DOI : 10.15613/sijrs/2016/v3i1/146545
*ISSN (Print): 2349–8919*
*ISSN (Online): 2350–0999*

**SciеXplore: International Journal of Research in Science,** *Vol 3(1), 30–35, January-June-2016*

# Design and Implementation of Modified Low Energy Adaptive Clustering Hierarchy to Prevent Flooding Attacks in Cloud Environment

**Manoharan Subramanian[1]* and Anoor Sindhu[2]**

[1]Head and Associate Professor, Department of Computer Science (P. G), Kongu Arts and Science College (Autonomous), Erode – 638107, Tamil Nadu, India; manomathi@yahoo.com
[2]Mphil, Research Scholar, Department of Computer Science (P. G), Kongu Arts and Science College (Autonomous), Erode – 638107, Tamil Nadu, India; anoorsindhu@gmail.com

## Abstract

Flooding attacks play a vital role in network. Most of the people are working on the cloud computing environment either as a provider or as a consumer. The flooding attack is a challenge to the resources of network and bandwidth of the host for web page. Nowadays, web based applications are developed in the cloud computing environment. The FAPA (Flooding Attack Prevention Architecture) is used to prevent flooding attacks in cloud based computing environment. The LEACH protocol helps to improve the system lifetime by reducing the energy used to transmit the data to the base station. The aim of this work is to prevent the flooding attacks in cloud and transfer the data in a fast and secured manner using MLEACH (Modified Low Energy Adaptive Clustering Hierarchy).

**Keywords:** Cloud Security, DDoS, MLEACH

## 1. Introduction

In today's IT industry, Cloud computing services use modern web and virtualization technique to energetically supply various kinds of electronically provided services [3]. The Cloud computing platforms are increasing in a fashionable manner. Most of the IT departments are enforced to expend a noteworthy fraction of their time on provoking implementation, maintenance and promote projects that do not add significant value to the company's bottom line growth. Progressively more IT teams are revolving to the cloud computing technology to minimize the time spent on inferior assessment actions [10]. Cloud computing is a technique that delivers the computing power as a service to share resources, software and information and other devices as an utility over a network [9]. Clouds can be classified as public, private or hybrid. The cloud system provides major three layers that are,

- IaaS consists of all the hardware modules of the cloud.
- PaaS contains the running applications on which the customers will obtain their virtual machines, and
- SaaS provides the actual computations requested by the customer.

The different types of flooding attacks are available but generally, they are all involved in a victim of getting, processing and/or sending a huge quantity of packets with reply to the original packets sent by an attacker.

In most cases, "the data deliverance in a sensor network is based on the hypothesis that data from sensor to sink are less tolerant due to the sheer amount of correlated data. Conversely, a sink may capture proper actions based on the information supplied by the sensors; the precision of the condition politeness is enhanced by reducing the data loss. To trim down the data loss, several researchers utilize a mathematical formula for data collection from sensors to sink in the network in a wide manner [1]".

*Author for correspondence

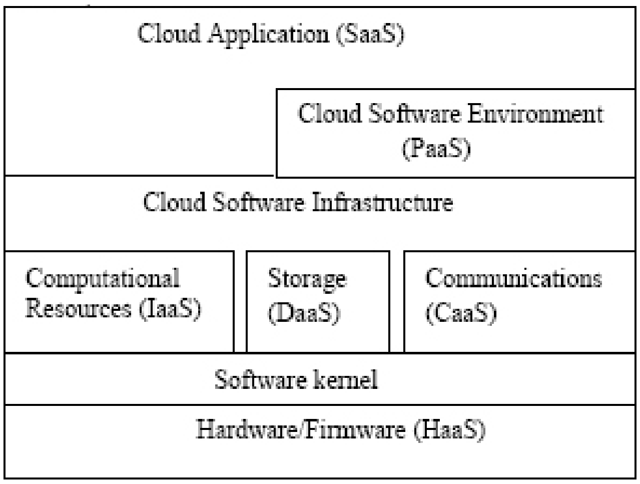


**Figure 1.** Cloud layered model.

### 1.1 FAPA Model

FAPA model is used to avoid illegal intrusion or any kind of flooding attack in the network. The hypervisor is used to study the nature of the traffic packets, ensure its validity and plan the task requested by the packets. The cloud system's hypervisor is the core engine and it is answerable for most of the message passing between different servers. Though there has been much previous works available on preventing DoS attacks, there is still no complete model for preventing DoS attacks in clouds.

