Securing Cluster Head Selection in Wireless Sensor Networks

Rupinder Singh[1], Dr. Jatinder Singh[2] and Rupinder Singh[3]

[1] Khalsa College, Amritsar

Received: 9 December 2015 Accepted: 1 January 2016 Published: 15 January 2016

Abstract

Wireless Sensor network routing protocols are prone to various attacks as these protocols mainly provide the function of routing data towards the sink. LEACH is a one of the routing protocol used for clustered implementation of wireless sensor network with Received Signal Strength based dynamic selection of Cluster Heads. But, as with other routing protocols, LEACH is also prone to HELLO flood attack when the malicious sensor node becomes the Cluster Head. Cryptographic and non-cryptographic approaches to detect the presence of HELLO flood attack also exist but they lack efficiency in some way. In this paper, an efficient protocol is proposed for the detection and prevention of HELLO Flood attack in wireless sensor network. Cluster heads are vulnerable to various malicious attacks and this greatly affects the performance of the wireless sensor network. Cryptographic approaches to prevent this attack are not so helpful though some non-cryptographic methods to detect the HELLO Flood attack also exist but they are not too efficient as they result in large test packet overhead. In this paper, we propose HRSRP (Hello flood attack Resistant Secure Routing Protocol) extension to LEACH protocol so as to protect the cluster head against Hello flood attack. HRSRP is base on encryption using Armstrong number and decryption using AES algorithm to verify the identity of cluster head. The proposed technique is implemented in NS2, the experimental results clearly indicate the proposed technique has significant capability for the detection of hello flood attack launched for making the malicious node as the cluster head.

Index terms— wireless sensor networks, leach, hello flood attack, armstrong number, aes, encryption, decryption, cluster head.

1 I. Introduction

ireless Sensor Network (WSN) is an infrastructure-less and self-configured wireless networks which is used to monitor physical conditions or environment such as sound, humidity, temperature, pressure, speed, pollutant levels etc. and so on. Sensors in WSN pass the data gathered to Base Station (BS) so that it can be further analyzed for further processing to take different decisions. Figure 1 shows the structure of a typical WSN. Sensor nodes in a WSN are very resource constrained and are susceptible to various attacks due to limited capacity of data processing, speed, storage, communication bandwidth etc. The complication of the implemented security algorithms also adds to the trouble of providing security to WSNs.The past proposed security techniques for WS Ns assumed that almost all sensor nodes are reliable and helpful, but the same is not true for most of the cases for many sensor network applications today. A large number of attacks are possible in WSN including jamming, tampering, exhausting, hello flood, collision, sinkhole, Sybil, denial-of-service, flooding, cloning etc.

Hello flood attack is a network layer attack in WSN caused when hello packets used for neighbour discovery are sent or replayed by an attacker with high transmission power. In this way, the attacker creates an illusion of being a neighbour to other sensor nodes so that the underlying routing protocol can be disrupted, which smooth the progress of launching further types of attacks. The attacker broadcast packets with such a high transmission power that a large number of sensor nodes in the WSN choose it as the parent node or cluster head (CH) in case of clustered implementation. All messages to be broadcasted in the WSN are routed through this parent sensor node that increases delay. The attacker broadcast these hello messages to a large number of sensor nodes in a wide area of the WSN. These sensor nodes are then forced to be convinced that the attacker node in the network is their neighbour. All the sensor nodes are going to reply to this HELLO message from the attacker and are going to waste their energy. This usually results in a confusion state in the WSN.

Heinzelman et al. [2] introduced a dynamic hierarchical clustering protocol called LEACH (Low Energy Adaptive LEACH divides the WSN into small clusters of which one is the CH head and others sensor nodes are the cluster members. The cluster sensor node members send their gathered data to the CH, which in turn send it to the BS W by aggregating all the received data from its cluster members so as to reduce the redundancy. In LEACH the CH sensor nodes are periodically re-elected so that the same sensor node is not repeatedly used for the high energy job of the CH. LEACH operations are divided into two phases of Setup phase and Steady phase. In the setup phase, the formation of clusters with CH and cluster members is done for the WSN while in the steady phase; data are sensed and sent to the BS. The steady phase is longer than the setup phase and is done in order to minimize the overhead cost.

