International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Clone Detection on Large Scale Social Networks Including Wireless Sensor Network

Sumandip Kaur*, Meenakshi Sharma
Computer Science Department, G.I.M.E.T, Amritsar, Punjab, India

ABSTRACT

Wireless sensor networks are low-cost, low-power and small sensor devices to collect information through networks. The stunning development of the internet use for all sorts of organizations has created in the meantime an expansion of Clone lent exercises, which calls for growing new strategies, devices for distinguishing Clone and different violations against reserve clients. Clone discovery needs to break down and interface data, which are assembled from heterogeneous data storehouses to address critical thinking calculations streamlining, parallelization, new learning representation of ideal models, affiliation instruments for connecting data, and diagram investigation for clustering and parceling. Authors show the inspiration of investigation and the initial steps of the work. Study will center on the development of new coding models in view of Clone attacks and WSN expansions.

Keywords: Large scale graphs analysis; graph partition and clustering; parallel processing, clone attacks, Clone detection, and security.

I. INTRODUCTION

The incredible growth of the internet use for all sort of applications such as data production and storage, business transactions, professional, cultural and personal information management, etc. are pushing back the frontiers of traditional computer and digital data management. [1,2] forgery and clone is common not only within the wireless sensor network but also in digital images as predicted in the existing. This overwhelming activity allows all kinds of players to propose new services and offers. Unfortunately, some did not hesitate to take advantage of this space to be engaged in Clone lent activities, such as Identity Theft Clone. The goal of this investigation is to take a shot at another approach to address large scale informal organization Clone detection by joining real time processing and bunch processing in information distribution center and Hadoop Disseminated Document Framework (HDFS)[3] Clone is frequently described by unpredictable convergence of exercises on subsets of hubs in sub networks of the web, especially on online informal organizations (OSN). This calls for Connecting information, which were not prone to be connected, in light of the fact that they try not to have a place with similar systems.[4,5] Connecting informal organizations information, spread upon various heterogeneous information stores, calls for tending to a few testing issues, for example, calculations enhancement and parallelization, new information portrayal ideal models for heterogeneous, excess, noncertified or then again false data, affiliation instruments, graph analysis for clustering and partitioning. [6]

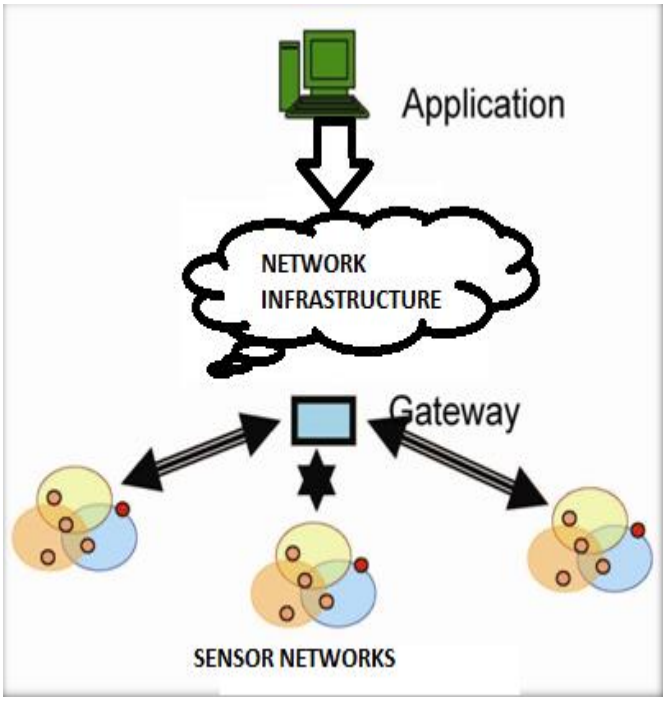

Figure 1. wireless sensor network architecture.

