Clone Attack Detection in Complex Network Using Overlapping Communities (DCA)

Ronika devi[1], Mohit trehan[2]
[1]*Student, Deptt.of CSE, GCET, Gurdaspur Punjab, India*
[2]*A.P (CSE), GCET, Gurdaspur Punjab, India*

Abstract- **In today's world the wireless sensor network has great significant in application like defense surveillance, patient health monitoring, traffic control etc. As WSN utilize radio frequencies so there is threat of interference in network. These threats also include distributed denial of service in which the messages that are sent over the network may be attacked by unauthorized user. It would harm the confidentiality of the network user and the services of network. There are various algorithm that are utilized to detect clone attack in WSN but these schemes only stress on prevention of attack after it is occurred. This would leads to the loss of data and more consumption of limited network resources. So in this paper we introduce a new algorithm that is based on DCA along with random walk detection. It would detect earlier the clone attack in WSN and prevent the data loss. The performance of this technique has been analyzed by using parameters like packet delivery ratio, energy consumption by network, throughput.**

Index Terms- DCA, WSN, clone detection.

INTRODUCTION

Wireless sensor networking stays a standout amongst the most requesting and rising exploration territories of our chance. A Wireless Sensor Network (WSN) is a gathering of self-ruling nodes, which transmits information in wireless channel with little transmission capacity utilization and recurrence. [1]
The various applications such as military application, data collection and monitoring utilize the sensor network because it gives minimal effort solution. Every hub can discover their neighbor nodes in network and this give assistance in courses arrangement in the gathering.[2] Because of a few shortcomings like restricted preparing memory, ability and because of communicate transmission medium Wireless Sensor Networks are generally helpless against attack like Denial of Service. These kinds of assaults lessen the ability of WSN, with the goal that they can't work for a drawn out stretch of time. It has often consequences for utilization assets in the network and expands the energy utilization, delay, and decreases the throughput. [3]
The un-ability of authorized user to access network resources that may be website or whole system is known as clone attack. A Distributed clone attack is a synchronized assault which is done on the accessibility of services of some specific network with the assistance of traded off processing frameworks in a roundabout way, so tracking the cloned packets turns out to be more troublesome [3]The principle point of this paper is to shield the Wireless Sensor Network from flooding, a kind of clone assault. Flooding can deplete all network assets, for example, data transfer capacity, energy and processing power and so on and plan another location plot named early identification of clone assault utilizing distributed method. This plan recognizes the attacker based on the quantity of transmissions relating to the quantity of neighbors of a hub and these transmissions are contrasted and the limit esteem registered and PDR of different nodes in the network. [4]
Clone attack (additionally called hub replication attack) is a serious attack in WSNs. In this attack, a foe catches just a couple of hubs, duplicates them and afterward conveys subjective number of imitations all through the system. The catch of hubs is conceivable in light of the fact that sensor hubs are typically unprotected by physical protecting because of cost contemplations, and are frequently left unattended after deployment. On the off chance that we don't distinguish these reproductions, the system will be helpless against a vast class of inner attacks.[5] For instance, the foe presently can catch the movement passing the reproductions (which may contain the

previously mentioned areas of troopers), infuse false information into the system (which might be false summons), slander different hubs and even disavow true blue hubs. Hitherto, most conventions for identifying hub replication have depended on a put stock in base station to give worldwide location. Additionally a portion of the current verification strategies [4, 5] can't identify such attacks, since every one of the reproductions hold real keys. The current methodologies fall into following two classes:
A. Brought together Detection The clearest recognition conspires requires every hub to send a rundown of its neighbors and their guaranteed areas to the base station. The base station would then be able to analyze each neighbor rundown to search for imitated hubs. On the off chance that it finds at least one copy, it can repudiate the imitated hubs by flooding the system with a confirmed renouncement message. [6]
B. Nearby Detection: To abstain from depending on a focal base station, we could rather depend on a hub's neighbors to perform replication identification. Utilizing a voting system, the neighbors can achieve an agreement on the authenticity of a given hub. Sadly, while accomplishing recognition in a disseminated design, this technique neglects to distinguish circulated hub replication in disjoint neighborhoods inside the system. For whatever length of time that the duplicated hubs are no less than two bounces from each other, a simply neighborhood approach will fail. [7]
A clear answer for protect against clone attacks is to give the base station a chance to gather the area data (e.g. area, neighbor list, and so forth.) from every sensor and screen the system centralized. This approach experiences high correspondence overhead by asking for excess data from the system. Further, a "shrewd" clone may report the area of the first hub, influencing the base station to flop in distinguishing the imitation. In [8], propose for one-jump networks that the base station (BS) can store the one of a kind flag trademark for every gadget, and in this way gadget cloning can be distinguished as needs be. Nonetheless, in a multi-bounce sensor organize; it is unreasonable for BS to track the flag attributes of sensors multi-jumps away. In restricted voting/trouble making identification plans [8], hubs inside an area concur/vote on the authenticity of a given hub in view of their nearby perceptions. By the by, these plans are not fit for identifying clones with typical conduct, and may fizzle when various clones in closeness intrigue. Moreover, limited voting/trouble making identification plots intrinsically do not have the capacity to identify dispersed clones that may show up at wherever in the system.