LEACH protocol is a more secure protocol as compared to the conventional multi-hop protocols as in conventional multi-hop protocols, the sensor nodes around the BS are more attractive to compromise as they are the major points of aggregation and forwarders of all packets to the BS. While in LEACH protocol, the CH are the only node that directly communicate with the BS and the location of these CH can be anywhere in the WSN irrespective of the BS. More over these CHs are regularly randomly changed. Therefore, spotting these CHs is very hard for the adversary in WSN. However, as LEACH is a cluster-based protocol, depending exclusively on the CHs for aggregation of data and its routing, attacks on the CH are the most harmful. If any adversary node becomes a CH, then it can make possible attacks like HELLO flood attack, Sybil attack, selective forwarding etc.

Hello packets in WSN are used for neighbour discovery but they can be used by a malicious node with high transmission power to launch Hello flood attack on CHs in WSN. A number of countermeasures against Hello flood attack in WSN have been proposed in the literature that we discussed in our previous work [1]. Most of the proposed countermeasures have limitation and need improvement for producing more efficient one. In this paper, we propose a HRSRP (Hello flood attack Resistant Secure Routing Protocol), an extension to LEACH protocol and is base on encryption using Armstrong number and decryption using AES algorithm to verify the identity of the CH so as to prevent the WSN from Hello flood attack. The remaining paper is organised as follows: In section II, we discuss related works; the section III describes the working of HRSRP. In section IV, we provide the simulation of proposed protocol in NS2 while we end with the conclusion in section V.

2 II. Related Works

In this section of the paper, we discuss the work proposed in the past for providing secure formation of clusters by LEACH protocol in WSN, and the proposed work for selecting CHs in a secure way.

Heinzelman et al. [2] proposed LEACH in which every sensor has a probability of becoming a CH without message exchange. This technique attempted to extend the network life time by making all sensor nodes play a role of CH. In LEACH, some sensor nodes with a high chance declare themselves as CHs and other sensor nodes join in one of them. Since, this method assumes no compromised sensor nodes in the WSN; it has no method to protect the cluster formation from the malicious sensor nodes. F-LEACH [3] was proposed in order to defend the cluster formation in LEACH protocol. In this proposal, when a sensor node declares itself as a CH, it employs the use of common keys shared with the BS so as to check the authentication of the CH declaration to the BS. Then, the sink securely broadcasts the authenticated CHs using ?TESLA [4]. Normal sensor nodes in WSN join in only one legitimate CH. However, this method has no means to validate the normal sensor nodes which join in any cluster. To resolve this problem, Oliveira et al. [5] proposed SecLEACH in which the BS authenticates the CH nodes and further the CHs authenticate the joining sensor nodes. In both F-LEACH and SecLEACH, sensors nodes are pre-assigned some keys for verification before their deployment. However, both F-LEACH and SecLEACH can help in preventing only external attackers from joining of the process of cluster formation i.e. they cannot avoid internal attacks from capturing CHs.

Many extensions to LEACH [7][8][9][10][11] have been proposed in the past but, most of them focus on balancing the consumption of energy over all sensor nodes and extending the lifetime of the network. A few of them [8] deals with electing a CH securely. However, this technique cannot prevent a malicious node from declaring itself as a CH as it can defraud other nodes that it has a short distance to the BS along with a large amount of residual energy. Liu proposed a cluster formation method in which only pre-determined nodes can declare themselves as CHs while other nodes can join any cluster either directly or via a relay node [13]. As any CH declaration or cluster join is authenticated by some pre-assigned polynomial share, the method avoids any external attacker from participating in the process of cluster formation. In this method, a compromised relay node can invoke a Denial of Service (DoS) attack by removing the connection between CH and its serving nodes. Pre-determined CHs become the targets of attackers because their roles are fixed. Sun et al. [14] proposed a protected scheme for cluster formation which checks the protocol conformity of nodes in order to discriminate mean nodes from usual nodes. In this method, physical network is transformed into cliques and members are openly connected to each other in a clique. After the formation of clique, each node checks that all members have the similar view of the clique membership. Even though the method of [19] has enhanced the safety of [14], it supposed that no collisions are possible during the cluster formation. This assumption is difficult to satisfy without the use of any special measure such as TDMA schedule assignment and code separation. Nishimura et al. [21] proposed a method where all nodes allocate a trust value to each candidate of CH and the most trusted nodes are allowed to become CH. Otherwise, the nodes join a close cluster to form clusters in the network. The drawback of this scheme is that it produces a lot of communication overhead for the building of trust evaluation system. So, this method is not appropriate for resource-constrained WSNs.

