HIGH THROUGHPUT CLONE AVOIDANCE IN WIRELESS SENSOR NETWORKS

Kavya.S, Jyothsana.R, Dinesh.P.S

B.E.,Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India.
B.E., Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India.
M.E., Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India.

ABSTRACT

It describes a high throughput clone avoidance protocol in densely deployed WSNs, which can guarantee successful clone detection and avoidance and maintain satisfactory lifetime network. Specifically, location information of sensors and randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks is exploited. The ring structure facilitates energy efficient data forwarding along the path towards the witnesses and the sink. The author proves that the proposed protocol can achieve 100 percent clone detection probability using ERCD protocol and clone avoidance using LAL protocol with trustful witnesses. The work can be further extended by studying the clone detection performance with untrustful witnesses and show that clone detection still approaches 98 percent when 10 percent of witnesses are compromised. In most existing clone detection protocols, the required buffer storage of sensors is usually dependent on the node density that is O (√n), while in proposed protocol, required buffer storage is independent of n but a function of hop length of the network radius h, i.e., O (h). Extensive simulations demonstrate that proposed protocol can achieve long network lifetime by effectively distributing the traffic load across the network. Clone is avoided by the determination of cluster head which is done using the localizability -aided localization (LAL).The throughput achieved in the existing system is of 46% while the throughput achieved in the proposed system is nearly about 92.5%. The existing system suffer from a delay of 160 nanoseconds whereas the proposed system has a delay of nearly 90 nanoseconds.

Keyword: - *Wireless sensor networks, clone avoidance protocol, Throughput, Cluster head.*

1. INTRODUCTION

Wireless sensors have been widely deployed for a variety of applications, ranging from environment monitoring to telemedicine and objects tracking, etc. For cost-effective sensor placement, sensors are usually not tamper-proof devices and are deployed in places without monitoring and protection, which makes them prone to different attacks For example, a malicious user may compromise some sensors and acquire their private information. Then, it can duplicate the sensors and deploy clones in a wireless sensor network (WSN) to launch a variety of attacks, which is referred to as the clone attack. As the duplicated sensors have the same information, e.g., code and cryptographic information, captured from legitimate sensors, they can easily participate in network operations and launch attacks. Due to the low cost for sensor duplication and deployment, clone attacks have become one of the most critical security issues in WSNs. Thus, it is essential to effectively detect clone attacks in order to ensure healthy operation of WSNs. To allow efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help certify the legitimacy of the nodes in the network. The private information of the source node, i.e., identity and the

location information, is shared with witnesses at the stage of witness selection. When any of the nodes in the network wants to transmit data, it first sends the request to the witnesses for legitimacy verification, and witnesses will report a detected attack if the node fails the certification. To achieve successful clone detection, witness selection and legitimacy verification should fulfill two requirements: 1) witnesses should be randomly selected; and 2) at least one of the witnesses can successfully receive all the verification message(s) for clone detection. The first requirement is to make it difficult for malicious users eavesdrop the communication between current source node and its witnesses, so that malicious users cannot generate duplicate verification messages. The second requirement is to make sure that at least one of the witnesses can check the identity of the sensor nodes to determine whether there is a clone attack or not. To guarantee a high clone detection probability, i.e., the probability that clone attacks can be successfully detected, it is critical and challenging to fulfill these requirements in clone detection protocol design [4]. Though the system is memory efficient, the system has a low throughput as well as a greater delay. The clone avoidance is done using LAL protocol.

2. LOCALIZABILITY- AIDED LOCALIZATION (LAL)

Localization is used in many sensor network applications. In the real world deployment for analysis network entirely localizable, leaving a certain number of theoretically in non-localizable nodes. To emulating localizability involves unnecessary adjustments and accompany costs. In this, fine-grained approach localizability-aided localization (LAL), which basically consists of three levels of phases in the algorithm. LAL algorithm triggers with single round adjustment to get some popular localization methods which can be successfully carried out being aware of node localizability. Thus by using LAL, avoidance of clone is successfully achieved with high throughput.

