Energy Efficient Wireless Sensor Network to Enhance Network Security by Detecting Clone Nodes

B.R. TapasBapu¹, V. Nagaraju², M. Ramesh³, S.K. Rajesh Kanna⁴, P. Sailaja⁵

¹Professor, Dept of ECE, S.A. Engineering College, India
²Professor, Dept of ECE, Rajalakshmi Institute of Technology, India
³Assistant Professor, Dept of ECE, Saveetha School of Engineering, India
⁴Professor, Dept of Mechanical, Rajalakshmi Institute of Technology, India
⁵Assistant Professor, Dept of IT, Velammal institute of technology, India

vankadarinagaraju@richtennai.edu.in

Abstract. For replica identification and clone detection a centralized system is proposed in this research, where the network has been separated into inspection node and segments. A clone node can be identified by checking the inspection nodes ID along with the Network security (Cryptographic) key. Detection of clone node done using Chord algorithm, where each and every node in the network have assigned with a unique key generated at random. Before the data transmission, it has been given with its key and the assigned keys have been verified for the cloned keys already assigned for some other nodes in the network by the witness node. Also the neighbor node ID and it locations have to be listed to those nodes. In this scheme, Energy-Efficient Clustering Protocol (EECP) has been used to implement different energy saving methods.

Keywords - Wireless Sensor Networks; chord algorithm; clone node; cryptographic key;

1. Introduction
In the modern world, Wireless sensor networks (WSN) have been noticed as a fortunate technology for the society, as it is having enormous pros in it ad has been used by majority of the real time applications. WSN has been linked with various sensor nodes and the sensor nodes can sense the surrounding environment, the obtained data statistics will be transmitted to WSN [1]. WSN having huge scope in the real time applications like agriculture, patient monitoring, aerospace, surveillance, military purposes, nuclear plants, ecological disorder nursing, wildlife monitoring, traffic control, under water surveillance, forecasting, mineral mining, etc. The WSN are commonly used to extract the data from the unreachable and the hazards areas from the sensors node, sometimes these sensor nodes in the unreachable area may vulnerable to numerous attacks. One such major attack is the replication attack i.e. name node replication [6][9]. This research is to overcome the attacks using chord algorithm and Energy-Efficient Clustering Protocol (EECP). This protocol is used to give energy to the nodes after data transmission. The WSN structure is having numerous sensor nodes and is adaptable to include any number of nodes in it. Also the WSN nodes can be accessed by the node ID, cryptographic key, etc. So any attackers with the key or ID can able to access the network and can manipulate the network data. Once the attackers physically seized the any of the original node in the WSN, attackers can easily get the required credential and permits. With those credentials, the attackers can formulate the clones for the nodes and include them in desired accessible locations within the network. Attackers used to create the clone nodes with similar identity and...
incorporate the seized confidential information data to make the cloned node to be the legitimate nodes in the network. Thus the WSN might be treating the cloned nodes as an original nodes and allow those cloned nodes to take part in all its network activities. In this case the attackers can manipulate the data or mislead the network interpretations. So a need arises to secure the WSN from the attackers. In order to solve this issue of hacking the nodes, in this research, chord algorithm based on Distributed Hash Table (DHT) had been implemented to overcome the harmful threat name node replication attacks.

2. System Analysis
In the common WSN application, the sensors used are off economical and cost-effective in nature, also those sensors have been installed in the remote locations with lack of monitoring and protection. Also most of those sensors may not have tamper proofing or locking devices, as the sensing will be disturbed. These type of tampering and the locking mechanisms for safe guarding the sensors done only for the high security WSN, which costs very high. This pitfall in the unprotected sensors paved the way for attackers to hack the sensor and able to read the required credentials. A vicious user may hack the sensors located in the remote and unprotected locations to collect their confidential information. With the hacked information, the attackers can replicate the similar sensors and deployed clones into the corresponding wireless sensor network (WSN). This type of cloning the sensors and included into the WSN is called as clone attack. Since the replicated sensors created by the attackers also have the similar information and keys, so the clone attacks become a great threat for the WSN. Thus, a need arises for effective detection of clone attacks and preventing the WSN from the clone attack to safeguard the network and data.