Rifà-Pous et al. [20] proposed a protected cluster formation method that is based on public key cryptography. The scheme is composed of three phases; cluster discovery phase, CH designation phase, and cluster maintenance phase. In the phase of cluster discovery, all nodes in a cluster have the same view on the membership of cluster with each other. In the phase of cluster designation, a CH is elected considering the number times it performed the CH and number of its neighbours. In the phase of cluster maintenance, the elected CHs provide an authorization certificate to every member in the cluster. But, this method assumes that no nodes depart from the cluster discovery protocol. For example, if a malicious node transmits its message to part nodes in the phase of cluster discovery, the sufferers have a dissimilar view on the membership of cluster. Consequently, it divides a cluster into multiple clusters, and the divided clusters elect their CH respectively in the phase of CH designation. That is to say, this method can produce a lot of clusters under the selective transmission attack. Crosby et al. [21] proposed a trust based CH election design where every node provides a trust value to other nodes according to their behaviour and extremely trustworthy nodes become CHs. Every node's behaviour is calculated by counting the occurrence of successful node transmissions and the occurrence of unsuccessful node transmissions. That is, the more a node succeeds in its transmission, the superior reputation value the node has. During the election of new CH, nodes with a more reputation value are suggested for the role of CH by cluster members and one of these is selected as a new CH. A malicious CH can put in a not guilty victim into a blacklist to take away its candidacy for CH in the cluster that is, with the number of blameless victims rises up, a malicious node can enlarge its winning chance.

Buttyan et al. [22] also proposed a CH selection method which conceals the process of election from outside nodes using cryptographic techniques. However, the concealment works only for external attackers as a compromised node can with no trouble expose the selection result. Moreover, the malicious node can announce itself as a CH even though it is not eligible. Sirivianos et al. [24] proposed the Secure Aggregator Node Election (SANE) protocol in which all eligible CH members in a cluster contribute to the production of a random value and a CH is elected randomly using this random value. SANE is classified into further three sub-schemes according to generating and distributing the random value. They are based on Merkle's puzzle scheme, commitment based scheme, and seed based scheme. Dong et al. ??25] proposed a method that prevents outside attackers from taking part in a CH election process through its ID assignment scheme, which firmly binds a node's ID, its commitments, and its polynomial shares. In this scheme, the nodes that do not broadcast participation message for CH election or explicitly transmit a nonparticipation message are excluded from the CH candidates. The final CH is selected by arbitrarily selecting one node amongst the rest of the candidates. However, an inside attacker can change CH election result by avoiding the distribution of its participation message; it can also generate numerous CH election results by the process of distributing its contribution message only to a subset of CH candidates. Even though this method has a recovery system to combine numerous election results into one result, it requires the voluntary co-operation of the CH candidates.

3 III. Framework and Working of HRSRP

In this section of the paper, we describe our proposed HRSRP for the detection and isolation of Hello flood attack in WSN. We first discuss the WSN model and assumption and then we describe the working of proposed protocol.

4 a) Network Model

The clustered sensor network selected in the paper consists of N static sensor nodes, including CH, member nodes, and BS. CHs are responsible for collecting the information within their clusters and passing it to the BS so as to make decisions and judgments. The formation of clusters is based on LEACH protocol. Every sensor node has a unique identity (ID). Following assumptions of the WSN are used in the proposed protocol HRSRP.

1. Hello flooding attack node, formed by the compromise of CH. 2. The compromised node has a high transmission power. 3. Except the malicious sensor node, all the nodes in wireless sensor network are isomorphic with the same initial energy, transmission power, computing power and internal storage structure. 4. Once each node's ID is allocated, it cannot be changed. 5. Each sensor node is allocated unique Armstrong number. 6. The sensor nodes of the network consume the same energy in the same stage of the work, e.g. the transmission and reception of data packets in the process of detection.