2.1 PHASES OF LOCALIZABILITY-AIDED LOCALIZATION (LAL)

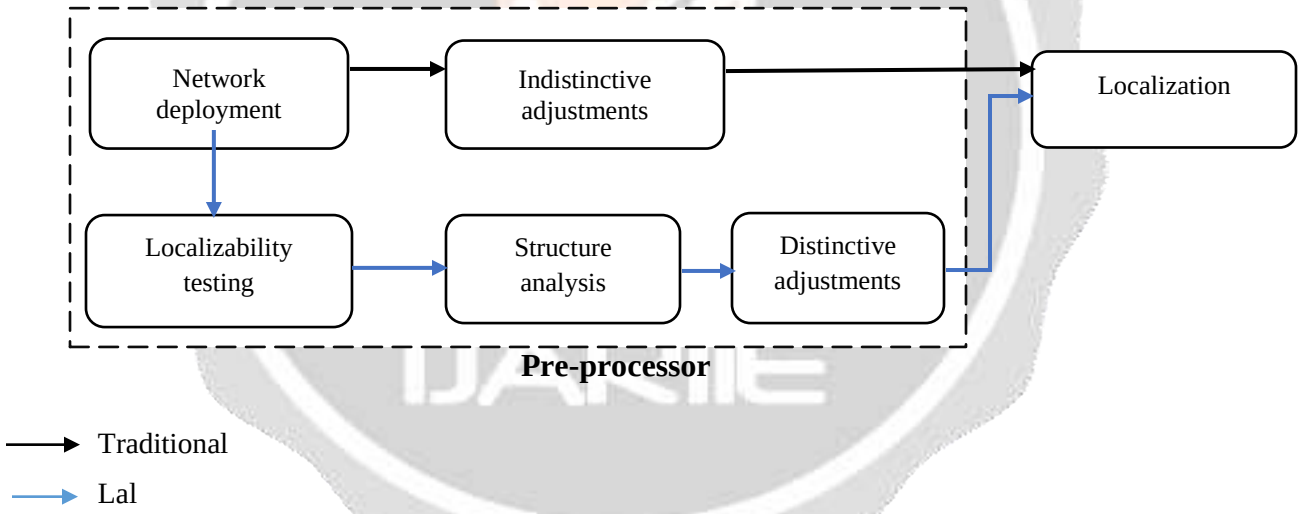

Fig- 1: Block Diagram for LAL Algorithm

Localizability aided-localization (LAL) is a fine-grained approach which basically consists of three phases as in Figure 4.1.

- Node localizability testing
- Structure analysis and
- Network adjustment.

Node localizability testing: By deriving necessary and sufficient conditions for node localizability, for the first time, it is possible to analyze how many nodes one can expect to locate in sparsely or moderately connected networks. To validate this design, implement the solution on a real-world system and the experimental results show that node localizability provides useful guidelines for network deployment and other location-based services. Node localizability testing is done by using some special nodes namely base station which knows their global location and rest of the location is determined by their Euclidean distances. The major challenge is to identify uniquely localizable nodes. An obvious solution is found and all the nodes are identified by sub graph localizable.

Structure analysis: Networks have also been studied extensively in social sciences. Typical network studies in sociology involve the circulation of questionnaires, asking respondents to detail their interactions with others. One can then use these responses to reconstruct the network in which vertices represent individuals and edges the interactions between them.Then it aims to predict what the behavior of the networked systems will be on the basis of measured structural properties and the local rules governing individual vertices. Now for example the network structure affect traffic on the internet, or the performance of a web search engine, or the dynamics of social or biological systems. Scientific community has drawn broad variety of disciplines, made an excellent start on the first two of these aims, the characterization and modelling of network structure.

