Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

Secure Cluster Head Selection In WSN Integrated With IOT

Rupinder Singh* and Rachhpal Singh

1Khalsa College Chawinda Devi, Amritsar, E-mail: rupi_singh76@yahoo.com
2Khalsa College, Grand Trunk Rd, Amritsar, Punjab. E-mail: rachhpal_kca@yahoo.co.in

ABSTRACT

Internet of Things (IoT) is of great significance in the future and is rapidly developing by connecting heterogeneous devices with several technologies. One of such network is Wireless Sensor Network (WSN) that is integrated with IoT. This interconnectivity of different networks leads to the risk of confidentiality and security of data. WSN routing protocols such as LEACH (Low Energy Adaptive Clustering Hierarchy) is prone to a large number of attacks and one of them is a HELLO flood attack. In this paper, HSRP (Hello flood attack Secure Routing Protocol) an extension to LEACH protocol is proposed for protecting the CH (Cluster Head) against Hello flood attack. HSRP makesdata encryption with the help of Armstrong number and decryption with AES algorithm so as to verify CH identity. The proposed technique can be used to protect IoT form HELLO flood attack consisting of various WSNs. The proposed HSRP is implemented by making use of network simulator NS2, the results indicate that the HSRP has a substantial ability to detect flooding attack HELLO for creating the malicious node as CH.

KEYWORDS: Internet of Things, Wireless sensor network, Hello flood attack, Armstrong number, Cluster head.

***Corresponding author:**

Dr. Rupinder Singh

Khalsa College Chawinda Devi

Amritsar

E-mail: rupi_singh76@yahoo.com

INTRODUCTION

Internet of Things (IoT) is a universal network architecture used to provide facilities in the physical world by analyzing and processing data.Wireless sensor network(WSN) composed of low powersensor nodes, along with Big Data and cloudcomputing led to a greatexpansion of IoT. Figure 1 shows the integration of WSN and IoT.This combination of various technologies can be used to place multiple sensor nodes everywhere, so that valuable information needed for collection can be obtained. This will help in data collection in places without appropriateinfrastructures and communication. The integration of WSN and IoT include a large number of applications includingremote patient tracking, medicine, environment monitoring,active volcanoes, toxic vapors industrial sites, radioactive areas, etc. One of the most important issues of this integration is to provide security and confidentiality of the data.

In this paper, an effective protocol for detecting HELLO flood in WSN is proposed when it is integrated with IoT. LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is used for the implementation of WSN. LEACH is used for clustered implementation of WSN making use of Received Signal Strength (RSS) so as to dynamically select Cluster Heads (CHs). LEACH is also exposed to HELLO flood attack in case a malicious node is selected as CH.

Cryptographic methods used for the prevention of a HELLO flood attack are not so supportive and certain non-cryptographic methods for detecting HELLO Flood attack exist but they lack efficiency

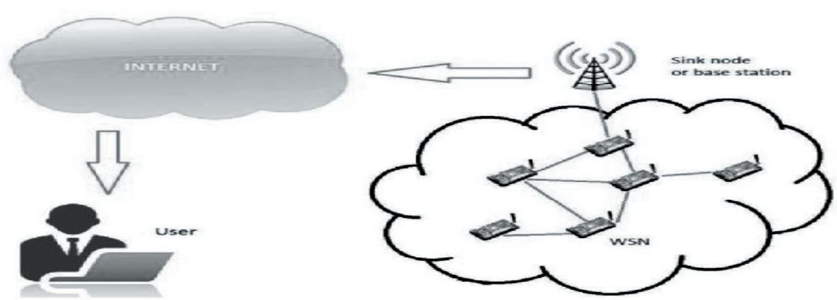

Figure 1: IoT & WSN integration

due to large test packet overhead. In this paper, HSRP (Hello flood attack Secure Routing Protocol) as an extension to LEACH protocol is proposed to protect CH from HELLO flood attack.

HSRP makes use of encryption using Armstrong number. The decryption is done with the help of AES algorithm so as to verify the identity of CH. The technique is implemented with the help of NS2 for the implementation of WSN. The results show that HSRP has substantial ability for recognition of HELLO flood attack which is launched for creating CH by the malicious node.The network layer attack Hello flood in WSN initiated when the attacker sent or replay hello packets used for neighbor discovery with the help of high power of transmission. This is done by creating an illusion of neighborsensor node to other nodes so as to disrupt underlying routing protocol. The attacker makes use of high transmission power to broadcast hello packets so that most of nodes in the network selectattacker as CH in LEACH protocol. The sensor nodes in the network are convinced that their neighbor is the attacker node. The nodes response to HELLO message generated by the malicious attacker and as a result are forced to energy waste, thus resulting in a confused state.