LITERATURE SURVEY

Clone attack detection methodology is proposed by [9]. The framework employed by Kontaxiset. Al can be used by the users to determine whether they are under clone attack or not. The components employed in this framework involves

Information distiller
This component is used in order to extract the information from legitimate social networking site. Information that could be used to identify the user is extracted by this component and maintained within the buffer.

Profile Hunter
Profile hunter used to locate the profile of the users. In case multiple records corresponding to single user is fetched then clone attack is detected.

Profile verifier
This component verifies the records filtered by profile hunter. The filtered information is compared against the profile of the user to find the nearest matches. In case matches do occur, profile clone attack is detected.
User footprint analysis is proposed by [10]. User may have multiple accounts over the various services over the internet. All the services over the internet uses digital mechanisms. All these digital footprints can be collected together to determine the profiles of the users consuming multiple web services.
Topological feature extraction mechanism is proposed by[11] for clone attack detection. In clone attack detection, earliest techniques assume that distinguished keywords are used by malicious users. But this may not be the case all the time. in order to tackle the situations, features like images, topological features etc. must be analysed. Topological analysis allow the user to construct the profile on the basis of heterogeneous features hence producing accurate result associated with the clone attack.

The clone attack detection techniques as proposed by [12] can be considered for such attack resolution. According to Dave et. Al., attack can either be on the access restricted information and anonymous data attacks. To tackle the situations attributes similarity based privacy preservation solutions are proposed. Several techniques corresponding to attribute similarity are used in order to determine the clone attacks.

Social networking is one of the most widely used internet activity as proposed by [9]. it is prone to profile clone attacks and its preservation is compulsory. Kontaxis et al proposed mechasnism for detection of profile clone attacks by the use of archituctural design and prototype system for detecting similarity of attributes in case profile of the user is copied. Experiment result shows better result of clone attack detection hence proving worth of the study.

Clone attack is a problem over the online social media. Detecting and preserving the state of the online social media is a need of the hour. Online social media plays a role of complex network. To detect the profile cloning attacks from such a network technique has been proposed by [13]. Entire social media is diided into tow parts. First part considered and dra the social network as a graph. In the second part, graph is divided into subparts based on the similarity of profile. The modular approach considered ultimatley led to the formation of smaller networks consisting of only those nodes having similar characterstics or properties thus facilitate detection of clone attacks. Online social media is a huge network of users. As the uers of the online social media grows, so does the chances of clone attack. To detect the clone attack a new approach for clone attack detection is proposed by [14]. Clone attacks causes the similar profiles from one or more users. In order to determine the similarity, strength of suers profiles matching is determined. The strength determines profile clone attack by the said mechanism. degree of modularity achieved through this technqiue is not perfect and required certain degree of modifications.

PROPOSED METHODOLOGY

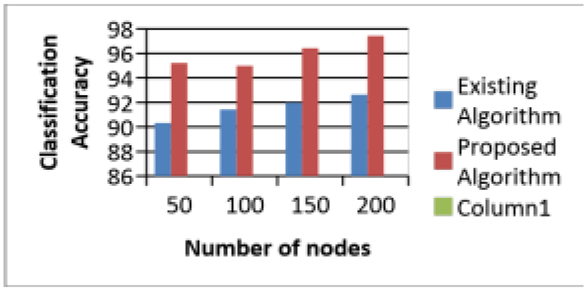
In numerous social networking destinations, network topological structure and properties esteems are the entire data. Hubs represent to clients and edges represent to the relationship among them. In every hub, there are a few characteristics, for example, name, sexual orientation, training, interests, area and social exercises. Clearly network topological structure and trait data can be utilized to recognize some shrouded designs in groups. In this examination, DAC clustering calculation is connected to distinguish groups in social network diagrams. The accompanying demonstrates a pseudo code of the calculation where it acknowledges a property expanded diagram and restore a clustered chart as yield.

```
Input number of nodes G, a
A←adj(G)
K= a X E[G]
Compute the attribute matrix, C
Sij= 1 if (I,j) €TopKpair(C), 0 otherwise
W= A+S
Cluster ←Apply Random walk for clustering
Return clusters
```