Network adjustment: To locate non-localizable nodes, the existing solution mainly focus on how to tune network settings. The first attempt is to deploy additional nodes in application fields. This incremental deployment increases node density and thus increasing the localizability. However, this attempts suffers from less feasibility due to the fact that the additional nodes are placed nearer to the non-localizable nodes whose locations are unknown.Using mobile nodes is another choice. The controlled motion of special nodes provides thorough information for localization, but also incurs adjustments delay and control overheads.

2.1 AVOIDANCE ALGORITHM

- Create a group of sensor nodes. The base station gives the unique ID to each node and makes that node as the original node.
- We divide a complete network into clusters.
- Cluster head is selected in each cluster.
    - This is applied for each separate cluster. RED algorithm is applied for overall distributed network, so there is a delay in detecting the clone attack when it is more.
    - We apply algorithm for different cluster group so the delay in detection of clone attack will be reduced.
    - The concept of RED algorithm is used for fair comparison.
- A random value is distributed by using centralized mechanism like satellite or any other central stations.
- Each node broadcast its ID and location to its claim.
- Neighbours receive the broadcast and each neighbours sends the claim.
- The claim is sent to any of the location. This is selected using pseudo random function (We are not using any ID to select the location).
- Before broadcasting, every node signs its message with its private key.
- Signature is verified at the destination end. At the destination ends:
    - The signature check is carried out by verifying the received signature.
    - Message freshness: The ID and location information is extracted from the received message. At the destination end it simply stores the ID and location if the claim node is first carrying that ID and location.
    - If it receives the same ID and location for second time, it checks for the coherence of ID and location. This is the proof of detection of clone with two in-coherent claims.
- The in-coherent ID and location is checked with cluster head and also with base station. It detects the clone node.
- Clone node information is broadcasted to all other nodes. By this we can avoid the claim of clone node with other nodes in the network

4. RESULTS AND DISCUSSIONS

6.1.1 Clone detection

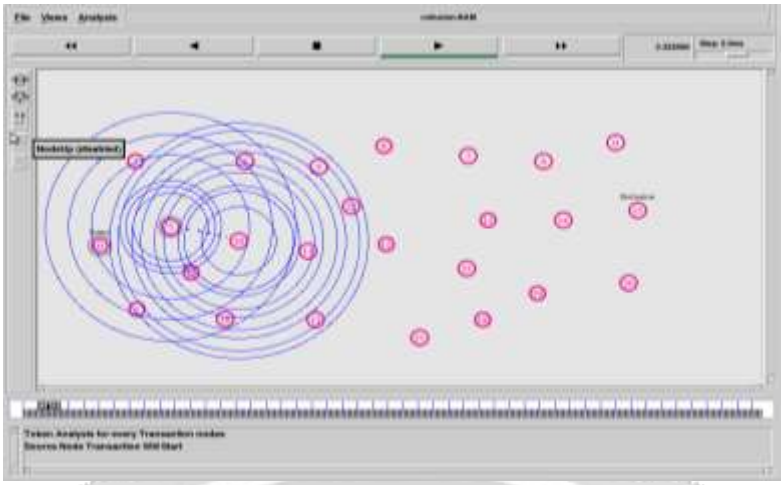

Fig 2:- Determination of Path

In the Fig 2, the nodes are distributed randomly. When source finds destination it establishes path between them using route reply and route request method.

