International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 24 No. 1 Jun. 2016, pp. 46-56

http://www.ijisr.issr-journals.org/

DETECTION OF COLLUSION ATTACK IN WIRELESS SENSOR NETWORK USING RDE PROTOCOL AND CHORD ALGORITHM

R. Ramalakshmi[1], S. Subash Prabhu[2], and C. Balasubramanian[3]

[1]PG scholar Dept. of CSE, P.S.R.R college of Engg, Sivakasi, India

[2]Asst. Prof Dept Of CSE, P.S.R.R college of Engg, Sivakasi, India

[3]Prof. and head of CSE, P.S.R.R college of Engg, Sivakasi, India

ABSTRACT: Wireless sensor network consists of entity nodes that are able to work together with their surroundings by sensing or scheming corporeal parameters. The major issue in wsn is information accessed by unauthorized party by clone node. Once a node is captured, the attacker can reprogram and then take over the network process. The proposed algorithm is chord and DHT (Distributed hash table).The RDE protocol is used to detect clone node and chord algorithm provides the neighbor details. The DHT is used to store the node ID, key, location and source ID, destination ID. Here every node is assigned with a unique key which is verified by a witness node before transmitting data. A distributed detection protocol, known as randomly directed exploration (RDE), presents outstanding communication performance and minimal storage consumption for dense sensor networks. It is a location based node identification protocol. The group leader will be generating random number with appropriate location. Witness node are used to verify the random number detect the clone.

KEYWORDS: witness node, randomly distributed efficient, chord ring.

1 INTRODUCTION

The detection of collusion assault is the development of sensor node are deploy in the hostile environment. In this situation sensor node are easily compromised by the adversary. The compromised node can send false data of aggregator node. The collusion attack and clone node will be occurred.

Wireless sensor networks are used to detect the clone node. The clone node is detected by the adversary or witness node. The witness node is used to store the all node information. The information may not be matched packet can be dropped.

The node are used to some attributes are their source node id, destination node id, node location, key of each node, random num.

The information may not be matched packet can be dropped. Here advantage are the provide high security mechanism attackers can easily find out. The node does not perform any illegal activities and high time consuming.

The application of the wireless sensor network is disaster relief application, environmental control biodiversity, telematics, logistics and military applications.

To overcome energy and memory demanding by rapidly discover simulated nodes because many imitation nodes can multiply the damaged to the network.

Corresponding Author: R. Ramalakshmi

The characteristics of wireless sensor network are the fault tolerance, life time, scalability, quality of service. The fault tolerance is the each sensor node operates in a battery power. The communication will be failure they can be used to redundant node. The redundant node can avoid duplications. The redundant node is used to handle previous node.

The being moment in time of a sensor node can be used to growing performance and network life time and performance increased. The scalability is the process of some constraint based on the request no of a sensor node used to it. The quality of service is sensor node should be quality one and energy efficient. The fraction of time to send information to sink node. They can be used to check information will be send correct source or not.

The challenging task of wireless sensor network is the battery power radio transmission of control packet elimination. The data aggregation is the process of combining sensor data in order to reduce the amount of transmission in the network. The data aggregation reduce the data transmission improve energy and bandwidth.

The distributed processing algorithm is used to the central processing different node. The programmability is used to changeable during an execution .the maintainability is used to changes should be adopted.

The security requirements of the wireless sensor network is data confidentiality, data integrity, source authentication, availability. The data confidentiality is the process of whether information can be stored in the system protected against unauthorized access. The data integrity is the process of content will be modifying authorized users.

2 RELATED WORK

In this paper sensor node are deployed in the hostile environment the sensor node are divide into the cluster .The cluster can send information to base station. The each sensor is based on the distance of readings of such a sensor from estimate of correct value. The each sensor node can assign initial weight. The weight will be compared of each node which node will be lower weight that node act as a cluster head. The remaining node can send information to aggregator node. The cluster head send information to base station.

REPLICATION ATTACK

The S. Ozdemir presents “A arbitrary regimented and distributed approval of node repetition attack in wireless sensor network” one of the main problem in designing a protocol to detect the replication attacks is the selection of whiteness node.

Randomized efficient and distributed protocol is used to detect the node replication attacks. RDE is used to fixed interval time. Two steps of RDE protocol is location based prevision and id based prevision. The drawback of the randomized efficient protocol is used to overhead and data loss is high cheater would increasing misbehavior.