To address this multi-dimensional issue, following methodologies have been accompanied:

i. Distinguish group sub networks by utilizing group detection calculations running in a parallel condition,
ii. Speak to information and learning put away in these systems in a typical learning plan
iii. Apply Iterative calculations for clustering and partitioning.

The paper is sorted out as takes after. Authors show in the second area, a portion of the fundamental qualities of OSN information, extraordinarily on account of Clone lent movement. At that point, study depict some current works in various zones, for example group detection in informal organizations, the analysis of large graphs, the clustering and partitioning of bi-partite graph and Clone detection.[7] At that point we present the premise of our approach. In the third segment, we exhibit how we expect to build up our investigation, and how we will test the proposed arrangements through trials. In the last part, we will give some preparatory conclusions.

II. LITERATURE SURVEY

G.Thomas et.al.proposed that the volume of information recorded and traded on systems requires growing new administration approaches for information capacity, refresh, hunt, representation and analysis. Furthermore, these information are not put away in a novel advanced organization, but rather are heterogeneous, organized or not, and sight and sound. In that undertaking, we will center all the more decisively around these systems framed by possibly connected information, because of the reality that they share the same Clone lent movement. The goal is to have the capacity to offer attributes to proposals hubs and connections, to appear how they are gathering, framing interest groups or even rising structures[8].

M.Conti.et.al.proposed that the connections are manufactured in light of certain data trades between people, living beings or elements A Wireless Sensor Network (WSN) is an stock of sensors with constrained assets that team up to accomplish a typical objective. Wireless sensor networks can fulfill the both civil and military related applications. These are prone to different kinds of attacks because of their operating nature [9].

J.Anthoniraj et.al.proposed the clone attack detection mechanism within wireless sensor network. An attacker captures the data from one node and the exact information of that node from the network. Then create a clone by reprogram the captured node, then these clones are expand in the network areas and considered as sensible members of network. So it is hard to distinguish a reproduced node. There are correspondence joins speaking to the messages traded between individuals, participation joins speaking to structures (organizations, social or expert gatherings, administrations, item classes, and so on.) and affiliation connects between substances [10,11].

D.Dave et.al. suggested that the clone attack detection within online social media is proposed through this research. Since this network is quite large in size hence consume huge amount of time

while evaluating clone attacks. A first qualification should be possible at this level between static connections illustrative of structures and dynamic connections illustrative of activities. In the field of informal community analysis numerous methodologies depend on systems disintegration into sub networks, such as on account of group detection in informal organizations. An agglomerative strategy permits distinguishing all maximal coteries speaking to connections. The bits of qualified groups are framed by iteratively including the left vertices to their nearest portions to acquire a partial group that speak to the fragmentary sub network. Bipartite graph partitioning and information clustering are especially promising methodologies for graph analysis. The issue is figured as a bi-partite graph to bunch/partition hubs by limiting an edge thickness work utilizing Singular Value Decomposition. A system formed of model and MR works that incorporate a few graph analysis capacities can be utilized for large graph processing. Distinctive kinds of Clone estimation and detection methods have just been proposed, some of which are utilizing group development in light of roundabout connections between people [12, 13].

R.Grewal et.al.proposed approach survey the techniques used to detect clone attack within wireless sensor network. An attacker physically compromised the node, make a copy of hardware with the captured information and introduce the position to that copied hardware in the network. Hence the detection of copied information becomes very important and challenging issues in the security. Surveyed techniques are commonly partitioned into application dependent and application independent schemes. Author proposed effective clone attack detection mechanism within wireless sensor network. The proposed mechanism solves the problem of cost encountered in the detection of clone attacks [14,15].M.V.Barbera et.al. proposed clone attack detection mechanism by using personal and community certificate scheme issued by the network. The main problem with this approach is time consumption and cost since extra node at server end is required to be maintained as a supervisor node [16].