5 b) Implementation of HRSRP

The HRSRP is an improved secure extension to the LEACH protocol, so the implementation of the Year 2016 ( ) proposed protocol has to take advantage of the characteristic of LEACH clustering. LEACH protocol is mainly divided into two phases of set-up phase and stable phase. In the set-up phase, all the sensor nodes have to follow the two guidelines of fairness criterion and randomness criterion. In fairness criteria all sensor nodes in the network have same probability to become a CH. While in randomness criterion, the election of the CH is done in a random way. The chance for a sensor node to become a CH in the round entirely depends on whether the sensor node has ever been elected as CH in the recent rounds and the percentage of the CH sensor in the WSN. When the election of the CH is over, every member node chooses the cluster to join on the basis of the maximum received signal strength until all the clusters are completed. In general, the implementation of LEACH has a longer stabilization phase.

Each member sensor node is responsible for sensing the surrounding environment and forwarding the data to their respective CHs. After collecting information from cluster member nodes, each CH forwards it to the BS. It is vulnerable for LEACH against Hello flood attack due to these characteristics of clustering. Hello flood attack is a common routing attack in the network, which broadcasts a large number of hello message with higher transmission power to nodes in the network. Any sensor node that receives the hello message with high signal will consider the malicious node as CH. This malicious node may damage the network by selectively modifying, discarding information received from its neighbours.

6 c) Determination of malicious CH

The BS maintains record of CHs, cluster members, malicious nodes in the registration table as different sets. The values are updated as per the changes in the clusters and CHs. The initial values of these sets are Set CH node = {null}, the CHs in the network. Set CH member = {null}, the members of each cluster in the network. Set CH malicious = {null}, which means the malicious nodes in the network.

Each sensor node with a certain probability (p) try for becoming CH based on the criterion of randomness and fairness. The sensor node that becomes a CH broadcasts the message of selfclustering in order to attract neighbouring sensor nodes so as to join it. The cluster head CH(i) is selected according to the level of the Received Signal Strength (RSS) to join in a certain range of area. The members of the cluster as calculated by each CH are added to the set CH member .

i

7 . Allocation of unique ID

The BS allocates a unique ID to each sensor in the network. Whenever any sensor node request for becoming CH, it has to send this ID to the BS so that the node identification can be validated.

ii

8 . Allocation of unique Armstrong number

The BS also allocates a unique Armstrong number against each ID for each of the sensor node in the network. An Armstrong number is an m-digit base n number such that the sum of its (base n) digits raised to the power m is the number itself. For example number 371 is an Armstrong number as 3 3 +7 3 +1 3 =27 + 343 +1 = 371 which is equals to number itself. Whenever any sensor node request for becoming CH, it has to send encrypted hello message with this Armstrong number. Table 1 shows example registration table maintained at BS. The flowchart in figure **??** describes the working of HRSRP for authentication of CH by the BS.

As LEACH is fragile to hello flooding attacks because of its characteristics and nature. The compromised non-cluster head sensor nodes have less effect on the performance of network with limit range. But, once it becomes a CH with higher transmission power, a large number of sensor nodes will be appealed for becoming one of its members in a cluster. If the malicious node discards or alters the packets, the circumstances would seriously smash the honesty and precision of the information in the network. The HRSRP can detect the presence of malicious node with fewer energy and small error rate, which can efficiently get better the network performance.

9 IV. Simulation Results

In this section of the paper, we present the results of the simulation to show the effectiveness of HRSRP. The simulation is carried out in ns2. 35 throughput as this is one of the crucial network parameters. Network throughput refers to the average rate of successfully delivered packets. Throughput is calculated depending on a total number of packets received at the destination in sensor network per unit of time. Throughput is calculated as Throughput = (Total number of packets received at the destination) / (simulation time)

Figure 3 shows the throughput analysis in the case of the sensor network without Hello flood attack, under Hello flood attack, and after implementation of proposed HRSRP. The figure clearly shows that the proposed protocol after the isolation of the Hello flood attack results in the increase of throughput.