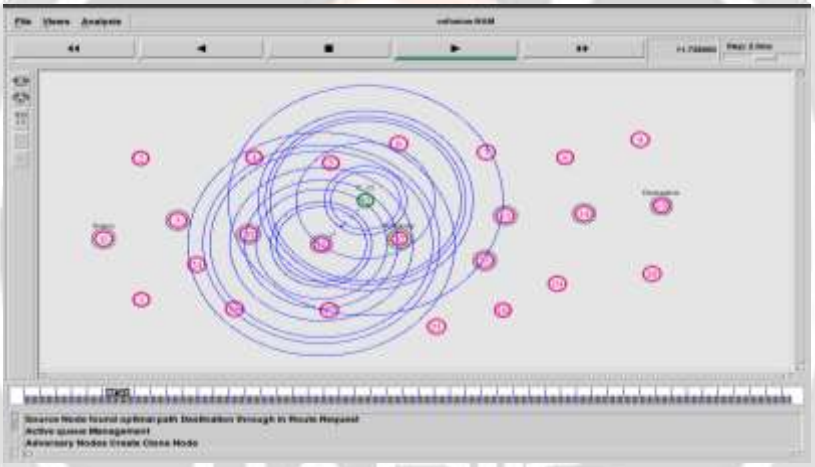

Fig 3:- Clone Detection by Adversary Node

In Fig 3, an adversary node is randomly assumed from the determined path. The node is identified as clone node when the packet loss occurs instantly. The clone is detected by using the adversary node. The detected clone is denoted as C_ adversary node number.

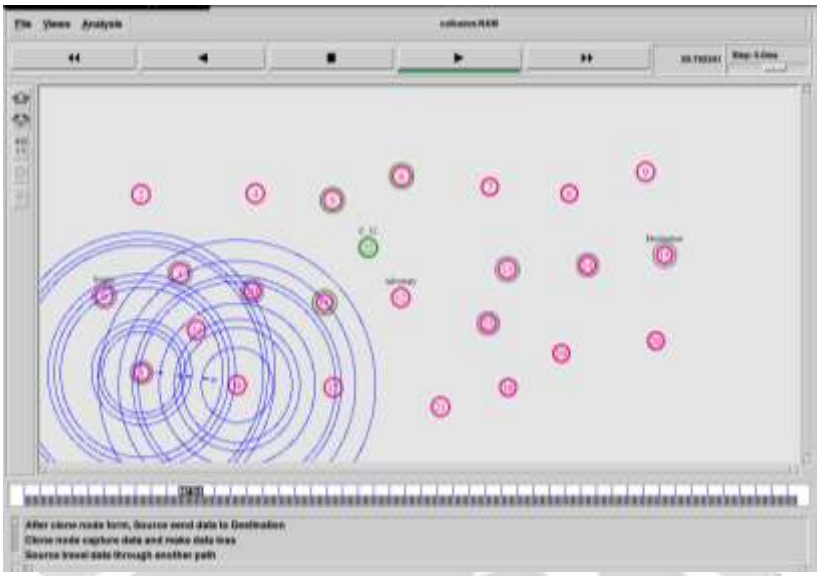

Fig 4:- Diverting the Path Due to the Presence of Clone Node

In Fig 4, the pre-determined path is diverted to a new path due to the presence of clone node in the path. This new path has the same adversary node as assumed previously. Adversary node checks the status of each node and delivers the message to the neighbour nodes, i.e., it is a clone node or node.

The Fig 5 shows that all the nodes are grouped into different zones which has three destination and one source. Each destination has a separate adversary node. This is the main disadvantage because the number of adversary nodes increases as the number of destination increases.

Hence to overcome this disadvantage nodes are assumed to be dynamic in nature by the determination of cluster head.

