International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Network Security Enhancement in WSN by Detecting Misbehavioural Activity as Copy Cat Nodes

**Dr. B. R. Tapas Bapu[1], Hemavathi S U[2], Poonkuzhali K[2], Sweety J[2]**

[1]Professor, [2]UG Scholar,
[1,2]Department of ECE, S.A. Engineering College, Chennai, Tamil Nadu, India

**ABSTRACT**

This system proposes a centralized system for replica identification. The network is divided into segments and an inspection node is chosen for each segment. Inspection node identifies a clone node by checking the nodes ID and cryptographic key. In this process, Chord algorithm is used to detect the clone node, every node is assigned with random key, before it transmits the data it has to give its key which would be verified by the witness node. If same key is given by another node then the witness node identifies the cloned node. Here every node only needs to know the neighbor list containing all neighbor IDs and its location. In this scheme, Energy-Efficient Clustering Protocol (EECP) protocol is used to implement different energy saving methods.

***KEYWORDS:*** *Chord algorithm, Clone node, Cryptographic key, Distributed Hash Table, Wireless Sensor Networks, Witness Node.*

**Abbreviations:** EECP, WSN, DHT, SHA, RSA, MD-5

***How to cite this paper:*** Dr. B. R. Tapas Bapu | Hemavathi S U | Poonkuzhali K | Sweety J "Network Security Enhancement in WSN by Detecting Misbehavioural Activity as Copy Cat Nodes" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.1098-1103, URL: www.ijtsrd.com/papers/ijtsrd31257.pdf

**IJTSRD31257**

## I. INTRODUCTION

Wireless sensor networks (WSNs) have been viewed as an auspicious technology. Sensor nodes can sense external event and combine the sense statistics and transmit it. WSNs are applied in a wide variety of applications such as patient monitoring, military surveillance, ecological disorder nursing, the internal wildlife of sea monitoring, underwater mineral mining etc. Sensor nodes are engaged in unreachable area, they are susceptible to various attacks such as replication attacks. In this scheme, we emphasis on this harmful threat name node replication attacks using chord algorithm and different energy saving methods are implemented using Energy-Efficient Clustering Protocol (EECP). This protocol is used to give energy to the nodes after data transmission. An attacker physically seizure one or multiple original node and get all credential such as ID, cryptographic key, code, data, etc. The attacker can make clones with the seizure credential and insert them in its desired location within the network. These clone nodes have the same identity and confidential information from the legitimate nodes which might be treated as an original node and can take participate in network activities. In this scheme, we emphasis on this harmful threat name node replication attacks using chord algorithm based on Distributed Hash Table (DHT). Using MD5 algorithm, switching over will be take place.

## II. SYSTEM ANALYSIS

For cost-effective sensor placement, sensors are usually not tamperproof devices and are deployed in places without monitoring and protection, which makes them prone to different attacks. For an instance, a vicious user may compromise some sensors and collect their private information which can then replicate the sensors and deploy clones in a wireless sensor network (WSN) to launch a variety of attacks. This is referred to as the clone attack. Since replicated sensors have the same information, clone attacks have become one of the most critical security issues in WSNs. Thus, effective detection of clone attacks is important to ensure the healthy operation of WSNs that are vulnerable to the node clone for which several distributed protocols have been proposed.

## III. SCOPE OF THE PROJECT

The main objective of this project is to identify the clone node by witness node based on node ID, Random number with time stamp and location ID through Wireless Sensor Networks (WSN). The goal of this project is to identify the clone nodes of user by using witness node between transmission. The witness node looks for the cloned node in the network. If such cloned node is not found, the system continues transmission. If clone is found the data transmission will be terminated. Hence the robustness of the network is improved.

### A. Related works:

In this project, chord algorithm is implemented to send the data in a more secured way. This algorithm is based on the Distributed Hash Table (DHT) which contains the information of all nodes in the network. Here, when the user sends any data, the information is first verified by the witness node which contains the Distributed Hash Table and then sent to the other user. After the verification is done, if the witness node finds any mis behavioral activity, it identifies as clone node and the data will not be sent.

