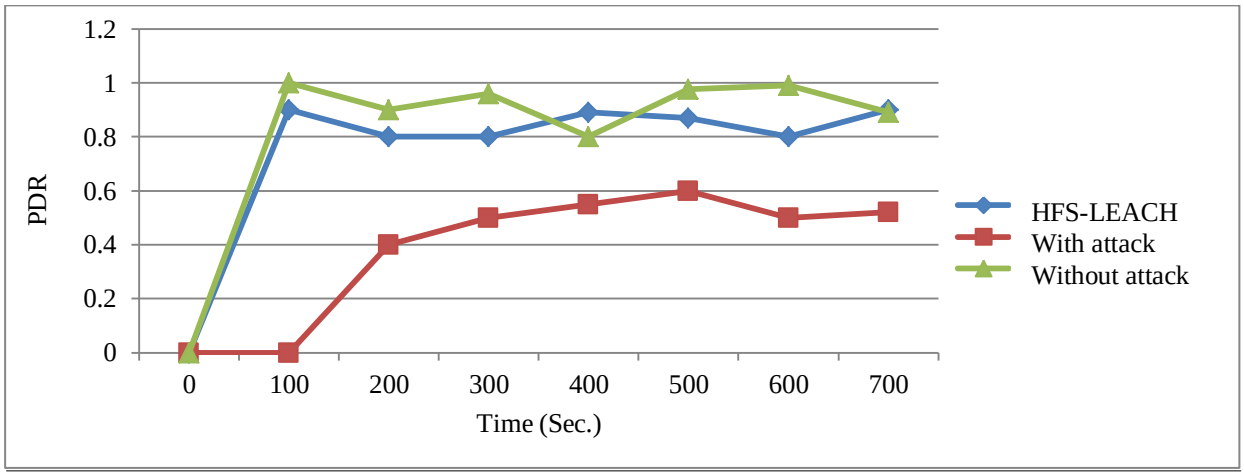

Figure 10: PDR

C. Delay

The postponement is the normal time for bundle conveyance at goal and furthermore incorporate Delay of course revelation and information parcel (packets) transmission line. The Delay is characterized as:

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

Figure 11 demonstrates the postponement for HFS-LEACH, without assault, and with assault

D. Overhead

Overhead is characterized as the inordinate time taken for the conveyance of parcels to the goal. Hello flood propelled as CH builds overhead in WSN. The overhead is the check of bundles that are utilized for WSN directing. Figure 12 shows overhead for HFS-LEACH, without assault, and enduring an onslaught. The proposed HFS-LEACH diminishes the overhead of the WSN organization in the wake of expelling a vindictive hub.

E. Energy consumption

Each sensor hub is allotted 10 joules at the beginning of recreation named as introductory vitality. This vitality worth is passed as info contention and a sensor hub uses an unmistakable measure of vitality for transmitting and accepting each bundle. The vitality utilization level is determined as:

Energy consumption = Initial energy - Current energy

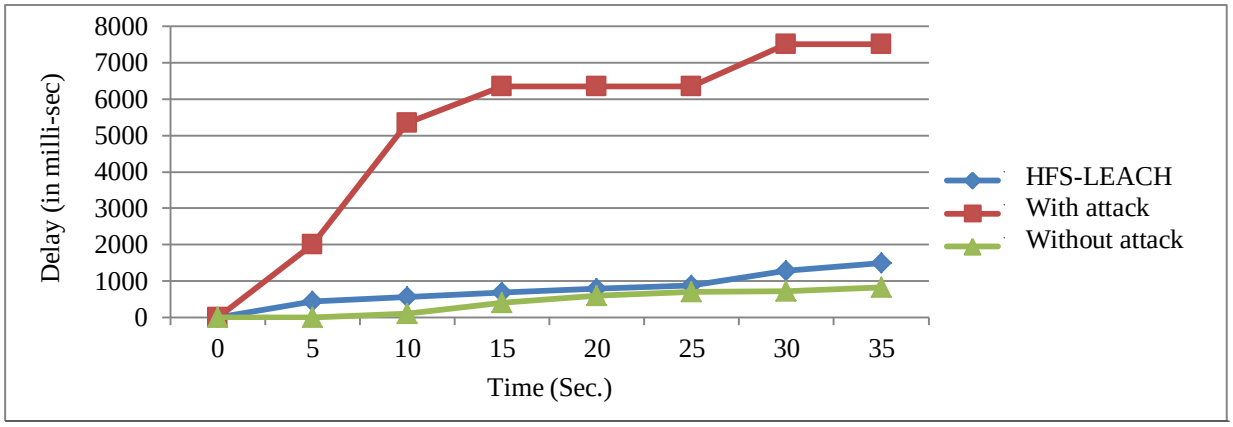

Figure 11: Delay

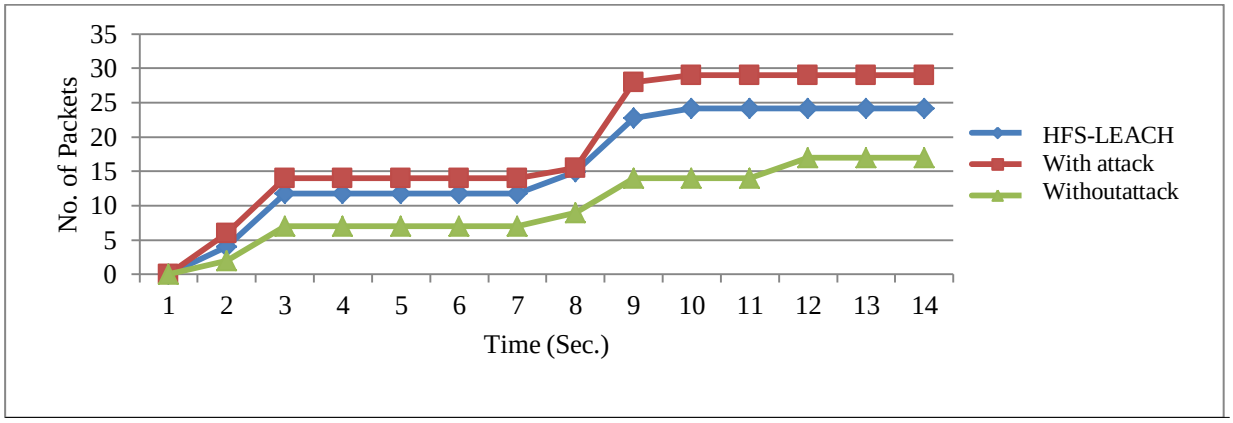

Figure 12: Overhead

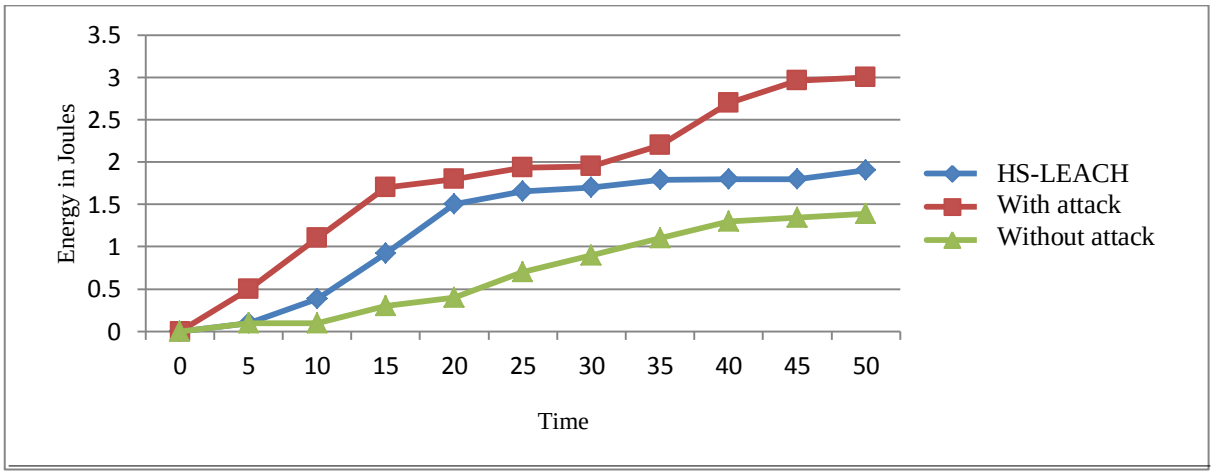

Figure 13: Energy consumption

VI. CONCLUSION

Internet of things is a collection of a large number of networks such as wireless sensor networks for connecting different technologies. Internet of things makes use of different tools for the communication of physical objects for processing the data collected at different locations that are collected by sensor nodes. The vast and rapid development in the field of the internet of things required efficient security tools for the communication of data. In this paper, a secure and efficient cluster head selection method is proposed that is used with different wireless sensor networks integrated with the internet of things. The election of the cluster head is vital, the data communication of the sensor node and the base station is done via this cluster head and should be done in a secure way as all data in a wireless sensor network with is communicated through the cluster head to the base station. The malicious node in the clustered implementation of WSN with high transmission power makes use of Hello flood attack for so as to make cluster head compromised. The research work in this paper proposes a novel technique based on ID, RBG color cube number, and unique Automorphic number for the purpose to authenticate cluster head. The proposed work in this paper, make improvement in the performance of WSN by early detection of malicious nodes for preventing wireless nodes from the association of cluster head. This approach helps in the formation of large-sized clusters. The NS2 simulator implementation shows that the purpose work results in the expel of malicious nodes in clusters for raising cluster quality and energy efficiency. The implementation of proposed work in NS2 is done for the delay, energy consumption, PDR, overhead, throughput, etc. In future work, additional simulations for increased sensor nodes will be performed for evaluating the performance of the proposed technique.

REFERENCES

[1] 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.

[2] 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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