Heinzelman et al. [2] Introduced LEACH protocol for routing in the sensor networks, whichdivides the network into small clusters in which one sensor node is selected as CH and others as cluster members. The CH after gathering data from nodes send it to the Base Station (BS) and this CH is periodically re-elected. LEACH is divided into Setup and Steady phase used for the formation of the clusters along with CH and sending data to the BS. CHs are randomly changed and it is very hard to spot CHs. If attacker becomes a CH, then the HELLO flood attack can be easily launched. In our previous work [1], a large number of measures to tackle with a Hello flood attackare discussed.In this paper, HSRP as an extension to the LEACH protocol is proposed. HSRP is based on Armstrong number encryption and AES algorithm decryption so as to validate CHfor preventing WSN from Hello flood attack. HSRP can be used with different WSNs integrated with IoT so that secure communication is possible.

I. RELATED WORKS

In this section of the paper, the proposed work regarding selecting and securing CH'susing the LEACH protocol in WSN is discussed.

LEACH protocol was proposed by Heinzelman et al.[2]in which each of the sensornode has equal probability to be elected as CH. This protocol extendsthe lifetime of the network by allowing every sensor node to play role as CH. In LEACH protocol, sensor nodes with high remaining energy declare themselves to be CHs so that other nodes join as cluster members. LEACH assumes that there are no compromised nodes in the network, and therefore has no method for protecting cluster formation. F-LEACH[3] was one of the extensionsto LEACH proposed to defend the clusterformation from malicious nodes in the network. F-LEACHmakes use of common keys that are shared with BS in case a sensor node wants to become a CH, so as to check the authenticity of the node to become CH. The sink broadcast secure authentication for CHs using μTESLA is proposed in[4]. Normally nodesin the network join one legitimateCH, this methodprovide noway to validatesensor nodes which join any one of the clusters. For resolving this issue, Oliveira et al.[5] proposedSecLEACH. In this proposed work, BS is used to authenticate CH nodes while the CHs are further used to authenticate joining of sensor nodes. Both SecLEACH and F-LEACH requires nodes to be assigned pre-assigned keys for the purpose of verificationbefore deployment. LEACH and SecLEACH only help the network in external attackprevention from the attackers before joining of cluster formation process, i.e.these protocols are not able to protect CHs from internal attacks.

Various extensions[7-11]to LEACH protocol in the past have beenproposed, but the majority of these focus on energy consumption balancing over all the availablenodes so as to extend thenetwork lifetime. Few of these[8]extensions dealsecure election of CH. However, most of these extensions are not able to preventmalicious nodes from CH declarationas it can cheat other sensor nodes pretending having short distance with large residual energy. Liu[13]proposed a method of cluster formation in which pre-determined sensor nodes only can be declared as CHs. Other sensor nodes are allowed to join any cluster either via a relay node or directly. Any CH allocation or cluster joins isdone by some pre-assigning of polynomial share, therefore this method protects network from any external attacker during the process of clusterformation. The method proposed avoid a compromised relay node from invoking a DoS(Denial of Service)attack by the process of removing CH and its serving nodes connection. Sun et al.[14]in the work proposed a protected method for cluster formation whichis used for checking protocol conformity of nodes so as to discriminatemalicious nodes. In this work, physical network transformation is done into cliques so that memberscan be connected openly to each other in a clique. After clique is formed, each node in the clique checkswhether every member has the similarclique membership view or not. The methods of[19]has enhanced[14] safety, but with the assumption that during cluster formation no collisionsare possible. This type of assumptionused is very difficult to implement without using special measure like TDMA schedule assignment along with separation code. Nishimura et al.[21] in the work,proposed a methodby allocating a trust value to every cluster node of CHin which most trusted are allowed as CH. The limitation of this work is that it produces a lot overhead communication for trust evaluation system and is not appropriatein the case of resource-constrained sensor network.

Rifà-Pous et al.[20]based on the public key cryptography in the paper proposed a protected cluster formation method. The proposed method contains three phases; the phase of cluster discovery, the phase of CH designation, and the phase of cluster maintenance. In thefirst phase of cluster discovery, every node in a cluster is given same view as far as membership is concerned with other nodes in the cluster. In thesecond phase of the cluster designation, election of CHis considered on the basis of a numberof times already elected as CH in the past including number of its neighbors. In the cluster maintenance phase, CHsthat has been elected to providea certificate of authorization to each cluster member. The limitation of this method is that it assumes no node departs from participating of cluster discovery. Crosby et al.[21]in the paper proposed a CH election based on trustwhere each of the node provides trust values to anotheron the basis of behavior and trust so that trustworthy nodes are elected as CHs. A node behavior is counted by occurrence ofsuccessful and unsuccessful node transmissions. The more anode is successful in its transmission, the more superior reputation it has. During the process of electing new CH, nodes having more reputation value are suggestedby cluster members for role of CH so that one of them is elected as a new CH.