### B. Proposed system:

In the modification process, the first one is based on a distributed hash table (DHT) in which Chord algorithm is used to detect the cloned node where every node is designated with the unique key and before it transmits the data it has to give its key which would be verified by the witness node. If any other node gives the same key, then the witness node identifies the cloned Node where every node only needs to know the neighbor-list containing all neighbor IDs and its locations. This is done by Chord Algorithm, by location-based nodes identification, where every location will have a group leader that generates a random number with time stamp to the available nodes in that location. Witness nodes verify the random number, time stamp and the encrypted message to detect the cloned node. Due to the energy limitation of sensor nodes, perpetuating lifetime of wireless sensor networks (WSNs) is a big challenge. This challenge becomes even more critical in large-scale sensor networks, which consumes more energy because of more data collections and packet transmissions. It is believed that clustering-based protocols are the best choice for such kind of WSNs. To designed the Energy Efficiency Clustering Protocol partition into a large-scale network into separate clusters. Based on this clustering scheme, different energy saving methods are proposed such as efficient cluster head and relay selection based on the some of the parameters like throughput, network lifetime, energy consumption, time consumption, sensor node lifetime, end to end delay, jitter, packet delivery ratio which is much better than hybrid cluster connection for saving the energy efficient and distributed clustering in terms of both energy saving and packet collection rate to be presented.

### C. Advantages of proposed system:

- High security.
- Data integrity.
- Easily find the attacker.
- Energy consumption is reduced.
- Sensor node lifetime is increased.

## IV. ARCHITECTURE DIAGRAM

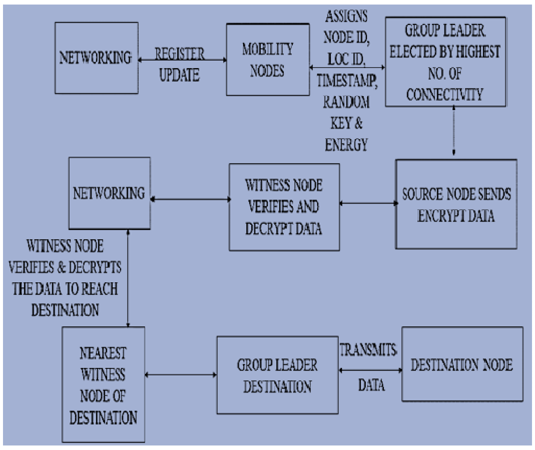

NETWORKING
REGISTER
UPDATE
MOBILITY NODES
ASSIGNS NODE ID, LOC ID, TIMESTAMP, RANDOM KEY & ENERGY
GROUP LEADER ELECTED BY HIGHEST NO. OF CONNECTIVITY
NETWORKING
WITNESS NODE VERIFIES AND DECRYPT DATA
SOURCE NODE SENDS ENCRYPT DATA
WITNESS NODE VERIFIES & DECRYPTS THE DATA TO REACH DESTINATION
NEAREST WITNESS NODE OF DESTINATION
GROUP LEADER DESTINATION
TRANSMITS DATA
DESTINATION NODE

**Fig.1. System Architecture**

In this system, whenever the user sends any data, the group id, sender id, group leader id, random number generated by group leader, Timestamp, predecessor and successor node id using chord algorithm, sender IP address and data in encrypted form will be sent to the witness node in encrypted form. The witness node will convert it to decrypted form and will send the details to the group leader for verification. If it is found to be a clone node the witness node does not send the data. Fig.2. also explains the work flow of the process is obtained. This diagram explains about how it detects the clone node. It also verifies energy whether it is able to become cluster head or not. If energy goes very low, then the node goes to sleep mode otherwise it is elected as cluster head and it is used to transmit the data to the destination.