3. 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 WSN. The primary aim of this research is to recognize 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.

Related works: In this research, chord algorithm has been implemented to transfer the data within the WSN in a more secured approach. This developed 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 initially certified 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.

Proposed system: In the modification process, the primary one is developed based on the distributed hash table (DHT) and Chord algorithm for detecting the cloned node, if any in the network. This is achieved by assigning unique key for each and every node in the WSN. This assigned key should be allowed to be verified by the witness nodes. If the witness nodes didn’t recognized any replication or duplication of the same key, then the developed module will allow the sensor nodes to send or transmit the data within the WSN as programmed. On the other hand, if any of the nodes in the network provides the same key or ID, then the witness node recognize that nodes and categorize as the cloned nodes. Also every node in network needs the details of the neighbor nodes and the IDs and locations, which is essential for the data transfer and communication. This have been done by the Chord Algorithm in this research, in this methodology, entire WSN segregated the sensor nodes based on the locations. Each category of the sensor nodes within the WSN have been assigned with the master node or leader node. These location group leader nodes can equip to breed random numbers along with the time stamp and geo details. This
generated random key will also be communicated to the nearby nodes in the location or to the nodes in the same category. Once all the group lenders generated and communicated all the random numbers to all the available nodes within the category, the WSN triggers the witness nodes. The duty of the witness node is to verify and authenticate the provided random values for each and every node along with the time stamp values. Also the witness nodes encrypted the message in the sensor nodes to detect the cloned node. Thus any cloned node available in the WSN can be detected and segregated from the WSN. Another major challenge faced by the WSN is the energy limitation for the sensor nodes and the extending lifetime of WSN. A the size of the network increases, the complexity of the challenges increases proportionally, i.e. as the network size increases, the number of sensors and the transmission devices increases, which requires more energy proportionally. In order to overcome the issue, clustering-based protocols are being used by many of the WSNs. In this research, Energy Efficiency Clustering Protocol partition have been used into a largescale wireless network, such as efficient cluster head and relay selection based on the some of the parameters like throughput, end to end delay, network lifetime, energy consumption, time consumption, sensor node lifetime, jitter, packet delivery ratio which is much better than hybrid cluster connection. The various advantages of the proposed system are High security, Data integrity, easily find the attacker, Energy consumption is reduced, Sensor node lifetime is increased.

4. Architecture Diagram

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 architecture diagram is given in the Figure 1.

![Architecture Diagram](image)

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. 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.

**DATA FLOW DIAGRAM:**

The data flow diagram of the deelope model is given in the Figure 2.
5. MODULES

A modular design is used to reduce complication, promote changes, and ease in implementation. This has been achieved by boosting parallel improvement of diverse part of system. Modularity can be defined as single association of software module that permitsthe developed program to be holistically controllable. 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

5.1 Network Construction

In this research, mobile nodes are constructed to form a network which constitutes ‘n’ number of sensor nodes. These nodes in the network have to be connected to the nearest witness node. Thus a communication link had been developed and it has also been used to monitoring those network and witness node bridge connections. The developed network module network, all the sensor nodes, information sharing within the network have been monitored completely. Each element in the network sends required requests to the neighboring nodes available within the segregated categories of the nodes Then network group formed from their constructed.

5.2 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. To execute the activity and to reduce the complexity in validating the nodes, the details of the neighboring nodes will be created and based on the list of neighboring nodes, information have been validated by the witness node. Thus it became easy to track, monitor and verify the originality of the nodes based on request.
5.3 Elected by group leader and using chord algorithm
In this module, chord algorithm has been used for verifying the nodes and the all the connectivity nodes. In this logic, each and every neighbor node information like ID, key, etc have been verified. Also the predecessor and successor node Id along with the key value of the requested node have been collected for verification. Group leaders are identified for each segments of the nodes in the WSN, for that the highest node Id's and Location Id's have been identified. In order to achieve it, it has been created the information list of the neighbor nodes for each and every node, thereby the Witness Node can easily validate the requested nodes and able to recognize the cloned node.