### 1.2 Related Work

"A flooding attack is a malevolent browsing behavior which causes resource wastage such as bandwidth, CPU time and memory on the cloud with results in extra and unnecessary cost. Flooding attack on cloud application layer doesn't cause complete denial of service to a Web server. In this paper, semantic concept is used to identify malicious browsing behavior to improve performance and cut down the cost [6]." (Chen-Yu Lee, Ching-Ru Chen, Hsing Lin, Jung-Chun Liu, May 2011).

(Yogesh) proposed "nonetheless of company size or volume and magnitude of the cloud, the tactics of IT virtualization strategy could be used in response to denial of service attack. When there is abnormal point in inbound traffic, the targeted application is immediately transferred to virtual machine hosted in another data center [8]."

(Chu-Hsing Lin, Chen-Yu Lee, Shin-Pin Lai1 and Wei-Shen Lai, April, 2012) "proposed to analyze PHP dynamic pages and developed a method based on semantic concept to formulate rules to identity malicious browsing behaviors in order to slice the cost [4]."

(Luigi Lo Iacono, November 2012) proposed "a novel algorithm which is based on an analytical approach to mitigate DDOS attacks on cloud [7]."

(Susan, 2012) proposed "the characteristics of attacks uses the validation checking. Learning phase and compatibility checking is through its hypervisor to prevent flooding attacks [2]."

## 2. Leach

W. R. Heinzelman [12] "introduced LEACH, a hierarchical protocol in which most nodes transmit the data to the cluster heads. The clusters heads aggregate and compress the data, then forward it to the base station (sink). Leach is mainly designed for sensor networks where an end user wants to remotely monitor the environment. In such a situation, the data from the individual nodes must be sending to a central base station often located far from the sensor network, through which the end user can access the data [11,12]. Consequently, the LEACH protocol assists to maximize the lifetime of the system by minimizing the energy used to transmit data to the base station [13,14]".

A sensible style theme of nodes in MSN is cluster. This may stabilize the configuration periodically and potency at the energetic consumption. Since LEACH is used to rise the network period, however this protocol isn't effective with quality [15,16].

## 3. Proposed Work

### 3.1 M-LEACH

Modified LEACH protocol could be a centralized algorithmic program. As LEACH, an associate algorithmic program operates in cycles by having every tower with two phases namely a setting part and a gentle state part. Within the configuration part, M-LEACH selects a variety of sensors to be known as Cluster Hierarchy (CH). The CH is used to support the nodes with assigned Weight. As a result, its application is restricted to nodes mounted with sensors. In this work, the M-LEACH is localized and outperforms LEACH in terms of atmosphere, field of use in underground and quality to extended Networks period. M-LEACH works with neighboring nodes to reorganize the node density. It selects active nodes that remain asleep during the transmission of data.

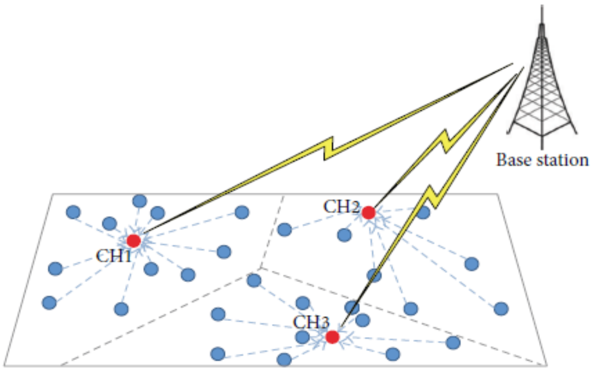


**Figure 2.** Data Transfer Cluster Head

Weighted LEACH: it is an associate extended LEACH to challenge the uniform and non-uniform networks. In set up phase, the bottom station supported density of nodes to divide member nodes in 2 teams. One cluster member nodes transmit their knowledge whereas the member nodes in the different cluster stay asleep. The choice of nodes which stay asleep is centralized.

$$w_i = \begin{cases} e_i * d_{i,} & \textbf{if } \mathbf{d_i > d_{thresh,}} \\ d_{i,} & \textbf{otherwise,} \end{cases} \qquad (1)$$

Equation (1) shows Modified Low Energy Accommodative Hierarchy (M-LEACH) which is an associate extension of LEACH with efficiency to handle non-uniform device distribution in MSNs. It will increase the period of time in the networks. Whomever, this protocol is centralized as a result of the bottom station and it is solely liable for choosing sleeping nodes and active nodes.