Buttyan et al.[22]proposed a CH selection scheme using cryptographic which hidesthe election processfrom outside nodes. But, the proposed work of concealmenttackles with only external attackers. A compromised nodein the network can expose the selection result with no trouble. The malicious node in the network can declare itself as a CH without having the eligibility.Sirivianos et al.[24]proposed SANE (Secure AggregatorNode Election) protocol. In this protocol all the legal CH membersof a cluster contribute in producing random value so that CH may be elected based on this randomvalue. SANE isfurther divided into three sub-schemes based on the generationand distribution of random value. The scheme makes use of Merkle's puzzle, commitment scheme, and scheme based on seeding. Dong et al.[25]in the work proposed scheme for preventing attackers from participating in the process of election by making use of IDassignment scheme, which binds ID of the node, itspolynomial shares and commitments. In this method,nodes not broadcasting participation message are not allowed for participating in CHelectionand are excludedfrom the process of electing CH candidates. TheCH is selected among one of the rest of the candidates, but still attacker may change election result of CH byescaping distribution of participation message. Although, this methodprovidesrecovery systemby combining various election results into one, but there is requirement of co-operation of CH candidates.

II. MATERIALS AND METHODS

The proposed HSRP to be used for detecting and isolating Hello flood attack in sensor network is discussed in this section of the paper. The WSN model along with assumptions is discussed first, followed by working of the proposed protocol.

A. WSN Model

The WSN considered to be a clusterednetwork having N static sensor nodes. The network includes special sensor nodes called CH and BS along with member nodes. CHs collectinformation from their clusters and then passes them to the BS for the purpose of making decisions/judgments. LEACH protocol is used for the formation of clusters in which every sensor node has a unique identity (ID). HSRP makes use of the following assumptionsfor the WSN.

1) Hello flooding attack sensor node is the compromised CH.
2) The attacker sensor node has a high power transmission.

3) All the sensor nodes in the network other than malicious nodes have same initial energy, power of transmission, power of computing, internal structure of storage, etc.
4) Nodes are allocated ID's that cannot be changed.
5) The Unique Armstrong number is allocated to each sensor node.
6) All the nodes in the network consume the same amount of energy for working on the same stage.

B. Implementation of HSRP

The HSRP is used as an improved extension to LEACH protocol with more security, therefore the proposed protocol make use of features of clustering used in the LEACH protocol. The working of LEACH protocol is divided into the steps of set-up and stable phase. In the first phase of set-up,all the nodes in the WSN follow the guidelines of fairness criterionalong with randomness criterion. In first and fairness criteria every sensor node in the WSN hasequal probability ofbecoming a CH. While in the second randomness criterion, random way is used for the election of CH. The chance of a node to be elected as CH entirely depends on two things. First whetherthe node is elected as CH in past recent rounds. Second,percentage of CH's IN the WSN. After the election of CH's in the WSN, each member chooses a cluster to join it on the basis of maximum RSS (Received Signal Strength)tillthe completion of all clusters.

Each cluster sensor node member has the responsibility of sensing surroundingof it, i.e.environment so as to forwarddata to CHs respectively. The CH's after collecting this information from member nodes forwardsthe information to the BS. The LEACH protocol is vulnerable against Hello flood attackbecause of these characteristics.Hello flood attack is one of the common routing attacksused in the WSN in which the malicious node broadcasts a huge number of hellomessagesto the sensor nodes with very higher transmission power in the WSN. The sensor nodes receiving such a hello message will consider malicious node as their CH. After becoming the CH, malicious node may create damage in WSNby modifying or discarding data received from cluster members.

C. Malicious CH determination

The BS of the WSN makes use of registration table in order to maintain records of created CHs andmembers of clusters along with malicious nodes as different sets. These set values are regularly updated as per the changesmade in the CHs and clusters.The following are the initial values for these sets

Set CH_{node} = {null}, to store CHs in the WSN.

Set CH_{member} = {null}, to store members of clusters in the WSN.

Set $CH_{malicious}$= {null}, to store detected malicious nodes in the WSN.

Each of the sensor nodesin the WSN trieswith a definite probability (p) to become CH following the criterion of both randomness and fairness. The nodes that are able to become CH broadcasts hello message for clusteringso as to attract sensor nodes tojoin it. The CH(i) is selected with the level of RSSso as to join in a specific area range. The memberscalculated by CH for the cluster are included in the set CH_{member}.

a) Unique ID allocation

The BS is used to allocate a unique ID number to each of the sensor nodes in the WSN. The request of any sensor node for becoming CH is accepted only if it providesallocated unique ID to the BS in order to fulfilnode validation.

b) Unique Armstrong number allocation

The BS is also given the responsibility of allocating a unique Armstrong number for each ID to the sensor node in WSN. Armstrong number is defined as m (digit) base n no. so that sum of its (base n) digits raised to the power m is no. itself. For example, $371 = 3^3+7^3+1^3 =27 + 343 +1$ is an Armstrong number. Any sensor node can become CH by sending an Armstrong number, encrypted hello message to the sensor nodes in the WSN. Table 1 displaysa sample registration tablewhich is maintained at BS.