III. METHODS AND MATERIAL

A. Research Plan

The research takes place by using MATLAB as tool for simulating WSN network having set of nodes and edges forming the network. The network is formed by randomly placing nodes over the network having size of 100x100 cm2. Once the network is formed hybrid firefly algorithm is applied for detecting the clone attack if any within the network.

The main steps of the study as follows:

i. Select social network dataset or link several social networks data together (Facebook, Twitter, LinkedIn, Google, wiki) by defining a large scale social network for analysis
ii. Use hybrid firefly algorithm to detect the clone if any within the network. The used dataset is derived from the snapford.edu website.
iii. Once a given clone will be identified (with a known structure or not), we will apply different Clone detection algorithms on clusters/partitions to the identified community matrix. Clone detection is predicted in terms of number of clone attack detected.

B. Methodology

Proposed work takes into consideration the identification of nodes. The ids assigned to each node is analyzed to determine whether the id as similarity. In case id matches clone is detected. To detect the clone attack hybrid firefly algorithm is used. The dataset required for investigation is derived from the stanford.edu machine learning website.

✓ **Dataset Used**

Wikipedia is a free reference book composed cooperatively by volunteers far and wide. A little piece of Wikipedia patrons are directors, who are clients with access to extra specialize highlights that

guide in support. Smart ids alert dataset derived from Stanford University is used for evaluation through the proposed system. The dataset description is given as under:

Table I Data set used

Dataset statistics	Value
Number of nodes	7115
Number of edges	103689
Nodes in largest cluster	7066
Edges in larges Cluster	103663
Nodes in smallest cluster	1300
Edges in smallest cluster	39456
Average clustering coefficient	0.1409
Diameter	7
Fraction of close triangle	3.8

The derived dataset is of Wikipedia from where analysis process begins. A Firefly Algorithm based approach is proposed to control blockage in WSN at transport layer. Firefly bug produces flashes of brief length through a procedure called bioluminescence. It is utilized to pull in potential prey or accomplice or for the issue of caution against predator. In this way power of glimmer turns into a vital parameter for the other firefly bugs. Firefly Algorithm takes after three principles [17]:

i. Fireflies of any sex can draw in towards the other firefly;
ii. An appeal factor is considered which relies upon the shine of the blaze, as the fireflies' turn towards the more alluring fireflies;
iii. The shine of fireflies is computed through a goal work.

✓ **Hybrid Firefly Algorithm**

a) Generate random Ids for the nodes.
b) Assign the Ids to the nodes.
c) Detect the Clone Entry using firefly algorithm
d) If Malicious(clone) then
e) Block the node
   Else
f) Move onto next step in sequence
   End of if
g) Calculate localization Error
h) Stop

The used algorithm first of all assigns random ids to each and every node within the network. The Ids stored within the routing tables also when the data is transmitted from source to destination the routing table is analyzed for determining whether ids of the node again occur within the table or not. In case id of the receiver is matched with the node in between the network then clone or attacker is detected. Briefly this mechanism is given within the flowchart as under