## 3.2 M-LEACH Localized Algorithmic Program

In M-LEACH localized, the choice of CHs are as in LEACH. Every device node N (i) elects itself to be cluster head with likelihood as conferred in Equation (1). In the following, we assume that node N2 is electoral CH and N1, N2 don't seem to be cluster head. Therefore, N2 spreading ADVCH tell its neighbors that it becomes a CH. Then N1, N3 aggregates the ADVCH messages from CHs and select its nearest CH. Then it transmits a be a part of REQ message to its CH and received be a part of REQ message from different Member nodes to see their neighbors' nodes and also the distance similar to each neighbor.

The CH in its flip, receives the part of REQ (Request) message to create its cluster and build Time Division Multiple Access (TDMA) Schedule. Then it spreads ADVCH (Advanced Cluster Hierarchy) message to tell their member nodes once will transmits their knowledge. Member nodes when receiving ADVCH, they calculate the amount of nearest neighbors to a lower most distance determined. If this number is a smaller amount than a restricted range the node goes to sleep throughout this spherical as N3. Else the nodes calculate their interval to transmit their knowledge as N1.

The Figure 3 describes the architectural process of M-Leach which makes the transaction of data from source to sink; using three neighbors send the data to the desired sink node. The LEACH-C also organizes the sensor nodes into clusters but it varies from LEACH by using a high-energy base station.

Every sensor node in each cluster sends its information about energy to remote Base Station during the set-up phase of each round. The transmission energy of transmitting a k-bit message and the power consumption of transferring one bit of data are calculated by the formula stated below:

$$E_{trans}(k,d) = \begin{cases} KE_{elec} + k\varepsilon_{fs}d^2\ (d < d_0), \\ KE_{elec} + k\varepsilon_{mp}d^4 (d \geq d_0.) \end{cases} \qquad (2)$$

Although LEACH and LEACH-C protocols are working efficiently, they are also suffered from some drawbacks like (i) Random selection of Cluster Heads, (ii) The high frequency of clusters wastes a certain amount of energy during the process of transmission. (iii) Limited area of transmission. (iv) Non uniform distribution of Cluster Heads, (i.e.) located at the edge of the each cluster.

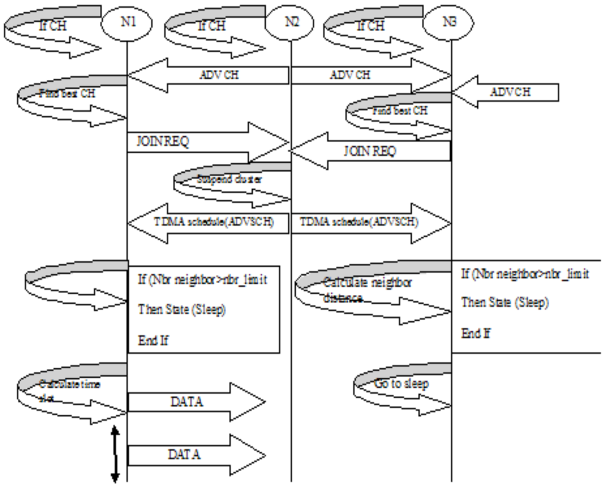


**Figure 3.** Architecture process of M-LEACH.

$$T(n) - \begin{cases} \dfrac{p}{1 - p * \left[ r \bmod \left( \dfrac{1}{p} \right) \right]} \\ \times \left[ \dfrac{E_n - current}{E_{n_{init}}} \right] + \left( 1 - \dfrac{E_n - current}{E_{n_{init}}} \right) \\ \times \dfrac{p}{CH_{times} + VCH_{times} + 1} & n \in G, \\ 0, & n \in G \end{cases} \tag{3}$$