The flowchart of figure 2 represents the working of HSRP for the purpose of authenticating CH by the BS. HSRP is a more secure version of the LEACH protocol as only authenticated sensor nodes in the WSN are allowed to become CH's. It becomes very difficult for a malicious node to become CH by only having high transmission power. Therefore, HSRP provides a secure network for the purpose of communication in the WSN.

Table 1: BS registration table

Sensor number	Allocated unique ID	Allocated Random Armstrong Number
001	S0001	153
002	S0002	407
.	.	.
.	.	.
N		54748

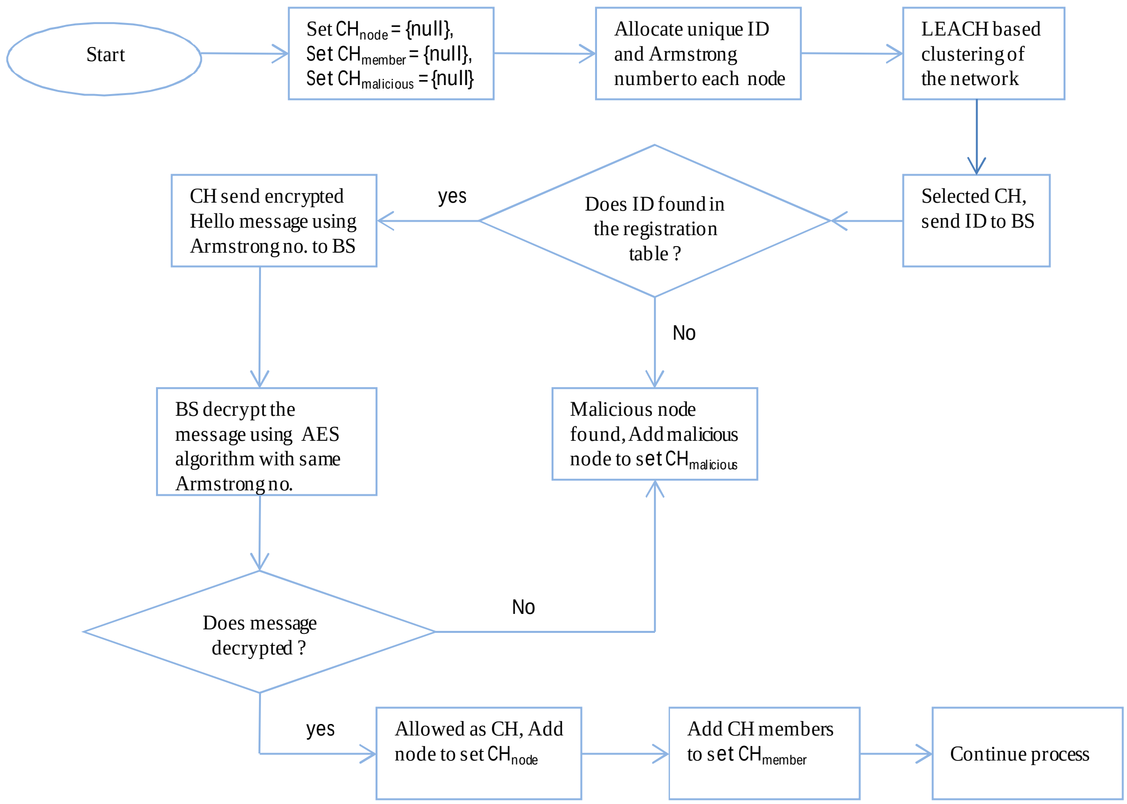

Figure 2: Proposed HSRP

III. RESULTS AND DISCUSSION

This part of paper presents results produced with the help of the simulation carried out in NS 2.35 to show HSRP effectiveness. The parameters of the simulation are shown in table 2.

A. Throughput

Network throughput is defined as the average rate of effectively delivered packets. Throughput calculation is done as:

Throughput = (Total no. of packets delivered) /(Simulation time);

The figure 3 displays throughput for WSN with, without, and under Hello flood attack. The figure also displays implementation of proposed HSRP. The proposed protocol after isolating Hello flood attack increases throughput.

Table 2: Parameters of Simulation

Parameter	Value
Simulator	Network simulator 2.35
Area in meters	800X800
Nodes	50
Routing protocol	LEACH
Type of Channel	Wireless
Size of Packet	512 byte
Model for Mobility	Two ray ground propagation model

B. Packet delivery ratio

Packet delivery ratio (PDR) of WSN is the ratio of total packets received to total packets generated. PDR is defined as

PDR = (Packets received at destination/packets generated by source) * 100

Figure 4 displaysPDR analysis for without attack, under attack, and implementation of HSRP. The figure 4 indicates that HSRP results in the increase of PDR.