### A. Data flow diagram:

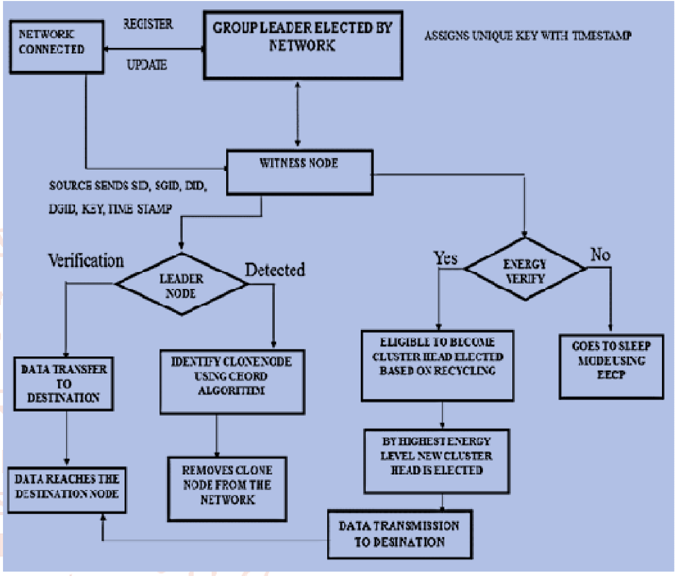

NETWORK CONNECTED
REGISTER
UPDATE
GROUP LEADER ELECTED BY NETWORK
ASSIGNS UNIQUE KEY WITH TIMESTAMP
WITNESS NODE
SOURCE SENDS SID, SGID, DID, DGID, KEY, TIME STAMP
Verification
LEADER NODE
Detected
Yes
ENERGY VERIFY
No
DATA TRANSFER TO DESTINATION
IDENTIFY CLONENODE USING CHORD ALGORITHM
ELIGIBLE TO BECOME CLUSTER HEAD ELECTED BASED ON RECYCLING
GOES TO SLEEP MODE USING EECP
DATA REACHES THE DESTINATION NODE
REMOVES CLONE NODE FROM THE NETWORK
BY HIGHEST ENERGY LEVEL NEW CLUSTER HEAD IS ELECTED
DATA TRANSMISSION TO DESINATION

**Fig.2. Dataflow Diagram for Clone Detection**

## V. MODULES

A modular design is used to reduce complication, promote changes, and for easier implementation by encouraging parallel development of different part of system. Modularity can be defined as single association of software that allows a program to be intellectually manageable. The modules of the proposed scheme are

- Network construction
- Node connection establishment from network
- Elected by group leader and using chord algorithm
- Witness node distribution
- Verification of random number
- Attackers detection and energy utilized on data transfer
- Performance evolution.

### A. Module Description:

**Network Construction:**

In the Project, mobile nodes are constructed to form a network which consists of ‘n’ number of nodes. Then each network to connect the nearest witness node to establish their connection and it also monitoring those bridge connections between network and witness node. The networks are monitoring for all the nodes and are sharing their information with each other network. Each network requests are sent into neighboring nodes based on covered area within the limitation of distance range. Then network group formed from their constructed.

**Node Connection Establishment from Network:**
Each mobile node is connected to send request neighboring nodes then node id, location id informed to their specific network. Then all the mobile nodes are registered to network and that network monitoring and assigning some verifying details to their mobile nodes via network specified. For this purpose, to create the list of the neighboring nodes information for each node so that witness node can easy to track and verify based on nodes request.

**Elected by Group leader and using Chord Algorithm:**
In this module, it can verify the total number of connectivity nodes of each neighbor nodes information of the Requested Node like Predecessor Node Id with key and Successor Node Id with key using Chord Algorithm. These are verifying the highest Node Id's and Location Id's then we can detect the group leader. For this purpose, we have to create the list of the Neighbor Nodes information for each node so that the Witness Node can verify the nodes request and track the cloned node.