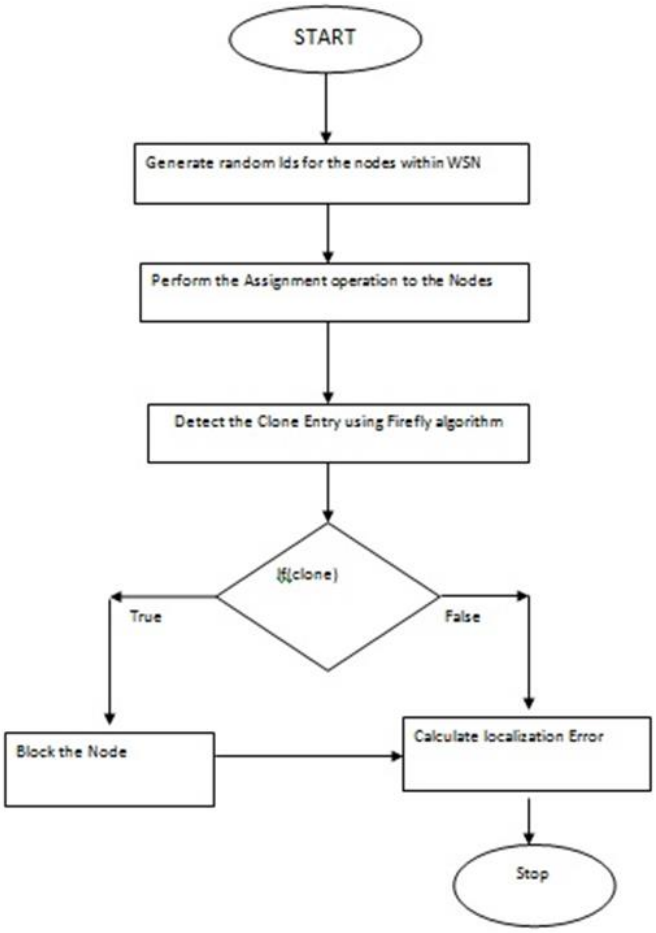

Figure 2. Flow diagram of firefly algorithm

IV. RESULTS AND DISCUSSION

The simulation takes place within the MATLAB. The produced simulation will indicate that the proposed system produces better result as compared to the existing system. The proposed system utilizes the Tabu Search along with power calculations in order to optimize the result obtained through the Grid structure. At first place the number of simulations, Clone detected with existing and number of Clone detected proposed are considered. The tabular structure of the proposed scheme is as follows:

Table II. Showing Clone detected through existing and proposed techniques

Simulators	Fuzzy Based	Fire fly Based
Test 1	12.5357	22.4715
Test 2	36.6243	44.4277
Test 3	48.6805	64.4345
Test 4	46.7414	60.4107
Test 5	73.0829	98.9666

The Plot for the same is given as under

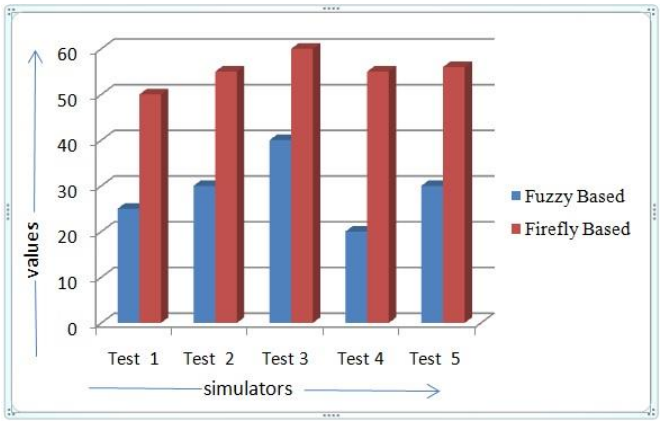

Figure 3. Plots for number of Grids, Power and Machines

Table III: Time Consumption through existing and proposed simulation:

Simulations	Fuzzy Based	Firefly Based
Test 1	25	50
Test 2	30	55
Test 3	40	60
Test 4	20	55
Test 5	30	56

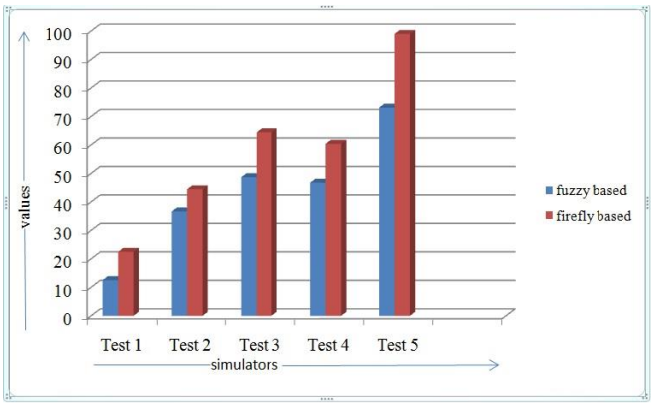

Figure 4. Plot of existing and proposed system time consumption

V. CONCLUSION

In this paper we have presented our motivations to study large scale social networks for characterizing communities. Study will address the problems of linking information spread over several heterogeneous networks, algorithm parallelization and optimization for network analysis, and graph partitioning and clustering for structure extraction. This paper outlines the different types of attacks and detection of clones by using firefly algorithm. Hence this work will provide an answer to Clone detection.