C. Delay

Delay is the average time required to deliver the packet at the destination, includingthe process of route discovery and queue time for packet transmission. Delay is calculated as:

Delay = ∑ (arrive time – send them) / ∑ (Number of connections)

Figure 5 provide end-to-end delay in WSN withoutattack, under attack, and HSRP implementation. The figure indicates that HSRP results in the decrease in delay.

D. Overhead

Overhead is a measure of excess time by a protocolfor delivering packets to the destination. Hello flood attack results in increase of overhead in WSN. Figure 6 displaysoverhead for WSN without attack, under attack, and for HSRP. The HSRP decreasesoverhead for WSN as shown in figure 6.

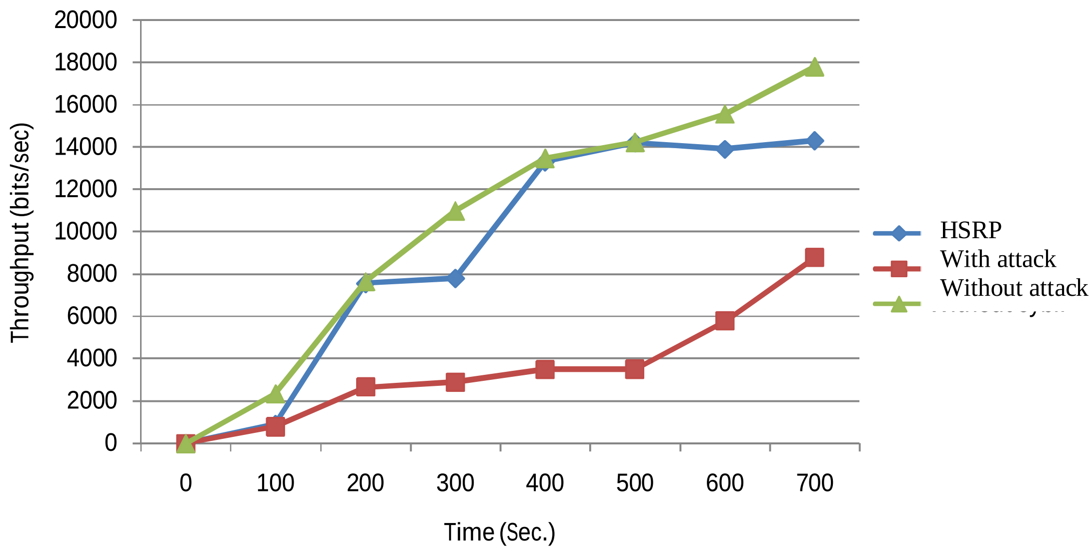

Figure 3: Throughput

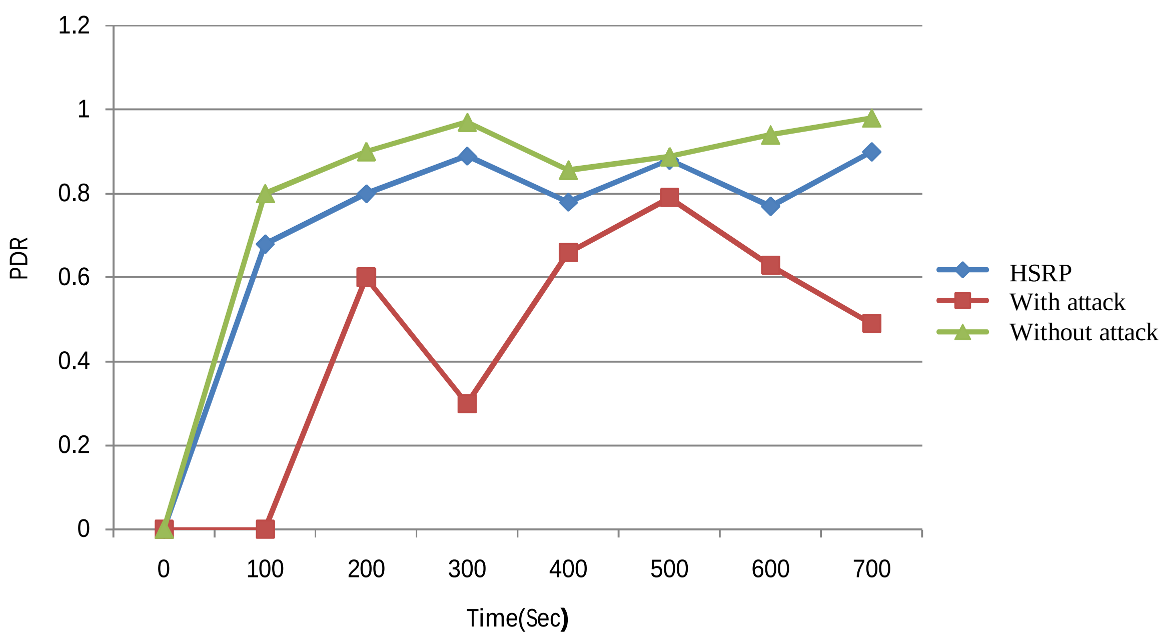

Figure 4: PDR

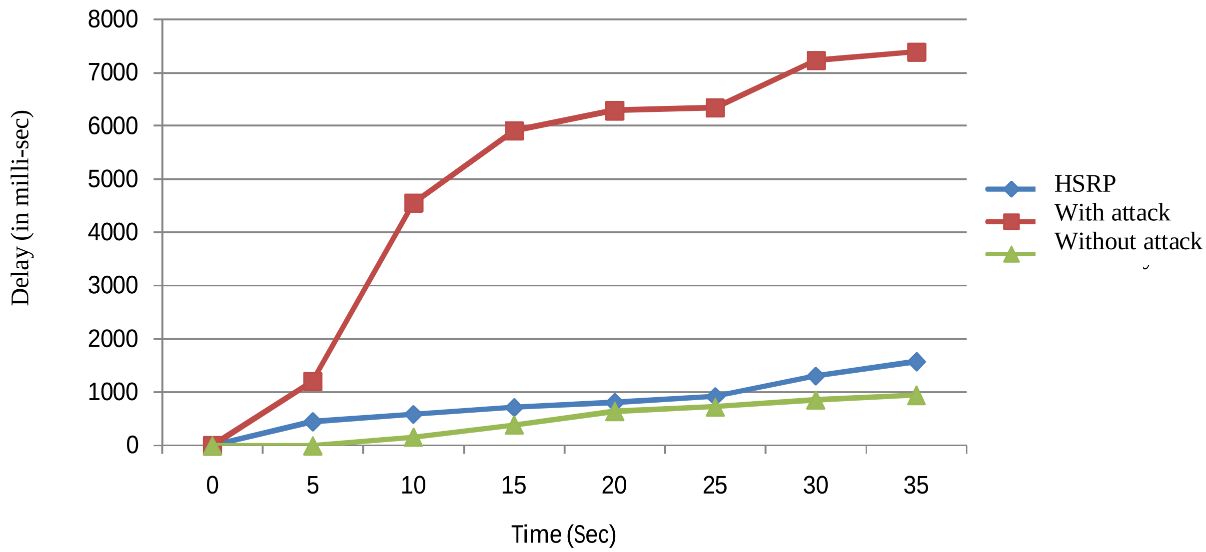

Figure 5: Delay

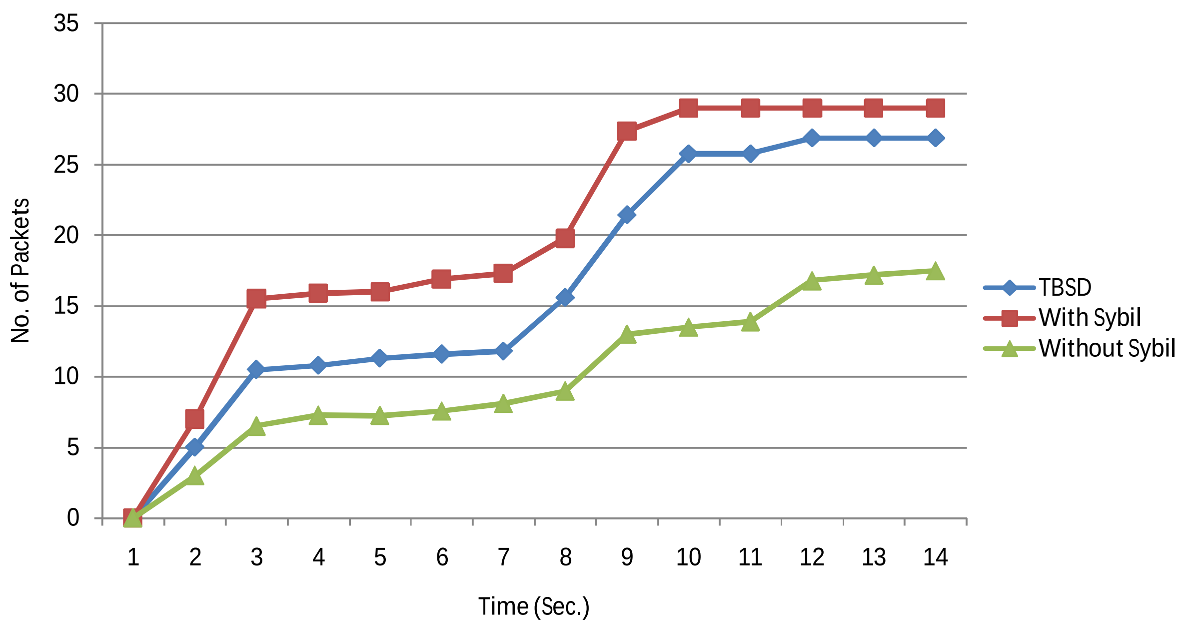

Figure 6: Overhead

IV. CONCLUSION

Io T make use of various network technologies for communication of physical objects. IoT also make use of different wireless sensor networks connected together so as to gather data present at separated locations. The huge progress in the services of IoT needs authentic security mechanism. The selection of cluster head in a secure way in wireless sensor network is important as all the communication between the sensor nodes and base station is done via the cluster head. Hello flood attack can be launched in sensor network so as to make cluster head compromised. In this paper, HSRP (Hello flood attack Secure Routing Protocol) as an extension to LEACH protocol in sensor networks is proposed. HSRP is based on Armstrong number encryption and AES algorithm decryption. HSRP can be used to increase performance by timely detection of malicious nods and avoiding the sensor nodes from such a mean cluster head. The IoT make use of different sensor networks connected together via different network technologies so as to share the information gathered. The proposed HSRP