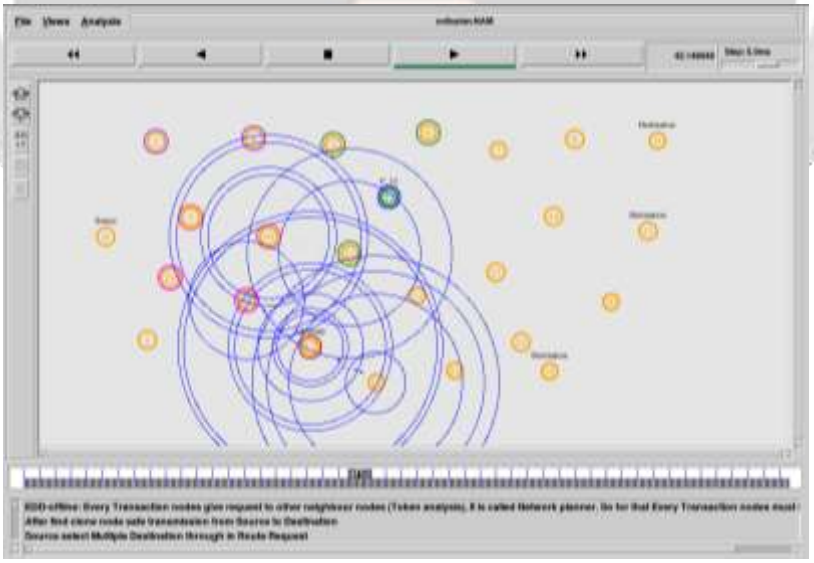

Fig 5:- Different Zone with Allocation of Multiple Adversary Nodes

6.1.2 Clone avoidance

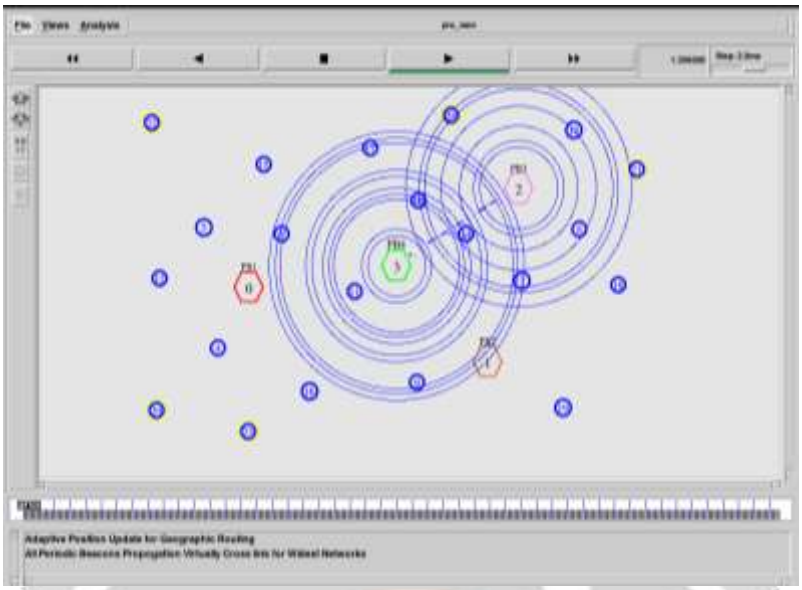

Fig 6:- Determination of Cluster Head and Base Station

In Fig 6, node 3 is assumed as base station and the remaining node 1, 2 and 0 are the cluster heads. Yellow colour nodes are assumed as the clone nodes. The base station starts to broadcast its ID to the cluster head and all neighbouring nodes.

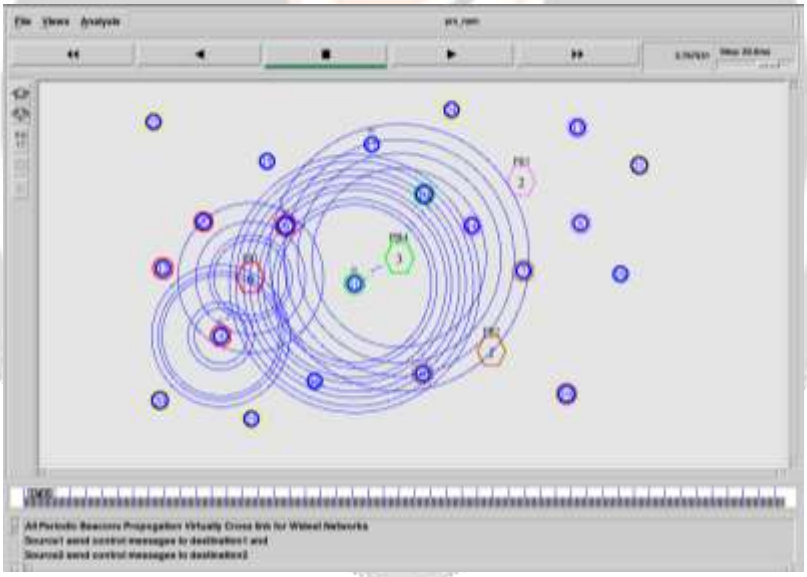

Fig 7:- Formation of Clusters

The Fig 7 shows that the clusters are formed once the ID is broadcasted. The different colours indicates that the clusters belong to their own cluster head alone and not any other cluster head. The other uncoloured nodes are assumed to be within the range but does not belong to any cluster head.