The threshold value of each cluster "the percentage of cluster heads in the overall nodes of the network and the number of rounds selection has been done in the current time" is computed in Equation (3). The CH_times and VCH_times are the time estimates for computing the transmission of each node in the respective cluster heads. By deducing from Equation (3), it can obtain only smaller value of energy consumption, which indicates that the node which has less energy will have a smaller probability to become the cluster head in the current round. "*Nmem*1 and *Nmem*2 are the number of members in clusters H1 and H2, *dh*1*toBs* and *dh*2*toBs* are the distance between the two cluster heads and node Sink". Therefore, the total energy consumed by the two clusters is

$$E_{h1} + E_{h2} = L\,E_{bit}(N_{mem1} + N_{mem2}) + LE(N_{mem1} + N_{mem2} + 2) + 2LE_{bit} + Lm(d_{h1\text{ to }Bs} + d_{h2\text{ to }Bs}) \tag{4}$$

Then Equation (4) becomes

$$E_{h1} + E_{h2} = (N_{mem1} + N_{mem2}) + LE(N_{mem1}) + LE\,(N_{mem1} + N_{mem2} + 2) + 2LE_{bit} + 2Lm\,d_{h1\text{ to }Bs} \tag{5}$$

In this case, the total energy consumption of two clusters is only *LE*R*bit*R+*Lmd*R*h*1*tobs* R which are greater than the case that there is only one cluster head. In addition, because *LE*R*bit*R+*Lmd*R*h*1*tobs*R is much greater, therefore, the total energy consumption when there are two cluster heads is approximately twice.

**Nearest Neighbor clustering Algorithm:**

*"A set of patterns L= {$x_1$, $x_2$, … … … $x_n$} is to be partitioned into k cluster. The user specifies a threshold, t on the nearest neighbor distance.*

*Step 1: Set the value as I ← 1 and k ← 1.*
*Step 2: Assign the pattern X1 to C1.*
*Step 3: Set I ← i+1. Find the nearest neighbor of $x_i$ among the patterns already assigned to cluster. Let dm denote the distance from $x_i$ to its nearest neighbor. Suppose that the nearest neighbor is in cluster m.*
*Step 4: If dm ≤ t, then assign $x_i$ to $C_m$. Otherwise, Set k ← k+1 and assign $x_i$ to a new cluster $C_k$.*
*Step 5: If every pattern has been assigned to a cluster then stop. Else go to step 2.*

In this algorithm, C represents the number of cluster generated; k is a function of the parameter (t). When the value of t increases, fewer clusters are generated with respect to the function k. Step 2 describes the average distance between $x_i$ and its p nearest neighbor in the $m^{th}$ cluster."

## 4. Experimental Result and Discussion

The M-LEACH is implemented in cloud environment to secure data transfer and traffic, both sender and receiver send the subject (like key) to send or receive a data. When the subject is correct the data will be received otherwise it will not be received. While the attackers hack any messages, or any week node, the result will be shown in data transfer node. The result is checked using three neighbors to send the data to sink.

Figure 4 and Figure 5 describe the accuracy and time comparision between the existing LEACH and proposed M-LEACH. While comparing with the existing model, the proposed M-LEACH avoids the traffic and saves the time and accuracy, also increassed during the transaction. Figure 6 describes the subject of the message requested and Figure 7 sending a subject to source for sending a data (message). Source is waiting for the subject to receive a data from client.

Figure 8 represents the request that are received by the sink (subject with message) after source sends the data to desired sink. Figure 9 describes the transaction of data