can be used to protect different WSNs from Hello flood attack in IoT. The proposed HSRPis implemented with the help ofNS2 and show the efficiency for parameter packet delivery ratio, throughput, overhead, and delay. The results of simulation show HSRP expels compromised nodes in the clusters. Further, simulation with more parameters will be done to increase number of sensor nodes in future.

REFERENCES

1. Singh R, Singh J, and Singh R. Hello flood attack Countermeasures in Wireless Sensor Networks.International Journal of Computer Science and Mobile Applications 2016;4(5), 2016;1-9.
2. HeinzelmanW. R., ChandrakasanA., BalakrishnanH. Energy-efficient communication protocol for wireless microsensor networks. In the proceedings of the 33rd Annual Hawaii International Conference on System Sciences. 2000.
3. FerreiraA. C., VilacaM. A., OliveiraL. B., HabibE., WongH.C., and LoureiroA. A.On the security of cluster-based communication protocols for wireless sensor networks. Proc. of 4th IEEE Int'l Conf. on Networking, Reunion Island, France. 2005; 17-21.
4. Perrig A. et al.SPINS: Security Protocols for Sensor Networks. Wireless Networks. 2002; 8(5):521-534.
5. Oliveira L. B. et al. SecLEACH-a random key distribution solution for securing clustered sensor networks. Proc. of 5th IEEE Int'l Symp. on Network Computing and Applications, Cambridge, Massachusetts, USA,. 2006.
6. Shen Y., Liu S., Zhang Z.Detection of Hello Flood Attack Caused by Malicious Cluster Heads on LEACH Protocol. International Journal of Advancements in Computing Technology. 2015; 7(2).
7. Kang S. and Nguyen T. Distance Based Thresholds for Cluster Head Selection in Wireless Sensor Networks. IEEE Communications Letters. 2012; 16(9):1396-1399.

8. Han Y., Park M., and Chung T. SecDEACH: Secure and Resilient Dynamic Clustering Protocol Preserving Data Privacy in WSNs. Proc. of the 2010 Int'l Conf. On Computational Science and Its Applications. 2010; 6018(1): 142-157.