10 b) Packet delivery ratio

Packet delivery ratio (PDR) of a network is defined as the ratio of the total received packets at the destination to total packets generated by the source node. PDR is calculated as PDR = (Packets received/packets generated) * 100

Figure ?? shows the PDR analysis in the case of the sensor network without Hello flood attack, under Hello flood attack, and after implementation of HRSRP. The figure clearly shows that the proposed protocol after the isolation of the Hello flood attack results in the increase of PDR. A high value of PDR is an indication that there is less packet loss in the sensor network.

11 c) Delay

The delay is defined as the average time taken by a packet (data) to arrive at the destination. The delay also includes any delay that is caused by the process of route discovery along with queue in data packet transmission. The data packets successfully delivered to the destinations are only counted. It is calculated as: Delay = ? (arrive time -send time) / ? Number of connections

The lesser value of delay is an indicator of the better performance of the protocol. Figure ?? shows the end to end delay in the case of sensor network without Hello flood attack, under Hello flood attack, and after

12 d) Overhead

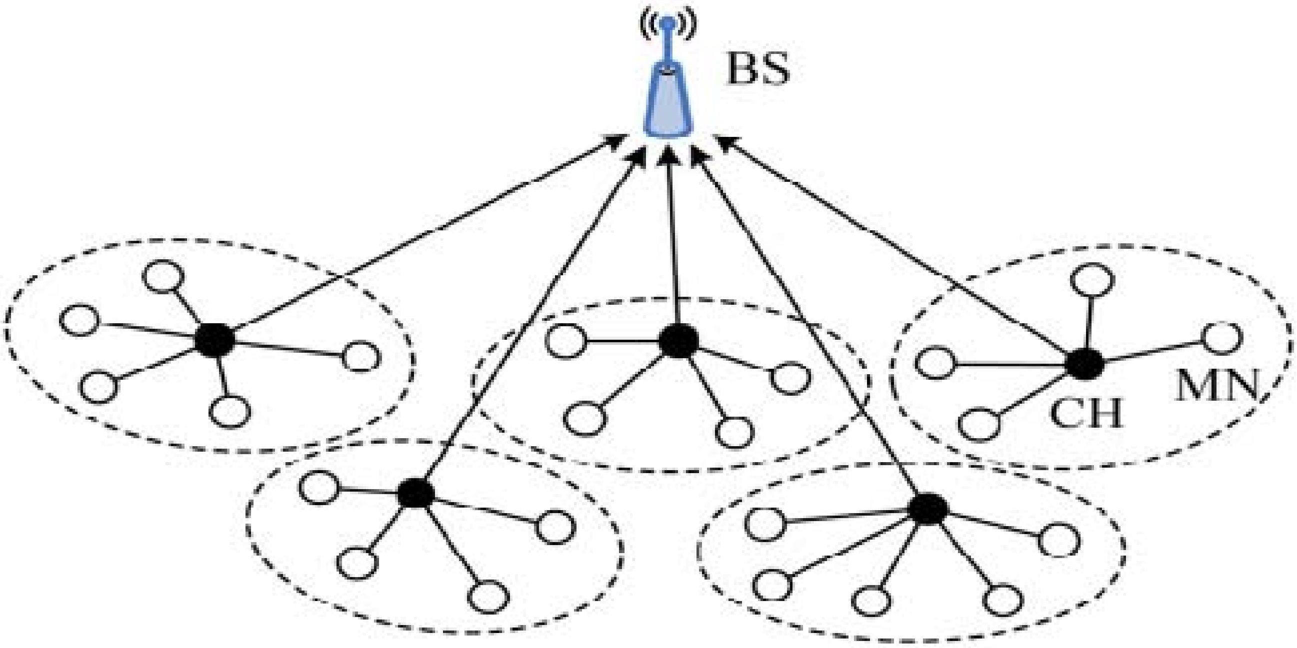
Overhead is the excess time taken by the protocol to deliver the packets to the destination. Hello flood attack increases the overhead in the sensor network. The routing overhead is defined as the count of packets used for routing in the sensor network. Figure ?? shows overhead in the case of sensor network without Hello flood attack, under Hello flood attack, and after implementation of HRSRP. The proposed protocol results in decreasing the overhead of the network as shown in figure ??.