**Witness node distribution:**
Witness node is used for the verification process. In our project source node sends data to destination, first, its data goes to witness node then only data moves to destination. So, source node sends all its detail to witness nodes like source node id, source node group id, predecessor node id, successor node id, random key with time stamp, destination node id, and destination node group id with encrypted data (using RSA Algorithm). Then only witness node verifies all the details of the source node.

**Verification of Random Number:**
In this module, each node is assigned a random key with Time Stamp from Group Leader. Then the witness node will receive a Random key which was generated concerning that Time Stamp by the Group leader. Witness node will now check the Random number from the distributed hash table which is generated with the node information. If both the data are matched then the Witness node will confirm that this node is Genuine.

## VI. ALGORITHMS

### A. Chord Algorithm:

The algorithm used here is Chord algorithm. Identification of the key is the peak element in any peer to peer protocol. The Chord protocol does this efficiently in a distributed environment. It is evolved from a Distributed Hash Table (DHT). Every node knows its successor and predecessor nodes. It follows a circular architecture. Every node has its elements and key-value pairs on the hash table. Each of the elements of the node are hashed using Secure Hash Algorithm-1 (SHA-1). Using SHA-1 key identifier identifies the key and node identifier identifies IP address. In key-value pairs, the file name is hashed and the hash value is stored. The chord finger table is built for each node based on its size. It is built as the routing path of each node. When a query emerges, the node searches the query by sending request to each node in the finger table. In chord algorithm, stabilization protocol running periodically in the background. When a new node is added the nodes are stabilized by sending updates. To ensure correct lookup, all successor pointer and finger table must be up-to-date. Node addition and deletion does not take much time to stabilize the architecture. The operations performed in chord algorithm are

1. Start
2. Join
3. Delete
4. Update
5. Insert
6. Get.

### B. RSA Algorithm:

The RSA (Rivest-Shamir-Adleman) algorithm is the most widely used public-key encryption algorithm which is used for both public-key encryption and digital signatures. RSA algorithm is mathematically infeasible to factor sufficiently large integers which are believed to be secure if its keys have a length of at least 1024-bits.

**Key generation steps:**

1. Choose first two largest prime integers as p and q.
2. Compute n and Q(n) where n=pq and Q(n)=(p-1) (q-1).
3. Choose an integer e, 1<e<Q(n) where (greatest common denominator) gcd (e, Q(n)) =1.
4. Compute d,1<d<Q(n) where ed=1

- The public key is (n, e) and the private key is (n, d).
- The values of p, q and Q(n) are private.
- E is the public or encryption exponent.
- d is the private or decryption exponent.

### C. Energy-Efficient Clustering Protocol

In Energy-Efficient Clustering Protocol (EECP), initially, all the nodes are deployed randomly in equal percentage over the network and the network is divided into four sections in the form of zone A, zone B, zone C and zone D.

Total network area=area(A+B+C+D).

This protocol reduces the internal overhead and improves the energy utilization and enhancement of energy remaining in the network. Here Cluster Head is selected based on Node Quality Index which is the fusion of initial and currently available energy of the node. The fundamental Cluster Head solution applied for this protocol is

Boundary=boundary of network layout±10%
CHi= [boundary n (Qni>Avgi)].