RESULT AND DISCUSSION

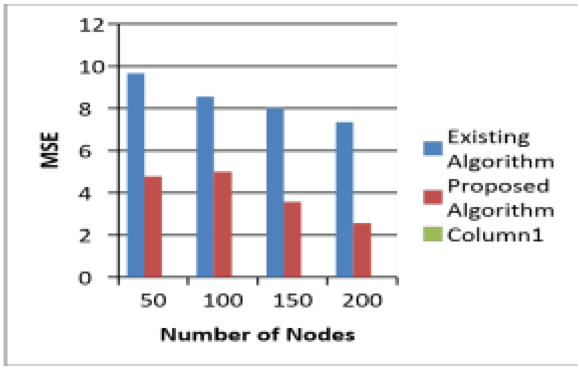
Classification Accuracy

Number of nodes	Existing Algorithm	Proposed Algorithm
50	90.33	95.22
100	91.44	95
150	91.99	96.44
200	92.66	97.45



MSE

Number of nodes	Existing Algorithm	Proposed Algorithm
50	9.67	4.78
100	8.56	5
150	8.01	3.56
200	7.34	2.55



CONCLUSION

In this paper we presenting the updated self-mending, Randomized, Efficient, and Distributed DCA-random walk calculation for the identification of hub replication assaults when contrast with the Line-Selected Multicast and Randomized , Efficient, and Distributed conventions. The fundamental commitment of this paper is the new proposition of DCA-Random walk that is capable for recognizing hub replication assault when contrasting with the .That DCA is stronger in its location capacities than Naïve Bias. We trust that the new technique creates the proficient and solid outcomes in future still our examination is going on this area.

REFERENCES

[1] Reyaz Ahmad sheikh, "Detection of Clone Attack in Wsn\n," IOSR J. Comput. Eng., vol. 16, no. 5, pp. 48–52, 2014.

[2] A. Kaur, "DDOS Attack Detection on Wireless Sensor Network using DSR Algorithm with Cryptography," vol. 175, no. 3, pp. 16–23, 2017.

[3] V. Subramanian, "Proximity-based attacks in wireless sensor networks," Int. J. Sci. Eng. Res., vol. 3, no. May 2013, pp. 2–5, 2013.

[4] V. A. Khandekar, P. Singh, and G. Shrivastava, "Simulation Approach To Detect Clone Attack in," no. May, pp. 7–13, 2013.

[5] M. H. Ansari and V. Tabatabavakily, "Classification and A analysis of clone attack detection procedures in mobile wireless sensor networks," vol. 2, no. 11, pp. 1–7, 2012.

[6] W. Znaidi, M. Minier, and S. Ubéda, "Hierarchical node replication attacks detection in wireless sensor networks," Int. J. Distrib. Sens. Networks, vol. 2013, 2013.

[7] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks," vol. 8, no. 5, pp. 685–698, 2011.

[8] N. Shruthi and C. K. Vinay, "Network Layer Attacks : Analysis & Solutions , A Survey," vol. 18, no. 2, pp. 67–80, 2016.

[9] G. Kontaxis, I. Polakis, S. Ioannidis, and E. P. Markatos, "Detecting Social Network Profile Cloning," IEEE, 2013.

[10] A. Malhotra, "Studying User Footprints in Different Online Social Networks."

[11] S. Y. Bhat and M. Abulaish, "Communities A gainst Deception in Online Social Networks 1 The Platform 2 The Mischef," Ieee, vol. 2014, no. 2, pp. 8–16, 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] M. Kharaji and F. Rizi, "An IAC Approach for Detecting Profile Cloning in Online Social Networks," vol. 6, no. 1, pp. 75–90, 2014.

[14] 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.