V. REFERENCES

[1]. I Amerini, L. Ballan, S. Member, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-Based Forensic Method for Copy – Move Attack

Detection and Transformation Recovery," vol. 6, no. 3, pp. 1099–1110, 2011.

[2]. Z Fei, S. H. I. Wenchang, Q. I. N. Bo, and L. Bin, "Image Forgery Detection Using Segmentation and Swarm Intelligent Algorithm," vol. 22, no. 2, pp. 141–148, 2017.

[3]. S Kiruthiga, "Detecting Cloning Attack in Social Networks Using Classification and Clustering Techniques," IEEE, 2014.

[4]. Y. Sylla and P. Morizet-mahoudeaux, "Fraud detection on large scale social networks," no. 1, pp. 1–2.

[5]. Meenakshi sharma and Dr. Himanshu Aggarwal ,Indian Journal of Science and Technology,Vol 9(34), DOI: 10.17485/ijst/2016/v9i34/100211, September 2016

[6]. C Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-based Fraud Detection Research."

[7]. D Sensarma and S. Sen Sarma, "A Survey on Different Graph Based Anomaly Detection Techniques," vol. 8, no. November, 2015.

[8]. G Thomas, "Cloud computing security using encryption technique," pp. 1–7.

[9]. M Conti, R. Di Pietro, L. V Mancini, and A. Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks," pp. 1–14, 2010.

[10]. Meenakshi sharma and Dr. Himanshu Aggarwal. "Methodologies of legacy clinical decision support system -A review", Journal of Telecommunication, Electronic and Computer Engineering(JTEC Journal) SJR and Scopus Ranking .

[11]. J. Anthoniraj and T. A. Razak, "Clone Attack Detection Protocols in Wireless Sensor Networks?: A Survey," vol. 98, no. 5, pp. 43–49, 2014.

[12]. D. Dave, N. Mishra, and S. Sharma, "Detection Techniques of Clone Attack on Online Social Networks?: Survey and Analysis," Elsevier, pp. 179–186.

[13]. "Scientific Advice Mechanism Scoping Paper?: Cybersecurity," vol. 2016, 2016.

[14]. H. W. J. L. L. Zhou, "Lightweight and effective detection scheme for node clone attack in wireless sensor networks," IEEE, no. December 2010, pp. 137–143, 2011.

[15]. R. Grewal and P. G. Scholar, "A Survey on Proficient Techniques to Mitigate Clone Attack in Wireless Sensor Networks," IEEE Access, pp. 1148–1152, 2015.

[16]. M. V Barbera and A. Mei, "Personal Marks and Community Certificates?: Detecting Clones in Wireless Mobile Social Networks," 2012.

[17]. F. S. Rizi, M. R. Khayyambashi, and M. Y. Kharaji, "A New Approach for Finding Cloned Profiles in Online Social Networks," ACEEE Int. J. Netw. Secur., vol. 6, no. April, pp. 25–37, 2014.

[18]. Yang, X.-S. and He, X.S. (2013) Firefly Algorithm: Recent Advances and Applications. International Journal of Swarm Intelligence, 1, 36-50.

[19]. Meenakshi sharma and Dr. Himanshu Aggarwal,"Grand Barrier In Clinical Decision Support System", International Journal of Latest Trends in Engineering and Technology Vol.(9)Issue(2), pp.111-115 DOI: http://dx.doi.org/10.21172/1.92.19 e-ISSN:2278-621X