9. Katiyar V., Cand N., Gautam G. C. and Kumar A. Improvement in LEACH Protocol for Large-scale Wireless Sensor Networks. Proc. of Int'l Conf. On Emerging Trends in Electrical and Computer Technology. 2011;1070-1075.
10. Saadat M., Saadat R. and Mirjality G. Improving Threshold Assignment for Cluster Head Selection in Hierarchical Wireless Sensor Networks. Proc. of Int'l Symposium on Telecommunications. 2010; 409-414.
11. Ren P., Qian J., Li L., Zhao Z., and Li X. Unequal Clustering Scheme based LEACH for Wireless Sensor Networks. Proc. of Fourth Int'l Conf. on Genetic and Evolutionary Computing. 2010;90-93.
12. Devi G., Sankar R., and Sahoo N. Hello Flood Attack Using BAP in WirelessSensor Network. International Journal of Advanced Engineering Research and Science. 2015; 2(1).
13. Liu D. Resilient Cluster Formation for Sensor Networks. Proc. of 27th Int'l Conf. on Distributed Computing Systems. 2007; 40-48.
14. Sun K. et al.Secure Distributed Cluster Formation in Wireless Sensor Networks. Proc. of 22nd Annual Computer Security Applications Conference. 2006; 131-140.
15. Mayur S., Ranjith H. D. Security Enhancement on LEACH Protocol From HELLO Flood Attackin WSN Using LDK Scheme. International Journal of Innovative Research in Science, Engineering andTechnology. 2015; 4(3).
16. Rawan S., Suhare M., Manal A. Intrusion Detection of Hello FloodAttack in WSNs Using Location Verification Scheme. International Journal of Computer and CommunicationEngineering. 2015; 4(3).
17. Kaur D., Singh R. Energy level based Hello Flood attack Mitigation on WSN. International Journal of Embedded Systems and Computer Engineering. 2015.
18. Jyoti, Bansal A. Detection of Hello Flood Attack on Leach Protocol Based on Energyof Attacker Node. International Journal of Innovations & Advancement in Computer Science, 2015; 4(1).
19. Wang G., Kim D., and Cho G. A Secure Cluster Formation Scheme in Wireless Sensor Networks. Int'l Journal of Distributed Sensor Networks. 2012.
20. Rifà-Pous H. and Herrera-Joancomartí J. A Fair and Secure Cluster Formation Process for Ad Hoc NetworksWireless Communications. 2011: 56(3): 625-636.