### D. MD5 Algorithm:

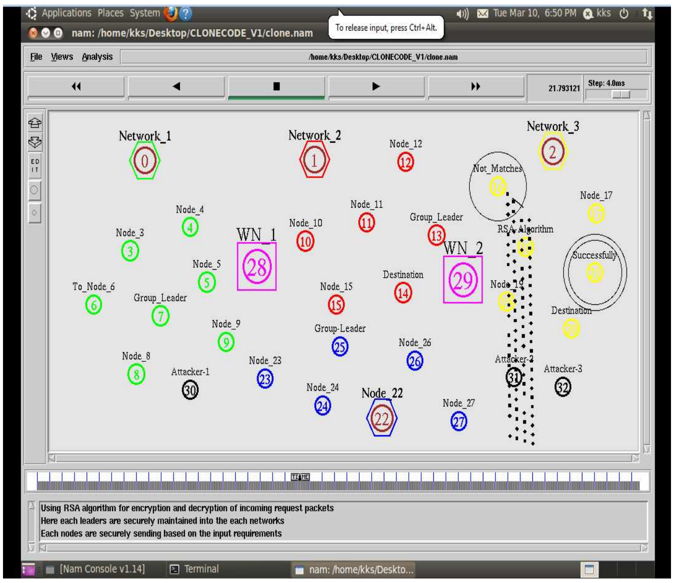
MD5 message digest algorithm is the fifth version of the Message Digest Algorithm and it is quite faster than any other Message Digest Algorithms which was developed to store one-way hash of a password. Here the user can compare the checksum of the downloaded file by pre-computed MD5 checksum of a file.

The 4 steps involved in this algorithm are

1. Append padding bits.
2. Append length.
3. Initialize MD buffer.
4. Processing message in 16-word block

## VII. OUTPUT

### A. PACKET DROP DUE TO CLONE NODE DETECTION:



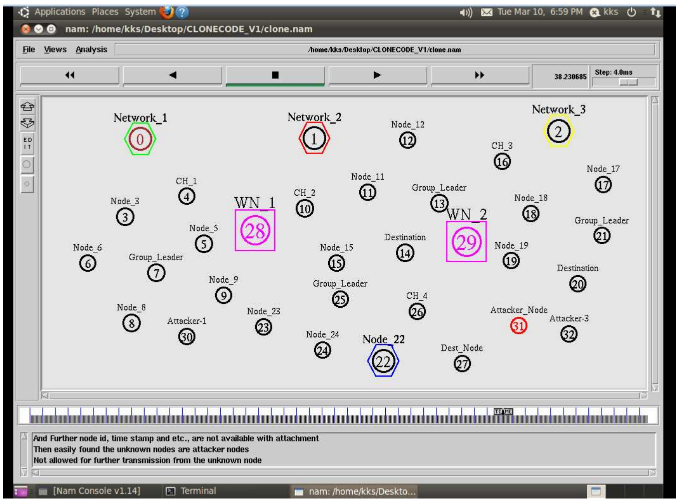
Using RSA algorithm for encryption and decryption of incoming request packets
Here each leaders are securely maintained into the each networks
Each nodes are securely sending based on the input requirements

**Fig.3. Packet drop due to clone node detection**

In the clone detection, group leader and witness node will play an important role to detect and enhance the network security. In this, the witness node is identified the cloned node using RSA algorithm and chord algorithm by verifying the sender id, group id, random number, group leader id and timestamp given randomly which was already given by group leader and hence the witness node will not allow the sender to transmits the data to the destination. Here the node18 in network2 is identified as clone node and hence the packet is dropped in node16 which will be a sender here and the data is not transmitted to the destination node. When the attacker node arrives with the worm file group leader identifies that attacker node and prevent from hacking the information from the sender node during transmits the data.

### B. ENERGY LOSS AFTER DATA TRANSMISSION:

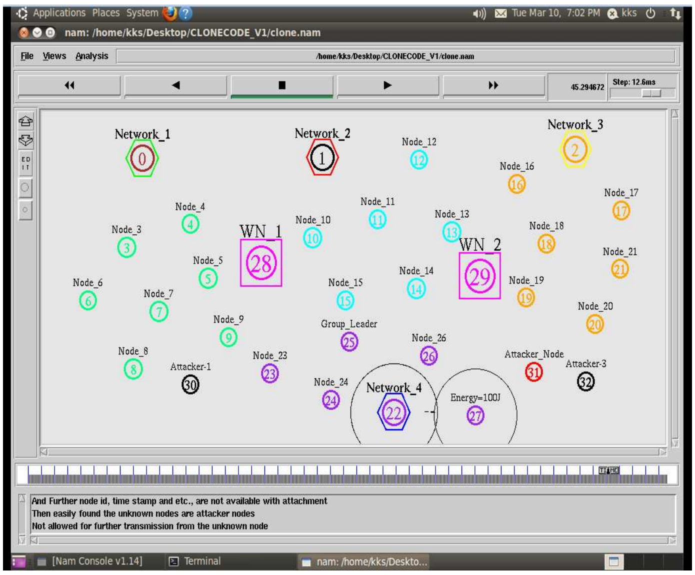
In these nodes are going to the sleep mode due to less energy and after data is transmitted from sender to receiver. Since the energy transfers take place via all the nodes. The black colour indicates the energy will be lost in the nodes.



