Resolving Based Low Storage Clone Detection for Secure Data Transmission in Wireless Sensor Network

[1]Dr.C.BalaSubramanian, [2] R.Saranya [3].S.Priya,[4].M.Alisha Banu
[1]Professor,[2,3] Assistant Professor,[4]PG Scholar
[1,2,3] Department of Computer Science and Engineering, P.S.R.Engineering College
4 Department of Computer Science and Engineering, PSR Rengasamy College of Engineering for Women,

ABSTRACT: Secure communication in WSNs is important because information transferred in the networks can be easily stolen and hack or replaced. LSCD is a approach used to detect cloned nodes and without recovering from the cloned node information. Clone estimation algorithm is used to recover the original information from the cloned nodes and leads to a successful communication.. Clone detection is processed in a nonhotspot region where a large amount of energy remains, which can improve energy efficiency as well as network lifetime. Wide simulations and demonstrate that the lifetime of the storage requirements, and then detection probability of our protocol are substantially improved over competing solutions from the literature**.**

IndexTerms: **Clone detected, distributed route protocol, network and lifetime, wireless sensor networks (WSNs) security.**

I.INTRODUCTION

A wireless sensor network (WSN) is a collection of nodes prepared into a helpful to the network. Each node consists of giving out ability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver therefore (usually with an the single Omni-directional antenna),and have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes converse wirelessly and often self-organize after organism deploy in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated.

Such the systems can be transform to the way of we live and work. Currently, WSNs are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with WSNs with access to them via the Internet. This can be the deliberate as the Internet fetching a fabric network. This new technology is exciting with infinite potential for frequent application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

Know the paper follows the new approach such as the clone estimation technique using to recovering the information that means to resolver node in the simulation time so that resolving node perform by the all actions. know that resolving node do that the process is continuously watching the cloned node in the network formation time. Then that time the original and cloned node activities are monitoring the in this resolving node.

In this resolving node continuously watching the that two node activities then the activities based to estimate the clone nodes and remove from the cloned nodes and then get original information that time, in this process done by the clone estimating algorithms, and then further action performed by using the Trust based mechanishm.In the mechanism using to send the original information from source to destination.

II.RELATED WORK

WSNs can be the deploy in unkind environments in to fulfill both military and civil applications. Then Due to their in service nature and they are often unattended, hence prone to different kinds of novel attacks. For instance, an attacker might imprison nodes and acquiring all the information are stored therein—sensors are commonly assumed and to be not tamper-proof. The opponent may be the replicate or captured sensors and then deploy them in the networks to open a selection of the hateful activities. And then this attack is referred as the clone attack.

The wireless sensor networks are either static else dynamic. In dynamic WSN, is the location of the sensor node and to changes and as the nodes are the mobile. In a static of the `wireless sensor network, are once the sensor nodes are deployed and then in one position, and it remains the same and does not change of the cloned nodes. The cloned node detection in the static of wireless sensor networks and then it can be carried out of the using centralized approach or distributed approach manner. In centralized approach manner, a node is to present at the centre of the network and which is it is responsible for all the activities in the network. Then, In distributed approach manner, [3] all the nodes are the equally responsible to for all the activities and then to perform activities and then in a distributed manner.

In wireless sensor networks are, [6] the follows as the SET protocol and to performs in the centralized manner and to detects cloned nodes and then to dividing the network area and into exclusive of the subsets. And then each subset will contain the subset of leaders and members. And the members of the subsets are at a distance of the one hop is away from the subset of the leader. The subset of leaders are collects and then subnet member's are information and forwards are it to the root of the sub-tree.and In distributed approach is says, that [2] the identity the of each and every nodes are shared in the distributed manner. and During data transmission time, every nodes are collected the information about it's the neighborhood along with the its location and then broadcasts it in this network. The Low Storage Clone Detection technique (LSCD) protocols are [4] has the increased probability for the identifying of the cloned nodes in the network

and The information's are not directly transferred to the witness node but it is an arc form around the sink nodes and the data is to passed in the one hop neighbors. In the clone detection stage, the several clone detections are routes and originated from the sink node and then which is compared with the other witness path to identify the cloned nodes in the networks.