EXCLUSIVE SUBSET CONSTRUCTION

E. Ayday presents “astuteness node reproduction in feeler system” is used to exclusive subset maximal independent set is used to construct the exclusive subsets are formed in a distributed way in a network. The each of the subset will have a subset leader. The drawback of all reported subsets has a no clones. This will incur high communication overhead. The many attackers will be occurred.

EFFICIENT AND DISTRIBUTED DETECTION PROTOCOL

P. Laureti, presents “proficient and scattered detection of node reproduction attacks in mobile sensor networks” It is used to the two then there are two types of schemes are used to it. The EDD scheme is used to two steps online and offline. The SEDD scheme is used to tradeoff between storage overhead and time interval length is high.

The drawback of the sensor network it provides a less security. The data transmission time is high and communication failure occurred.

TOLERANT SECURITY MECHANISM

Roberto di pierto “locality based declaration the central point position tolerant security tool for wireless sensor networks” it is used to the LBK based neighborhood authentication scheme (LOCATION BASED KEY) is used to the find out the attacks.

Location based threshold endorsement scheme is used to the bogus data bogus data injection attack in which adversaries inject lot of bogus data into the network. The drawback of the attacker can cause the communication overhead.

DETECTION OF CLONE NODE

In this paper present a random key pre-distribution is used detect the clone node. This paper focuses an adversary captures a sensor node reprogram it and add multiple copies of node to the network. The drawback of the cloning gives the adversary an easy way to build an army of spiteful nodes that can cripple the sensor network.

3 SYSTEM DESCRIPTION

The secure data aggregation techniques used to tree topology. The tree topologies are used to type of network topology that includes at smallest amount three explicit levels in a topology pecking order.

A) Tree Topology
B) Setting up Network Model
C) Chord Algorithm
D) Witness Node Distribution
E) Verification of Random Number
F) Collusion Detection and Data Transfer

A) TREE TOPOLOGY

This involves variety of single nodes connected to central node. Each node in a ladder level has indicate to direct links with each neighbouring node on its below level. The drawback of the tree topology is used to entire system can be crippled by any damage or failure of primary node.

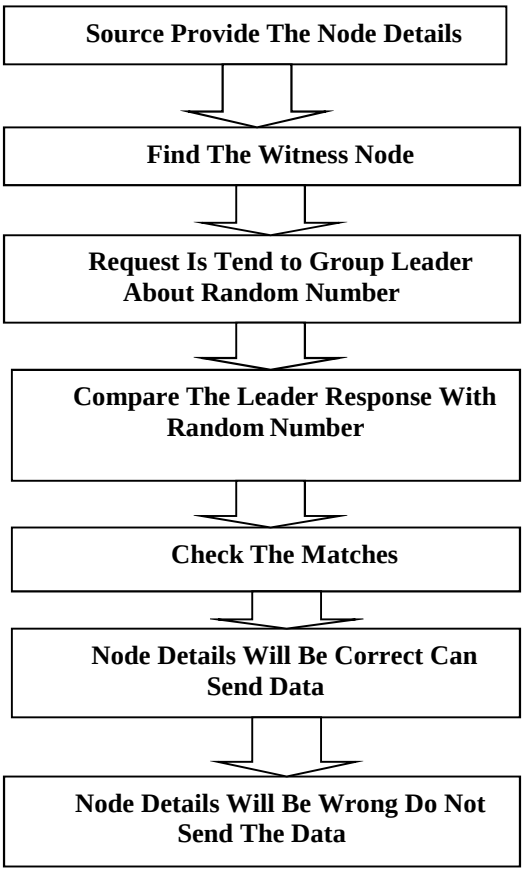


Figure 1: System Architecture

B) SETTING UP NETWORK MODEL

In this module sensor node consists of 'n' number of Nodes. So that nodes can request data from other nodes in the network. In a network, nodes are registered with the separate group then only group leader provide a node id for each node, so group leader also assigns random key with time stamp for all its sub nodes. Network is monitoring for all the nodes. Each and every one node is allocation there in sequence with each other's.

C) CHORD ALGORITHM

In this module we can verify the Neighbor nodes in sequence of the request Node like precursor Node Id with key and Successor Node Id with key using Chord Algorithm. These are verifying the Node Id's and Location Id's then we can detect the Clone Node. For this reason we have to generate the catalog of the Neighbor Nodes in order for each node so that the observer Node can confirm the nodes demand.