And Further node id, time stamp and etc., are not available with attachment
Then easily found the unknown nodes are attacker nodes
Not allowed for further transmission from the unknown node

**Fig.4. Energy loss after data transmission**

### C. ENERGY DISTRIBUTION BY NETWORK:



And Further node id, time stamp and etc., are not available with attachment
Then easily found the unknown nodes are attacker nodes
Not allowed for further transmission from the unknown node

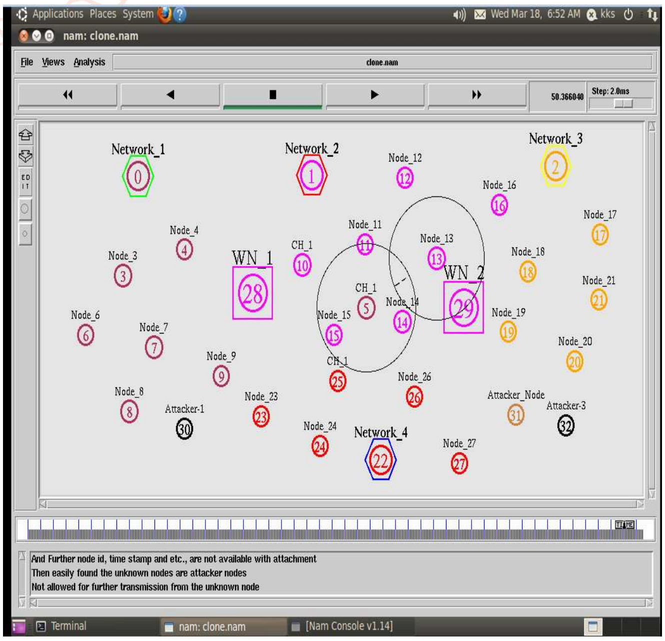
**Fig.5. Energy distribution by network**

Since the energy is lost for all nodes from each network energy will be given to the nodes. So the nodes will not go to sleep mode and will be active always which will enable the nodes to send the data again and again continuously. The coloured nodes represent the energy received by every node.

### D. SWITCHING OF THE NODE:

Switching of nodes represent the movement of the node from one network to the other network. When the switching is done the timestamp, node id and group id are verified by the witnessnode and then by the group leader of the network to which the node is moved. If the verification is succesful, the node enters the new network and registers itself in the new network and connects with all other nodes in that new network.

Here switching is shown by the node 5 from Network_1. The maroon colour node in the Network_2 represents that it is switched from Network_1 to Network_2.



And Further node id, time stamp and etc., are not available with attachment
Then easily found the unknown nodes are attacker nodes
Not allowed for further transmission from the unknown node