2.1 Existing system:

A cloned node has to attack of the information's, and it may be the contributes into the networks and operations in the same way as an uncompromised node; and hence, cloned nodes can launch a diversity of attacks. Similarly, data transmission within the network has become difficult due the various kinds of attacks. And the lifetime of the sensor nodes is another threat to Sensor networks.

The main objective is to efficiently identifying the cloned in the WSN with respect to successful data transmission. And to provide an efficient and secure way to transfer data between sensor nodes.

2.2 Proposed system:

It is recovered using a recovery node present in the same network. Each and every node in the network will have a recovery node and the recovery node for each node will be different for each round of transmission. If a cloned node is identified in the network, the neighbor node notifies the recovery node of the cloned node. The recovery nodes check the cloned node for all its functions and properties.

III. FLOW MODEL OF DATA TRANSMISSION

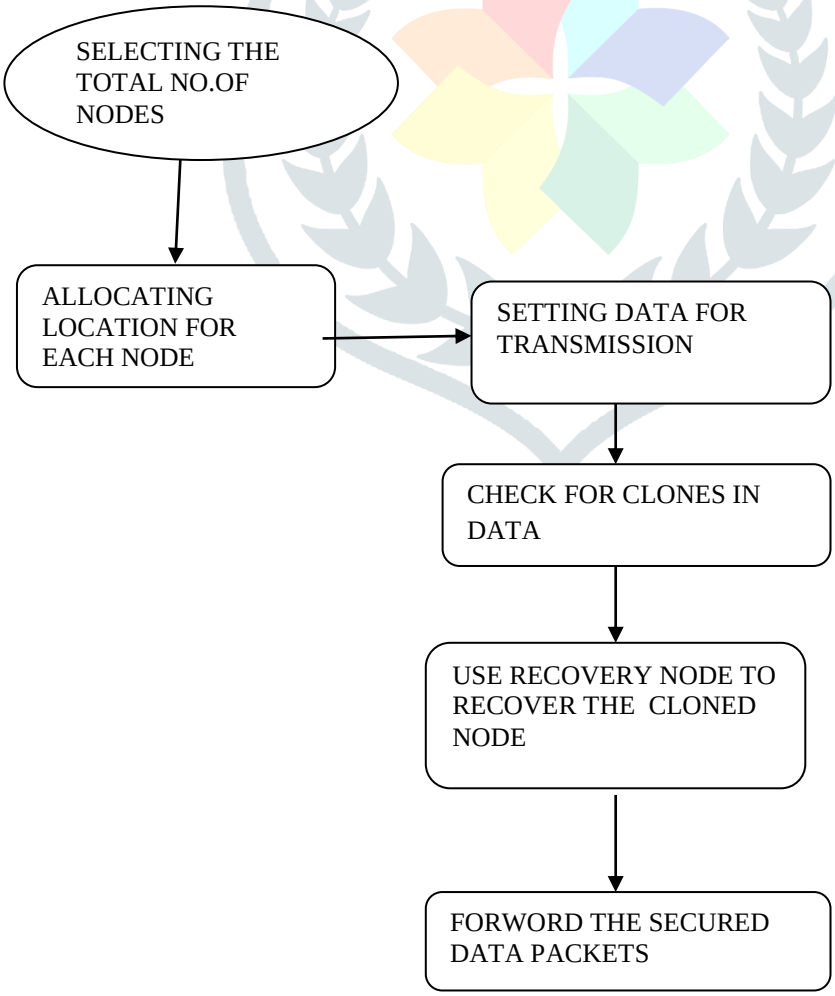

Fig3.1SYSTEM DIAGRAM

3.1SIMULATION PARAMETER SETUP:

IV. IMPLEMENTATION:

4.1. Network Formation

The total number of the sensor nodes in the networks are varies depending upon the purpose of the network. And then Each node will be placed in geographic locations to keep in track of the environmental changes that occur in the network. All the activities in the network are performed in a distributed manner. Each and every node will have a specific ID and unique location that is known only to that particular node and its witness node