13 V. Conclusion

Cluster head selection in a secure way in clustered implementation of wireless sensor network is vital as all the cluster sensor members data to the base station is communicated through cluster head. Hello flood attack in wireless sensor network can be used for making a cluster head compromised by making use of high transmission power used for sending or replaying hello packets which are used for neighbour discovery. LEACH protocol is hard to attack by adversary excluding the case when it can become cluster head. In this paper, a approach to detect and prevent HELLO Flood attack in LEACH protocol in wireless sensor networks is proposed. We propose a HRSRP (Hello flood attack Resistant Secure Routing Protocol) extension to LEACH protocol base on encryption using Armstrong number and decryption using AES algorithm to verify the identity of cluster head. HRSRP improves the network performance by early discovery of adversary and preventing the sensor nodes from associating with such a malicious cluster head. The implementation of the proposed technique in NS2 shows its efficiency for the factors of throughput, packet delivery ratio, delay, overhead. The simulation results prove that HRSRP expels more compromised nodes from clusters and suppresses the separation of clusters. Other simulation results also represent that HRSRP raises the quality of clusters and more energy efficient than an opponent scheme. Additional simulation will be done in the future by increasing the number of sensor nodes.

14 VI. Acknowledgement

[1]



1

Figure 1: Figure 1 :

1

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

Figure 2: Table 1 :

2

with the

Figure 3: Table 2 :

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab for providing opportunity to conduct this research work.

[Mohammad Sayad Haghighi et al.] , Kamal Mohammad Sayad Haghighi , Vijay Mohamedpour , Barry G Varadharajan .

[Singh et al. (2012)] 'A Cross-Layer Based Intrusion Detection Technique for Wireless Networks'. Jatinder Singh , Dr Savita Gupta , Dr Lakhwinder Kaur . *The International Arab Journal of Information Technology* May 2012. 9 (3) .

[Rifà-Pous and Herrera-Joancomartí ()] 'A Fair and Secure Cluster Formation Process for Ad Hoc Networks'. H Rifà-Pous , J Herrera-Joancomartí . *Wireless Communications* 2011. 56 (3) p. .

[Waldir Ribeiro Pires J´ Unior Thiago et al. ()] 'A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN'. H Waldir Ribeiro Pires J´ Unior Thiago , Chi De Paula Figueiredo Hao , Wong . *18th International Parallel and Distributed Processing Symposium*, Dr Savita Singh, Dr Gupta, Lakhwinder Kaur (ed.) 2010. 7. (Print) (Malicious Node Detection in Wireless Sensor Networks)

[Wang et al. ()] 'A Secure Cluster Formation Scheme in Wireless Sensor Networks'. G Wang , D Kim , G Cho . ID 301750. *Int'l Journal of Distributed Sensor Networks* 2012. 2012 p. 14.

[Dubey et al. (2014)] 'A Survey in Hello Flood Attack in Wireless Sensor Networks'. Akhil Dubey , Deepak Meena , Shaili Gaur . *International Journal of Engineering Research & Technology (IJERT)* 2278- 0181. January 2014. 3 (1) .

[Fatema and Brad (2013)] 'Attacks and counterattacks on wireless sensor networks'. Nusrat Fatema , Remus Brad . *Sensor & Ubiquitous Computing (IJASUC)*, December 2013. 4.

[Steffi et al. (2014)] 'Attacks and countermeasures in WSN'. J Steffi , Agino Priyanka , S Tephillah , A M Balamurugan . *International Journal of Electronics & Communication* 23215984. January 2014. 2 (1) .

[Crosby and Pissinou ()] 'Cluster-based Reputation and Trust for Wireless Sensor Networks'. G V Crosby , N Pissinou . *Proc. of the 4th IEEE Consumer Communications and Networking Conference (CCNC '07)*, (of the 4th IEEE Consumer Communications and Networking Conference (CCNC '07)) 2007. p. .