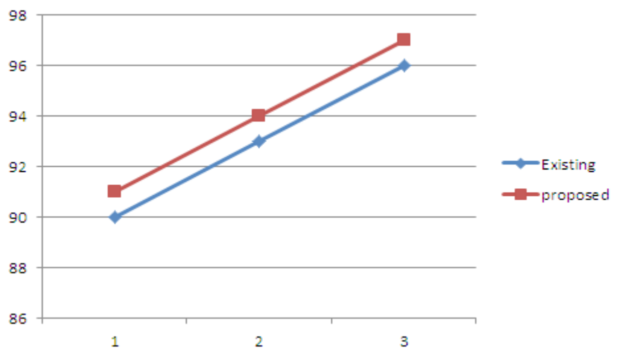


**Figure 4.** Accuracy comparision.

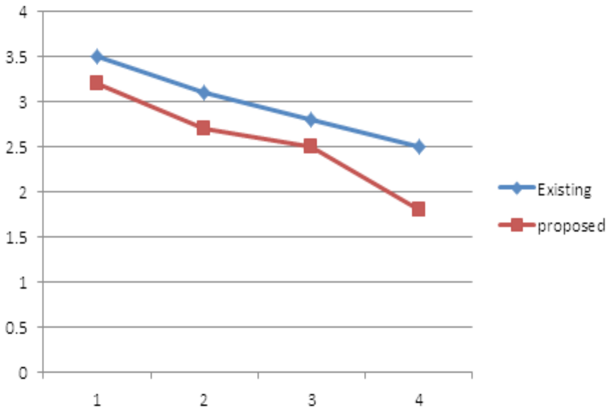
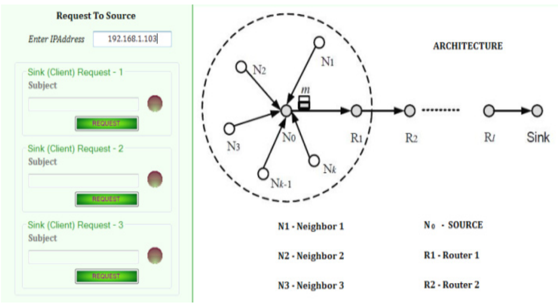


**Figure 5.** Time comparision.


Request To Source

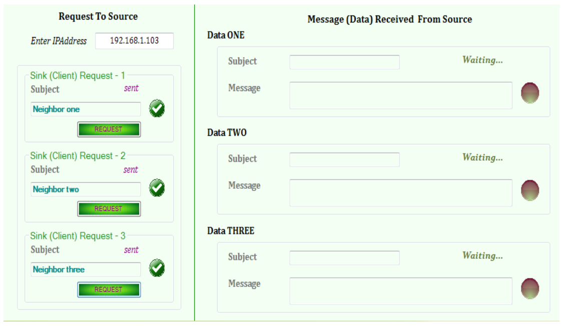
Enter IPAddress 192.168.1.103

Sink (Client) Request - 1
Subject
REQUEST

Sink (Client) Request - 2
Subject
REQUEST

Sink (Client) Request - 3
Subject
REQUEST

**Figure 6.** Request to source.


Request To Source

Enter IPAddress 192.168.1.103

Sink (Client) Request - 1
Subject sent
Neighbor one
REQUEST

Sink (Client) Request - 2
Subject sent
Neighbor two
REQUEST

Sink (Client) Request - 3
Subject sent
Neighbor three
REQUEST

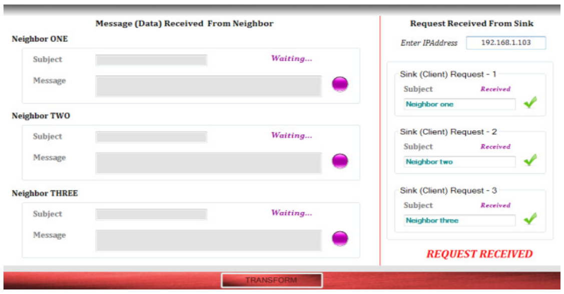
Message (Data) Received From Source

Data ONE
Subject Waiting...
Message

Data TWO
Subject Waiting...
Message

Data THREE
Subject Waiting...
Message

**Figure 7.** Checking subject (key).


Message (Data) Received From Neighbor

Neighbor ONE
Subject Waiting...
Message

Neighbor TWO
Subject Waiting...
Message

Neighbor THREE
Subject Waiting...
Message

Request Received From Sink

Enter IPAddress 192.168.1.103

Sink (Client) Request - 1
Subject Received
Neighbor one

Sink (Client) Request - 2
Subject Received
Neighbor two

Sink (Client) Request - 3
Subject Received
Neighbor three

REQUEST RECEIVED

TRANSFORM

**Figure 8.** Request received by sink.

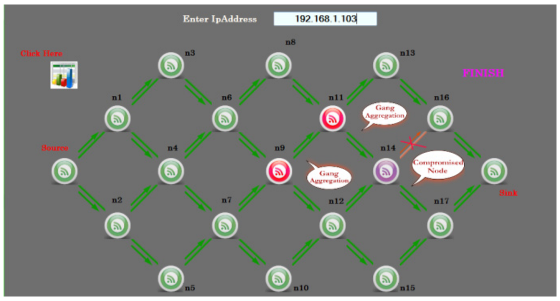

Enter IpAddress 192.168.1.103

**Figure 9.** Sending process (message).

between the nodes by showing the hackers in the respective nodes with different color. If there is any week node, it is also displayed in different color.