4.2. Communication or Exchange of Data between the Sensor Nodes

The similar data are reduced to one by applying a Clone Estimation algorithm. The sensed data has to be exchanged between sensor nodes to perform the network activates successfully. Therefore, the sensed data is checked for total number of clones present in the sensed and collected data

4.3 Identifying the Cloned nodes

In this section, the cloned nodes present in the network are identified. The cloned nodes are not easily identifiable. The cloned node present in the network will observe all the network activities and report it to the adversary. The cloned node can be identified during exchange of information between the sensor nodes. The SLSCD algorithm is applied to the during transmission of the sensed data packets. The cloned nodes are identified by a trust-based authentication mechanism. Using this method, during transmission of packets from source to destination node, the intermediate nodes take part. While passing the information via., intermediate nodes there are possibilities of cloned nodes to be present in the intermediate node.

4.4 Recovering the Cloned Nodes

If any cloned node is present in the intermediate nodes. It is recovered using a recovery node present in the same network. Each and every node in the network will have a recovery node and the recovery node for each node will be different for each round of transmission. If a cloned node is identified in the network, the neighbor node notifies the recovery node of the cloned node. The recovery nodes check the cloned node for all its functions and properties.

4.4.1 cloned nodes algorithm:

While i</r
Let b record Xa;
b ← NextNodeOnSameHop(b), i ← i + 1;
end while;
Random walk ε3 hops to node a; a.tag = true
node a routing reverse sink to a with broadcast Xa;
whilea.hop= 2
a ← NextNodeOnLeastHop(a); Broadcast Xa;
end while;
//clone;
While a ←Next Node (a);
Next Node (ID, loc)! =true;
Then,
Start resolver;
Resolver R;

end if;

V.PERFORMANCE ANALYSIS AND RESULTS

The proposed methodology is implemented into NS2; the performance of the SLSCD protocol is the WSN environments are simulated and thus the succeeded in identifying of the cloned node with uppermost likelihood of clone detection. The figure-1 represents the graph of generated from the values obtained from the networks with different scales.

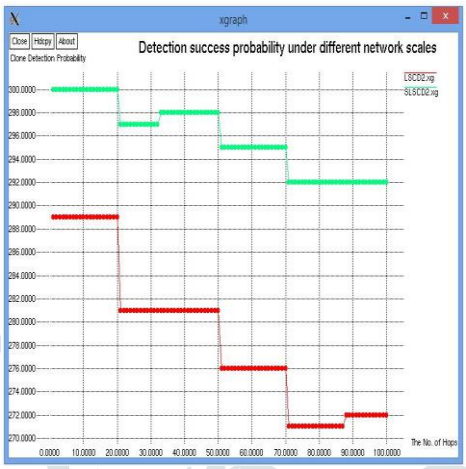

Fig5.1. CLONE DETECTION PROBABILITY

The figure-2 represents by the comparison of low energy consumption by the proposed system of the existing approach.

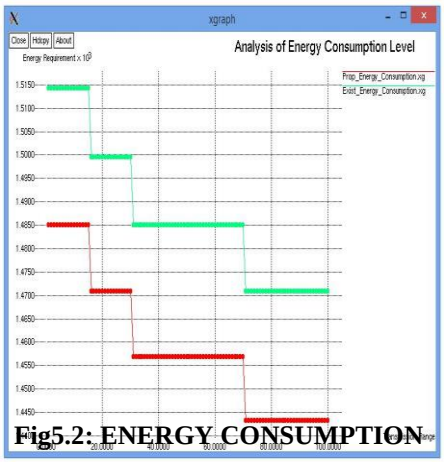

Fig5.2: ENERGY CONSUMPTION

The figure-3 represents as the comparison of the average delay and with speed of the data packets release. It shows that the delivery of data packet delay reduce as the speed increase.