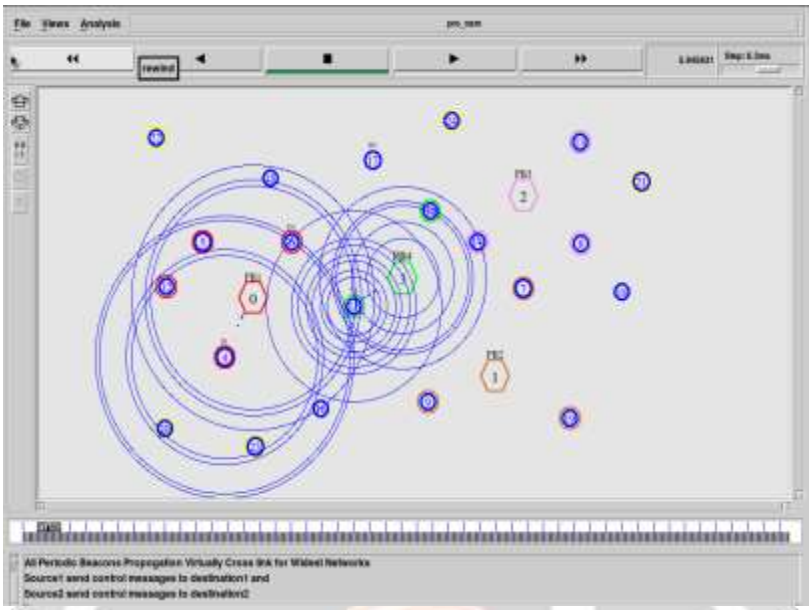

Fig 8:- Transmission of Data

The Fig 8 shows that the data is transmitted through base station and cluster head. Base station transmits the data to the clusters only that are on its own range of ring structure.

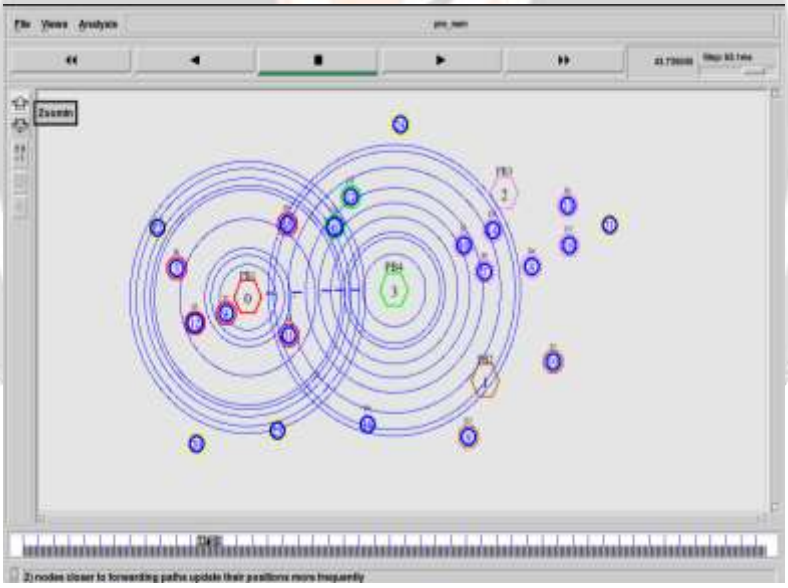

Fig 9:- Avoidance of Clone

The Fig 9 shows that the clone is avoided though it is in the range of the cluster head. Thus by forming cluster head clone node information is broadcasted to all other nodes. By this the claim of clone node with other nodes in the network can be avoided.