## 5. Conclusion

Wireless sensor network applications are progressively being used in the health care system, transportation, manufacturing and more. M-LEACH protocol improved the accuracy and the time to send the data in cloud environment. The FAPA and LEACH protocol models are used to prevent flooding attack in the cloud environment. MLEACH protocol model reduces the traffic and secure the data transmission. The Distance-Based DDoS technique applied here uses a simple but effective exponential smoothing technique to predict the mean value of distance in the next time period based on the selection of threshold values. A distributive approach to identify and prevent the flooding attack has also been proposed.

## 6. References

1. Lim Y, Kang S. Intelligent approach for data collection in wireless sensor networks. The International Arab Journal of Information Technology. 2013 Jan; 10(1).
2. Zunnurhain K, Susan. FAPA: A model to prevent flooding attacks in clouds. Proceedings of the 50th Annual Southeast Regional Conference; 2012. p. 1–8.
3. Katkamwar NS, Puranik AG, Deshpande P. Securing Cloud Servers against Flooding Based DDoS Attacks. International Journal of Application or Innovation in Engineering and Management. 2012 Nov; 1(3):1–6.
4. Lin C-H, Lee C-Y, Lai S-P, Lai W-S. A semantic rule-based detection scheme against flooding attacks on cloud environment. International Journal of Security and its Applications. 2012 Apr; 6(2):1–3.

5. Shah JJ. Impact of DDOS attacks on cloud environment. International Journal of Research in Computer and Communication Technology. 2013 Jul; 2(7):1–4.
6. Lee C-Y, Chen C-R, Lin H, Liu J-C. A detection scheme for flooding attack on application layer based on semantic concept. IEEE Trans on Software Eng. 2011 May; 24(5):376–90.
7. Lacono LL, Gruschka N. SOAP message security validation revisited. IEEE Trans on Cloud Computing. 2012 Nov; 26:276–90.
8. Bakshi A, Yogesh B. Securing cloud from DDOS attacks using intrusion detection system in virtual machine. 2nd International Conference on, Communication Software and Networks ICCSN ‘10; 2010 Feb 26-28. p. 260–4.
9. Santhi K. A defense mechanism to protect cloud comuputing against distributed denial of service attacks. International Journal of Advanced Research in Computer Science and Software Engineering. 2013 May; 3(5):2–5.
10. Katkamwar NS, Puranik AG, Deshpande P. Securing cloud servers against flooding based DDoS Attacks. IJAIEM. 2012 Nov; 1(3):1–4.
11. Shang F, Abolhasan M, Wysocki T. An energy-efficient adaptive clustering algorithm for wireless sensor networks. International Journal of Information Acquisition. 2009; 6(2):117–26.
12. Heinzelman W, Chandrakasan A, Balakrishnan H, Energy efficient communication protocol for wireless sensor networks. Proceeding of the Hawaii International Conference System Sciences; Hawaii. 2000 Jan. p1–6.
13. Bakaraniya P, Mehta S. K-LEACH: An improved LEACH protocol for lifetime improvement in WSN. IJETT. 2013 May; 4(5).
14. Sharma K, Ghose MK. Wireless sensor networks: An overview on its security threats. IJCA Special Issue on MANETs. 2010; 1.
15. Kumar SV, Pal A. Assisted-Leach (A-Leach) energy efficient routing protocol for wireless sensor networks. International Journal of Computer and Communication Engineering. 2013 Jul; 2(4).
16. Liao Q, Zhu H. An energy balanced clustering algorithm based on LEACH protocol. Proceedings of the 2nd International Conference on System Engineering and Modeling (ICSEM-13); 2013.