[Hamid and Rashid ()] 'Defense against lap-top class attacker in wireless sensor network'. A Hamid , Mamun Rashid . *The 8th International Conference Advanced Communication Technology*, 2006. IEEE. p. . (Print ISBN) (Choong Seon Hong)

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

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

[Jyoti and Bansal (2015)] 'Detection of Hello Flood Attack on Leach Protocol Based on Energy of Attacker Node'. Ashu Jyoti , Bansal . *International Journal of Innovations & Advancement in Computer Science* 2347 -8616. September 2015. 4.

[Satwinder Kaur et al. (2014)] 'Detection of Malicious Cluster Head causing Hello Flood Attack in LEACH Protocol in Wireless Sensor Networks'. Satwinder Kaur , Mansi Saini , Gupta . *International Journal of Application or Innovation in Engineering & Management (IJAIEM)* 2319 -4847. May 2014. 3 (5) .

[Kang and Nguyen (2012)] 'Distance Based Thresholds for Cluster Head Selection in Wireless Sensor Networks'. S Kang , T Nguyen . *IEEE Communications Letters* Sep. 2012. 16 (9) p. .

[Kaur and Singh (2015)] 'Energy level based Hello Flood attack Mitigation on WSN'. Dilpreet Kaur , Rupinder-pal Singh . *International Journal of Embedded Systems and Computer Engineering* 23213361. July 2015.

[Heinzelman et al. (2000)] 'Energy-efficient communication protocol for wireless microsensor networks'. W R Heinzelman , A Chandrakasan , H Balakrishnan . *the proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Jan. 2000. 2.

[Anup Wanjari and Dhamdhere (2014)] 'Evading Flooding Attack in MANET Using Node Authentication'. A Anup Wanjari , Vidya Dhamdhere . *International Journal of Science and Research* December 2014. 3 p. .

[Virendra Pal et al. (2010)] 'Hello Flood Attack and its Countermeasures in Wireless Sensor Networks'. Virendra Pal , Sweta Singh , Jyoti Jain , Singhai . *International Journal of Computer Science Issues* 1694-0814. May 2010. 7 (11) .

[Singh et al. (2016)] 'Hello flood attack Countermeasures in Wireless Sensor Networks'. Rupinder Singh , Dr Jatinder Singh , Dr. Ravinder Singh . *International Journal of Computer Science and Mobile Applications* April 2016. 4 (5) p. .

[Devi et al. (2015)] 'Hello Flood Attack Using BAP in Wireless Sensor Network'. Gayatri Devi , Rajeeb Sankar Bal , Nibedita Sahoo . *International Journal of Advanced Engineering Research and Science* 2349-6495. Jan. 2015. 2 (1) .

[Osama (2008)] ‘Hello Flood Counter Measure for Wireless Sensor Network’. Mohamed Osama , Khozium . *International Journal of Computer Science and Security* May 2008. 2 (3) .

[Katiyar et al. (2011)] ‘Improvement in LEACH Protocol for Large-scale Wireless Sensor Networks’. V Katiyar , N Cand , G C Gautam , A Kumar . *Proc. of Int’l Conf. On Emerging Trends in Electrical and Computer Technology*, (of Int’l Conf. On Emerging Trends in Electrical and Computer Technology) Mar. 2011. p. .

[Saadat et al. (2010)] ‘Improving Threshold Assignment for Cluster Head Selection in Hierarchical Wireless Sensor Networks’. M Saadat , R Saadat , G Mirjality . *Proc. of Int’l Symposium on Telecommunications*, (of Int’l Symposium on Telecommunications) Dec. 2010. p. .

[Int’l Conf ()] Int’l Conf . *On Computational Science and Its Applications*, 2010. 6018 p. .

[Rawan and Suhare (2015)] ‘Intrusion Detection of Hello Flood Attack in WSNs Using Location Verification Scheme’. S Rawan , M Suhare , A . *International Journal of Computer and Communication Engineering* May 2015. 4 (3) .