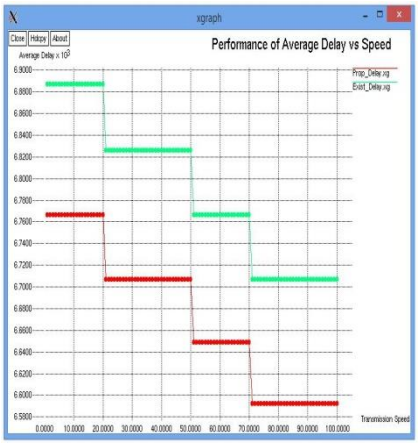

Fig5.3: DATA TRANSMISSION SPEED

The figure-4 those are represents as that the storage requirements under different network scenario i.e., with different network nodes and nodal degrees have been reduced when compare with the earlier proposed methods. This is due to the transmission of data packets by eliminating the similar data set. And also, the information about the source and destination nodes will node is stored anywhere in the network.

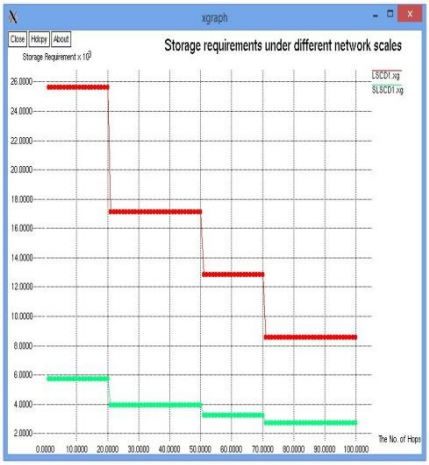

Fig5.4: STORAGE REQUIREMENTS UNDER DIFFERENT NETWORK SCALES

VI. CONCLUSION

The novel method to detected and the cloned nodes and the WSN and then to recovering the cloned nodes using a recovery mechanism approach was introduced. Thus, the proposed methodology shows that the increased probability of detecting the cloned nodes. And It also provides security to the data packets to sent by encryption of the packets after that eliminating number of clone nodes are present in the networks are analyzed data. Thereby, the reducing storage requirements and then utilizing minimal energy for all its activities and it which improves the lifetime of the network

REFERENCES

[1] A. Liu, X. Jin, G. Cui, and Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," Inf. Sci., Vol. 230, pp. 197–226, May 2013.

[2] C.M.Yu, C.S.Lu and S.Y.Kuo,"CSI: Compressed sensing based clone identification in sensor networks" in proceedings of the IEEE International conference on pervasive computing and communications workshops, pp. 290-295, March-2012.

[3] Dong, Kaoru Ota, Laurence T. Yang, Anfeng Liu, and MinyiGuo, "LSCD: A Low-Storage Clone Detection Protocol for Cyber-Physical Systems" Mianxiong, IEEE Transactions on Computer-Aided Design of Integrated Circuits And Systems, Vol. 35, no. 5, May 2016.

[4] Hesiod Choy, Cancun Zhu and T.F.La Porta," SET: Detecting Node clones in Sensor Networks", Proc of 3rd International Conference on Security and Privacy in comm...Networks (Secure Comm) pp. 341-350, 2007.

[5] Jun-Won Ho, Dogging Lin, Matthew Wright, SajaiK.Das "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks", Preprint submitted Elsevier, March 2009.

[6] KaiXing,FangLiu,XiuzhenCheng,DavidH.C.Du," Realtime Detection of clone attacks in Wireless Sensor Networks", IEEE ICDCS 2008.

[7] L. Jiang, A. Liu, Y. Hu, and Z. Chen, "Lifetime maximization through dynamic ring-based routing scheme for correlated data collecting in WSNs," Comput. Electr. Eng., Vol. 41, pp. 191–215, Jan. 2015.

[8] Mauro Conti, Roberto Di Pieto, L.V.Mancini and A.Mei,"A Randomized and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks ", Proc.ACMMobiHoc, pp. 80-89, Sept 2007.

[9] Wen Tao zhu, "Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme", International Conference on Network Computing and Information Security, pp. 156-160, 2011.

[10] Y. Liu, A. Liu, and Z. Chen, "Analysis and improvement of send-and wait automatic repeat-request protocols for wireless sensor networks," Wireless Pers. Commun., Vol. 81, no. 3, pp. 923–959, Apr. 2015.