D) WITNESS NODE DISTRIBUTION

Witness node is used for verification process. In this module source node sends data to destination means first its data goes to witness node then only data moves to destination if one group to another group network process occurred.

So source node sends all its detail to witness node like source node id, source node group id, predecessor node id, successor node id, random key with time stamp, destination node id, and target node group id with encrypted data (using RSA Algorithm). Then only witness node verifies the details of the source node.

E) VERIFICATION OF RANDOM NUMBER

In this module, each node is assigned a key randomly with Time Stamp from Group Leader. Then the Group Leader will also transmit Random key which was generated with respect to that Time Stamp to the Witness node. Witness node will now check the Random number from distributed hash table which is generated with the node information. If both the data's are coordinated then the observer node will authenticate that this node.

F) COLLUSION DETECTION AND DATA TRANSFER

Only the Witness node confirms the Sender node, the data is send to the Destination, which is Genuine using RDE. If user specified information and the internal information are varied then the Witness node will identify that Cloning or some Mal practice has occurred and the Packets are discarded by the witness node.

4 IMPLEMENTATION

The detection clone in wireless sensor network using RDE protocol and chord algorithm. It is used to two types of techniques in proposed system.

A) Rde Protocol
B) Chord Algorithm
C) Distributed Hash Table

A) RDE PROTOCOL

The Randomly, Distributed, and Efficient (RDE) protocol for the detection of replica node attacks and we show that it is entirely suitable with respect to the requirements. General simulations also show that our protocol is highly efficient in transmission of data, luggage compartment, and processing speed, it has an improved attack detection probability compared to last techniques. And it is protective to the new attacks. RDE executes at fixed intervals of time.

In the first step a random value is to be generated; this random value can be broadcasted with centralized and distributed mechanism to all nodes. In the second step, each node digitally signs and locally broadcast its claim—ID and geographic location.

RED does not send the assert to a specific node ID because this kind of a solution does not scale well: A claim send to a node identification that is no more in attendance in the set of connections would be misplaced nodes deploy after the

foremost system exploitation might not be used as witness lacking update each nodes in network. However, RDE has ability to adapt to work when a specific node is used as the message destination. This is future to provide highly efficient announcement performance with sufficient detection likelihood for dense sensor networks.

In the protocol, to begin with nodes send claim communication contain a neighbor-list along with a most hop perimeter to arbitrarily selected neighbors; then, the consequent significance broadcast is synchronized by a probabilistic directed technique to approximately continue a line possessions through the network as well as to acquire sufficient unpredictability for better recital on communication and elasticity against opponent.

In addition, border determination mechanism is effective to further condense communication payload. During forward, in the middle of nodes recover out claim communication for node clone detection. By design, this procedure consume almost negligible reminiscence, and the simulations show that it outperforms all previous disclosure protocols in terms of communication cost, while the revealing possibility is acceptable.

B) CHORD ALGORITHM

Chord is an algorithm and protocol for a peer-to peer distributed hash table. A distributed hash table having key and value assigning it to different nodes. Function of Chord is assigning keys to nodes and discovers value for the key.

Chord algorithm is construction of the chord ring and localization of nodes [2]. By using Chord protocol, keys are arranged in a circle format has at most 2m nodes. Range may be varying from 0 to 2m-1. Chord [14] assign ID‘s to both keys and nodes from the same unsophisticated ID space.

The node trustworthy for key k is called its descendant, defined as the node whose ID the majority intimately follows k. The ID space veil of secrecy around to form a circle, so identification follows the uppermost ID. Chord require each node to keep a "manipulate board" contain up to *m* Chord requires each node to maintain a finger table containing up to *i*th entry of node *n* will contain the address of successor *(n+2i-1 mod 2m)*. Chord performs lookups in *O (logN)* time, where *N* is the number of nodes, using a for each swelling finger table of *logN* entries.

A node‘s manipulate board contains the IP address of a node intermediate around the ID space from it, a neighborhood-of-the-way, and so forward in power of two. A node forwards a query for key k to the node in its fiddle with board with the highest ID less than k.

The power-of-two organization of the manipulate counter ensures that the node can for all time forward the query in any case partially of the residual ID-space remoteness to k. As a consequence Chord lookups use O(logN) communication. Chord ensures correct lookups in spite of node failure using a successor list: each node keeps track of the IP addresses.