[Sirivianos (2007)] ‘Non-manipulable Aggregator Node Election Protocols for Wireless Sensor Networks’. M Sirivianos . *Proc. of IEEE 6th Annual Comm. Society Conf. on Sensor, Mesh and Ad Hoc Communications and Networks(SECON)*, (of IEEE 6th Annual Comm. Society Conf. on Sensor, Mesh and Ad Hoc Communications and Networks(SECON)Cyprus) Apr. 2007. 2009. p. . (Proc. of Int’l Sympo. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt ’07))

[Ferreira et al. ()] ‘On the security of cluster-based communication protocols for wireless sensor networks’. A C Ferreira , M A Vilaca , L B Oliveira , E Habib , H C Wong , A A Loureiro . *Proc. of 4th IEEE Int’l Conf. on Networking*, (of 4th IEEE Int’l Conf. on NetworkingReunion Island, France) Apr. 17-21, 2005.

[Buttyan and Holczer ()] ‘Private Cluster Head Election in Wireless Sensor Networks’. L Buttyan , T Holczer . *Proc. of the Fifth IEEE Int’l Workshop on Wireless and Sensor Network Security (WSN ’09)*, (of the Fifth IEEE Int’l Workshop on Wireless and Sensor Network Security (WSN ’09)) 2009. IEEE. p. .

[Liu ()] ‘Resilient Cluster Formation for Sensor Networks’. D Liu . *Proc. of 27th Int’l Conf. on Distributed Computing Systems (ICDCS ’07)*, (of 27th Int’l Conf. on Distributed Computing Systems (ICDCS ’07)) 2007. p. .

[Han et al. ()] ‘SecDEACH: Secure and Resilient Dynamic Clustering Protocol Preserving Data Privacy in WSNs’. Y Han , M Park , T Chung . *Proc. of the*, (of the) 2010.

[Oliveira et al. ()] ‘SecLEACH-a random key distribution solution for securing clustered sensor networks’. L B Oliveira , H C Wong , M W Bern , R Dahab , A A Loureiro . *Proc. of 5th IEEE Int’l Symp. on Network Computing and Applications*, (of 5th IEEE Int’l Symp. on Network Computing and ApplicationsCambridge, Massachusetts, USA) Jul. 24-26, 2006.

[Nishimura et al. (2011)] ‘Secure Clustering for Building Certificate Mangement Nodes in Ad-Hoc Networks’. I Nishimura , T Nagase , Y Takehana , Y Yoshioka . *Proc. of 14th Int’l Conf. On Network-Based Information Systems (NBiS)*, (of 14th Int’l Conf. On Network-Based Information Systems (NBiS)Tirana, Albania) Sep. 07-09, 2011.

[Sun ()] ‘Secure Distributed Cluster Formation in Wireless Sensor Networks’. K Sun . *Proc. of 22nd Annual Computer Security Applications Conference (ACSAC’06)*, (of 22nd Annual Computer Security Applications Conference (ACSAC’06)) 2006. p. .

[Mayur and Ranjith (2015)] ‘Security Enhancement on LEACH Protocol From HELLO Flood Attack in WSN Using LDK Scheme’. S Mayur , H D Ranjith . ISSN (Print): 2347 -6710. *International Journal of Innovative Research in Science, Engineering and Technology* (Online): 2319 - 8753. March 2015. 4.

[Venkata et al. ()] ‘Security in wireless sensor networks’. C Venkata , Mukesh Singhal , James Royalty , Srilekha Varanasi . *Wireless communications and mobile computing Published online in Wiley Inder Science*, 2006.

[Virendra Pal et al. (2013)] ‘Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks’. Virendra Pal , S Singh , Anand Aishwarya , Sweta Ukey , Jain . *International Journal of Computer Applications* January 2013. 62 (15) .

[Perrig (2002)] ‘SPINS: Security Protocols for Sensor Networks’. A Perrig . *Wireless Networks* Sep. 2002. 8 (5) p. .

[Quinn (2011)] ‘Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks’. Quinn . *IEEE transactions on information forensics and security*, December 2011. 6.

[Ren et al. (2010)] ‘Unequal Clustering Scheme based LEACH for Wireless Sensor Networks’. P Ren , J Qian , L Li , Z Zhao , X Li . *Proc. of Fourth Int’l Conf. on Genetic and Evolutionary Computing*, (of Fourth Int’l Conf. on Genetic and Evolutionary Computing) Dec. 2010. p. .