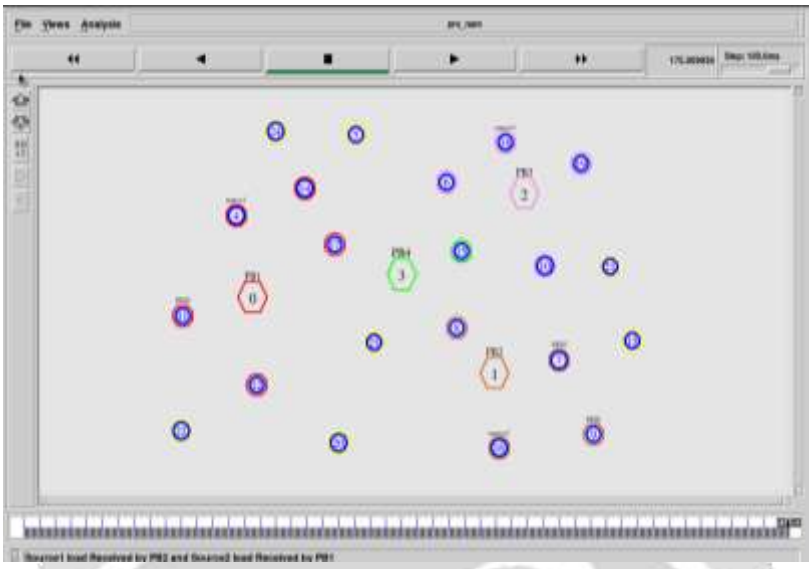

Fig 10:- Optimum Transmission

Finally, LAL shows that optimum transmission is achieved from source to the destination and improve the routing performance in terms of packet delivery ratio with periodic beaconing as in Fig 10.

6.2 SIMULATION OF GRAPHS

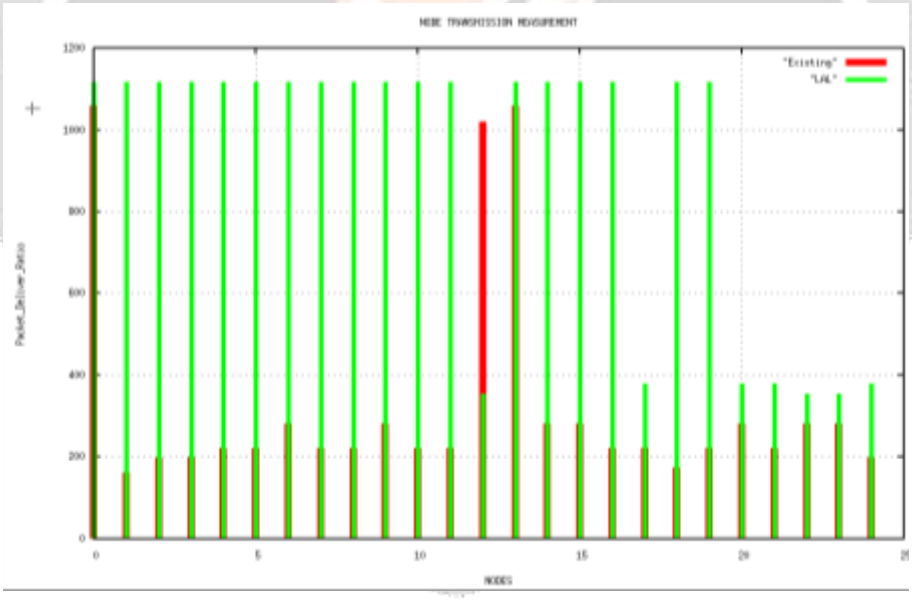

Fig 11:- Node Packet-Delivery

This graph is a comparison between the existing system and the proposed system (LAL) as in Fig 11. It indicates that the packet delivery is more by using LAL protocol than the existing system.