21. Crosby G. V and Pissinou N. Cluster-based Reputation and Trust for Wireless Sensor Networks. Proc. of the 4th IEEE Consumer Communications and Networking Conference. 2007; 604-608.
22. Buttyan L. and Holczer T. Private Cluster Head Election in Wireless Sensor Networks. Proc. of the Fifth IEEE Int'l Workshop on Wireless and Sensor Network Security, IEEE. 2009;1048-1053.
23. Magotra S., Kumar K. Detection of HELLO flood Attack on LEACH Protocol. IEEEInternational Advance Computing Conference. 2014.
24. Sirivianos M. et al.Non-manipulable Aggregator Node Election Protocols for Wireless Sensor Networks. Proc. of Int'l Sympo. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks. 2007;1-10.
25. Dong Q. and Liu D. Resilient Cluster Leader Election for Wireless Sensor Networks. Proc. of IEEE 6th Annual Comm. Society Conf. on Sensor, Mesh and Ad Hoc Communications and Networks. 2009;108-116.
26. Nishimura I., Nagase T., Takehana Y., and Yoshioka Y. Secure Clustering for Building Certificate MangementNodes in Ad-Hoc Networks. Proc. of 14th Int'l Conf. On Network-Based Information Systems, Tirana, Albania. 2011.
27. Steffi J., Priyanka A., Tephillah S., and Balamurugan A. M. Attacks and countermeasuresin WSN. International Journal of Electronics & Communication. 2014; 2(1).
28. Saini S. K., Gupta M. Detection of Malicious Cluster Head causing Hello FloodAttack in LEACH Protocol in Wireless Sensor Networks. International Journal of Application or Innovation inEngineering & Management. 2014; 3(5).
29. Dubey A., Meena D., Gaur S. A Survey in Hello Flood Attack in Wireless SensorNetworks. International Journal of Engineering Research & Technology. 2014; (1).
30. Singh V. P., Aishwarya S., Ukey A., and Jain S. Signal Strength based Hello FloodAttack Detection and Prevention in Wireless Sensor Networks. International Journal of ComputerApplications. 2013; 62(15).
31. Fatema N,Brad R. Attacks and counterattacks on wireless sensor networks. International Journal of Ad hoc, Sensor & Ubiquitous Computing. 2013; 4(6).
32. Wanjari A., Dhamdhere V. Evading Flooding Attack in MANET Using NodeAuthentication. International Journal of Science and Research (IJSR). 2014; 3(12).
33. Haghighi M. S., Mohamedpour K., Varadharajan V., and Quinn B. G. Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks. IEEEtransactions on information forensics and security. 2011; 6(4).

34. Singh V. P., Jain S., and Singhai J. Hello Flood Attack and its Countermeasures inWireless Sensor Networks. International Journal of Computer Science Issues. 2010; 7(3).
35. Venkata C., Singhal M., Royalty J., and Varanasi S. Security inwireless sensor networks. Wireless communications and mobile computing Published online in WileyInder Science. 2006.
36. Khozium M. O. Hello Flood Counter Measure for Wireless Sensor Network. International Journal of Computer Science and Security. 2(3).
37. Hamid A., Rashid M., Hong C. S. Defense against lap-top class attacker inwireless sensor network. The 8th International Conference Advanced Communication Technology. 2006.
38. Thiago H. et al. Malicious Node Detectionin Wireless Sensor Networks. 18th International Parallel and Distributed Processing Symposium. IEEE. 2004.
39. Singh J., Gupta S. and Kaur L. A MAC Layer Based Defense Architecturefor Reduction-of-Quality (RoQ) Attacks in Wireless LAN. International Journal of Computer Science andInformation Security. 2010; 7(1).
40. Singh J., Gupta S. and Kaur L. A Cross-Layer Based IntrusionDetection Technique for Wireless Networks. The International Arab Journal of Information Technology. 2012; 9(3).
41. Kumar, Alampalayam S., Vealey T., and Srivastava H. Security in internet of things: Challenges, solutions and future directions. System Sciences (HICSS). 2016.
42. Khalil N., Abid M. R., Benhaddou D., Gerndt M. Wireless Sensors Networks for Internet of Things. IEEE Ninth International Conference on Intelligent Sensors, SensorNetworks and Information Processing (ISSNIP) Symposium on Public IoT. 2014.
43. Zorzi M., Gluhak A., Lange S., Bassi A. From Today's Intranet of Things to a Future Internet of Things: A Wirelessand Mobility-Related View. IEEE Wireless Communication. 2010; 43–51.