**Fig.6. Node switching**

**PERFORMANCE GRAPH:**

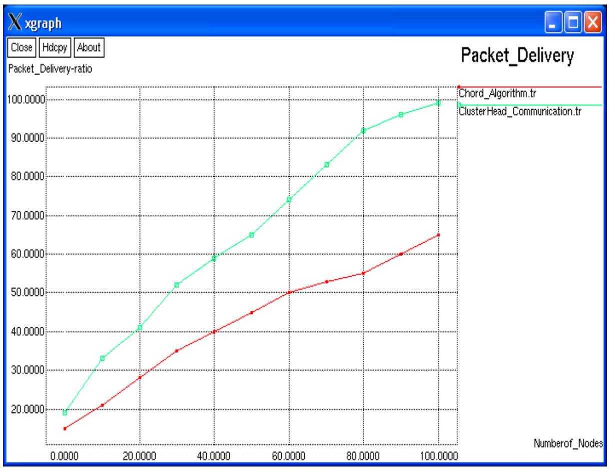


**Fig.7. Packet delivery**

In X-axis is the number of nodes and Y-axis is the Packet Delivery Ratio for the parameters are Chord algorithm performance are improved and increasing when Cluster head to Cluster head communication to be also increased. So, packet transmission is increased when improved the parameters in the secure cluster network.

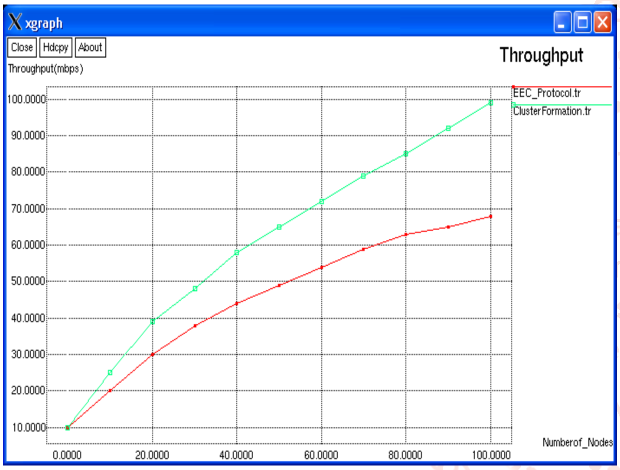


**Fig.8. Throughput**

In X-axis is the number of nodes and Y-axis is the Throughput (mbps) for the parameters are Optimization of energy efficient protocol along with cluster formation based on distance covered from the network location. There are increasing the throughput of packet transmission when using those parameters.

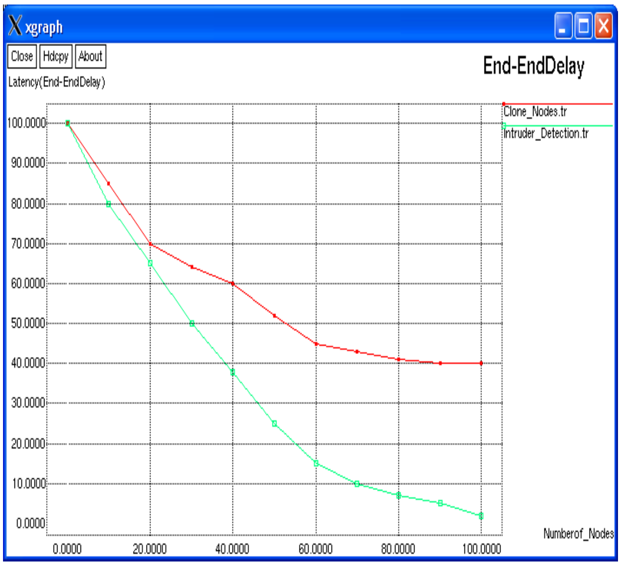


**Fig.9. End-End delay**

In X-axis is the number of nodes and Y-axis is the Latency (End-End Delay) for the parameters are decreasing when clone sensor nodes little bit reduced then also intruder detection of unknown nodes is too reduced from the cluster network and improve their cluster network lifetime.