Fig 12:- Delay Measurement

The Fig 12 describes the delay measurement between the proposed and the existing system. In the proposed system a minimum delay due to the transfer of data through base station and cluster head is inferred. By comparing both it can be concluded that delay achieved in existing is 160 and delay is reduced to 70 in proposed system.

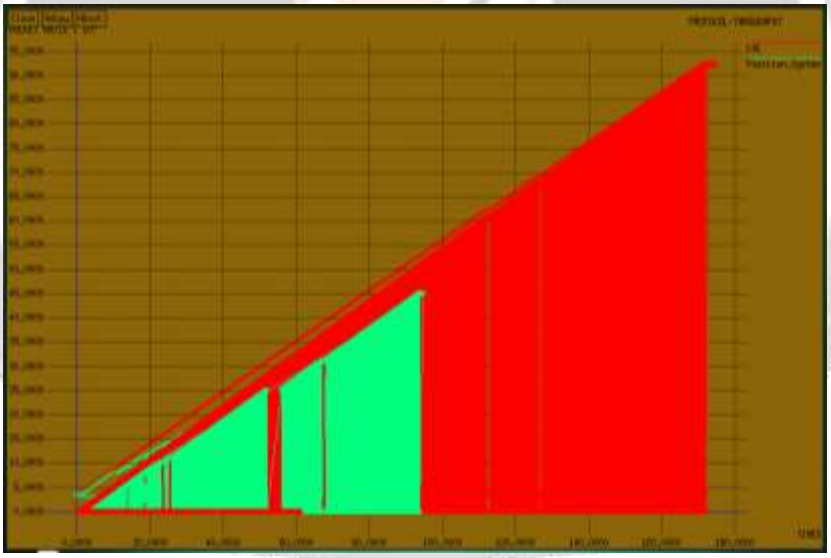

Fig 13:- Throughput

The comparison of throughput between the existing and proposed system is been depicted in the Fig 13. In the case of existing system throughput of about 46% is achieved whereas in the proposed system higher throughput of about 92% is achieved. This is achieved due the reduction in the delay.

4. CONCLUSION

The LAL protocol can achieve better network lifetime and energy consumption with reasonable storage capacity of data buffer. This is because, advantage of the location information by distributing the traffic load over WSNs, such that energy consumption and memory storage of the sensor node around the sink node can be relieved and the network lifetime can be extended. It also proposes energy-efficient clone avoidance by the determination of cluster head with increased throughput and the delay is reduced.

When a cluster head is cloned, base station becomes the verifier. Now that attacker cluster head will select any random key and attempts to authenticate. But the fake secret key will not allow the attacker node to have verified. In all the above attacks even if attacker tries to authenticate using different keys (secret fingerprints), it has to try surplus number of keys. Also rekeying mechanism changes the keys of the network for every verification process. Because key size is not much more it will not add large overhead on the network. This makes attacker node nearly impossible to guess the secret fingerprints of the nodes.

5. REFERENCES

[1]. Brooks. R, Govindaraju P.Y., Pirretti. M, Vijaykrishnan. N, and Kandemir M. T (2007), 'On the detection of clones in sensor networks using random key predistribution', IEEE Trans. Syst., Man, Cybern., vol. 37, no. 6, pp. 1246-1258**.**

[2]. Conti. M, Pietro R. D., Mancini. L, and Mei. A (2011), 'Distributed detection of clone attacks in wireless sensor networks', IEEE Trans Dependable. Secure Comput., vol. 8, no. 5, pp. 685-698.

[3]. Fadlullah Z. M., Fouda. M, Kato. N, Shen. X, and Nozaki. Y (2011), 'An early warning system against malicious activities for smart grid communications', IEEE Netw., vol. 25, no. 5, pp. 50-55.

[4]. Zhongming Zheng, Anfeng Liu, Lin X. Cai, Zhigang Chen and Xuemin (Sherman) Shen (2016),'Energy and memory efficient clone detection in wireless sensor networks',IEEE Transactions on mobile computing., vol 15 ,no. 5,