5.4 Witness node distribution
Witness nodes in this WSN have been used to verify and validate the sensor nodes at the time of request made by the sensors node. To achieve this process, in this research, the data transfer have been designed such a way that, any information requested by any of the node in the network, then that information will be extracted and those information will be send to the witness node. Once the witness node identifies that the node is not the cloned node, then the information transferred to the requested node. So by this mechanism of transferring information from the source node to the witness node and then to the destination node avoids the attackers from data hacking. Further to enhance the security, in this research, information such as source node group id, source node id, predecessor node id, random key with time stamp, successor node id, destination node group id, location tag, destination node id and with RSA Algorithm encrypted data.

5.5 Verification of random number
In this random number verification module, initially all thenodes have been allocated with a random key along with the geo tag time stamp by the group leader. Then the same data have been sends to the witness node immediately by the group leader. Witness node will now ready to validate the nodes in the network, in order to reduce the validating complexity, the witness node generates the distributed hash table, in which the random numbers, keys, time stamp and all other information gets appended. At the time of validation, the witness node checks the data received form the source or requested node with the data in the hash table, any mismatch leads to the assumption that the node is a non-genuine node. Thus the witness node validates the source node in the network for its originality.

6. Algorithms
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.

**RSA ALGORITHM:**
It is one of the commonly used algorithm by the researchers for the purpose of public key and digital signatures. RSA algorithm is mathematically infeasible to factor sufficiently large integers which are supposed to be protected safely for the minimum key length of 1024-bits.

**STAGES OF KEY GENERATION:**
1. Select first 2 largest prime integers and assign them to the variables p and q.
2. Calculate the values for n and Q(n)
   - n = p x q
   - Q(n) = (p-1) x (q-1)
3. Select an integer for e, such that it satisfy the equation 1 < e < Q(n)
   - where (greatest common denominator) gcd (e, Q(n)) = 1.
4. Compute d, 1 < d < Q(n)
   - Whereas, ed = 1

• (n, e) and (n, d) are the public and private key respectively.
• p, q and Q(n) are private values.
• E is the encryption exponent.
• d is the decryption exponent.

**ENERGY-EFFICIENT CLUSTERING PROTOCOL:**
In Energy-Efficient Clustering Protocol (EECP), in the beginning, entire nodes in the WSN have to be assigned with random key values in identical percentage and the entire WSN has to be segmented into four sections i.e. zone A, B, C and D. Thus the total area of the entire network will be sum of all the areas of the zones. \( A_{network} = \sum \text{Zone area}(A, B, C, D) \). 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 combination of initial and presently available energy of that particular node. The fundamental Cluster Head solution applied for this protocol is

\[ \text{Boundary} = \text{boundary of network layout} + 10\% \]
\[ \text{Chi} = [\text{boundary n (Qn)} > A_{\text{avg}}] \]

7. **RESULTS and DISCUSSION**
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. It is given in the Figure 3.
ENERGY LOSS AFTER DATA TRANSMISSION:

Energy loss after data transmission is shown in Figure 4. 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.
Energy distribution by network is shown in the Figure 5. 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.

In the Figure 6, 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.
In Figure 7, 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.

In Figure 8, 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.

In Figure 9, X-axis is the number of nodes and Y-axis is the Time-Efficiency.
In Figure 9, 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.

8. CONCLUSION
Thus, the paper infers that through chord algorithm, time stamp verification and random number verification clone node will be identified. In this research work, aninnovative collision attack statebeside a number of prevailing IF algorithms have been attempted. Furthermore, it has been proposed enhancements for that IF algorithm, by means of implementing an initial estimate of the trustworthiness of sensor nodes. These developed methodologies strengthen the algorithm for collusion robustness and also reinforce for more accurate and faster convergence. In future, protection against compromised aggregators can be developed and implemented.

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 analysis,” 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.