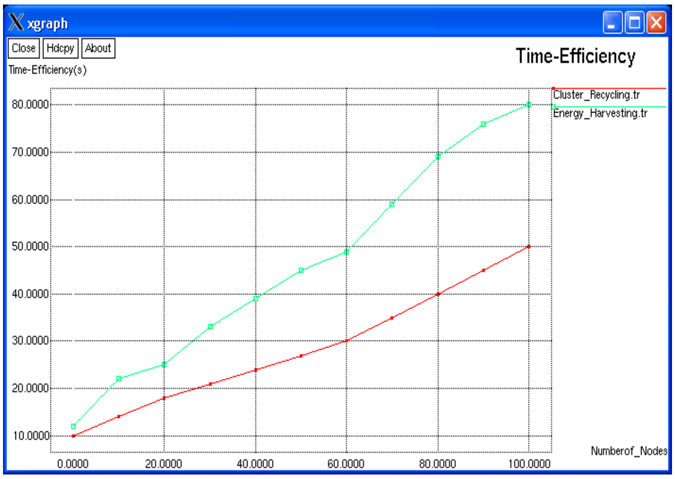


**Fig.10. Time-Efficiency**

In X-axis is the number of nodes and Y-axis is the Time-Efficiency(s) for the parameters are Energy-Harvesting to increasing the storage with time consumption when number of nodes is increasing and based on cluster recycling in the network for the cluster to cluster via network communication to be handled.

## VIII. CONCLUSION

Thus, the paper infers that through chord algorithm, time stamp verification and random number verification clone node will be identified. In this paper, a novel collision attack scenario against a number of existing IF algorithms have been introduced. Moreover, we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust but also more accurate and faster converging. In future work, an investigation on whether our approach can protect against compromised aggregators and implementation of our approach in a deployed sensor network may be done.

## IX. FUTURE SCOPE

In future more advanced algorithms can be used to enhance the speed where same computer needs to encrypt large data and different topologies can be used where the failure of one node does not affect the other.

**Conflict of interest:** The authors confirm that there are no known conflicts of interest associated with this publication of this paper.

## REFERENCES:

[1] A. More, V. Raising Hani, “A survey on energy efficient coverage protocol in wireless sensor networks,” Journal of King Saud University-Computer and Information Science, vol. 29, pp. 428-448, Oct. 2017.

[2] R. Sruthi, “Medium Access Control Protocols for Wireless Body Area Networks: A Survey,” Global Colloquium in Recent Advancement Effectual Researches in Engineering, Science and Technology, pp. 621-628, 2016.

[3] M. Ahmed, M. Salleh, M. I. Channa, "Routing protocols based on protocol operations for underwater wireless sensor network: A survey," Egyptian Informatics Journal, vol. 9, pp. 57-62, Mar. 2018.

[4] B. Parno, A. Perrig, V. Gligor, "Distributed detection of node replication attacks in sensor networks," IEEE Symposium on Security and Privacy, 2005.

[5] Ho, Jun-Won, Matthew Wright, Sajal K Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analusis," IEEE INFOCOM, 2009.

[6] Zhongming Zheng, Anfeng Liu, Lin X. Cai, Zhigang Chen, Xuemin Sherman Shen, "ERCD: An energy-efficient clone detection protocol in WSNs," Proceedings IEEE INFOCOM, pp. 2436-2444, April 2013.

[7] Lee-Chun Ko, Hung-Yuan Chen, Guan-Rong Lin," A Neighbor- Based Detection Scheme for wireless sensor networks against node replication attacks," International Conference on Ultra-Modern Telecommunications & Workshops, Oct. 2009.

[8] Meng X, Lin K, Li K, A note based randomized and distributed protocol for detecting node replication attacks in wireless sensor networks, In: Hsu C-H, Yang I, Park J, Yoe S-S, editors. Algorithm and architecture for parallel processing, lecture notes in computer science, Berlin, Heidelberg: Springer, pp. 559-570, 2010.

[9] Mouri Conti, Roberto Di Pietro, Luigi Mancini, Alessandro Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, vol-8, pp. 685-698, 2011.

[10] Wibhada Naruephiphat, Yusheng Ji, Chalermpol Charnsripinyo, "An Area-Based Approach for Node Replica Detection in Wireless Sensor Networks," 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 745-750, 2012.