Randomness to make sure that Chord key and node IDs are distributed unevenly in ID space, balanced load along the nodes. Chord takes consideration over the key space present on node with help of virtual nodes. Every node participates in network with many ID of virtual node.

The Chord design is strength and correctness; even there is problems and failures. Chord is in use as a part of the investigational CFS [3] wide-area file store, and as part of the thread [1] resource come through system.

This allows a uncertainty to make incremental progress in ID space even if many finger table entry turn out to arrangement to given up the apparition nodes. The only situation in which Chord cannot assurance to find the in improvement be alive descendant to a key is if all *r* of a node‘s instantaneous descendant not succeed concurrently, before the node has a likelihood to acceptable its successor list.

Since node ID‘s are assign at random, the node in a descendant list are likely to be not related, and thus suffer independent failures. Small values of r (such as logN) make the possibility of on the spot breakdown vanishingly very small.

A new node n finds its place in the Chord circle by asking any present node to look-up n‘s ID. All that is obligatory for the new node to contribute accurately in lookups is for it and its antecedent to update their descendant lists. Chord has to check correctness even though nodes with same IDs join in the network.

New nodes and old nodes are have to be updated their tables. In the background, it is happening due to it is not used for performance. New node knows the data about successor and association flanked by them.

C) DISTIBUTED HASA TABLE

The DHT, by which a flattering decentralized, key-based caching and glance scheme is construct to grasp clone nodes. The protocol's performance on recollection expenditure and a important safety measures metric are hypothetically deduct through a likelihood model, and the resulting equations with indispensable fine-tuning for real submission, are support by the simulations. In accord with our scrutiny, the wide-ranging simulation results show that the DHT-based protocol can perceive node clone with high security level and holds strong confrontation alongside adversary's attacks.

DHT has competence to note combination of new node, malfunction of node and disentanglement in node. It is able to scale large number of node in network. DHTs build a transportation by which more multifaceted military can be handled. Services like disseminated file systems, Web caching, domain name services, multicast, instant messaging, content distribution systems peer-to-peer file sharing.

PROPERTIES OF DHT

1) Autonomy and Decentralization*:* The nodes together form the scheme lacking any middle management.
2) Fault tolerance*:* The classification must be dependable (in some sense) even with nodes participate, disconnect, and fading.
3) Scalability*:* The coordination should occupation resourcefully even with thousands or millions of nodes.

The basic supplies are that data be recognized using exceptional numeric keys, and that nodes be willing to accumulate keys for each other [2]. DHT has one important operation called key, which represents the IP address of the node. For implement DHT, following issues to be concerted.

KEYS TO BE MAPPED TO NODES

By using regular hash function nodes and keys are map in the arrangement of filament of digit. The digits are in binary arrangement in CHORD. The digits are in towering order base in CAN. Then given digit string is assign to node with adjacent digit string. It represents the node is the nearest to descendant.

FORWARDING A LOOKUP FOR A KEY TO AN APPROPRIATE NODE

The node that get key identifier can send it to node whose id is near to it. Thus adjacent concept is suited to this situation. For expressive these details, each node has table which contains in sequence about choose the adjoining node. If key ID is superior than the present node, then send it to node which is superior than present node. If it is slighter than key, then it is numerically closer. Then it holds key ID is smaller than current node ID. Otherwise, send to node where ID has ordinary key ID. Node has ID 8115 and a key has ID 8815, then forward to node 8365.

STRUCTURE OF A DHT

The structure of a DHT can be decayed into more than a few significant mechanism. The core part is an theoretical key space, which is 160 bit string as set. This possession is partition among the nodes in attendance in the system. It then connect the nodes in the system, and then they find their possessor.

CONSTRUCTING ROUTING TABLES

All nodes have to be familiar with the other nodes for distribution messages to other nodes. For receiving closer to the key ID, every node need to know its successor and it's ID. By noteworthy this only, the node able to propel message to descendant node. Afterward every node should be familiar with the corresponding identifiers. maintain the direction-finding table which contains the node connect and depart in sequence.

Algorithm 1: Detect replica node

1: **Procedure**: Initiator
2**: Broadcast**- exploit message
3: exploit message← {Nonce, Random seed, Action time}
4: specify transmission time in action msg for sending every claiming message
5: **end procedure**
6: **Procedure:** Observer
7: **Receive** exploit msg
8: **if** (msg nonce > last nonce) **then**
9: **check "**msg signature**"**
10: valid
11: Node operate as witness **then**
12: **Broadcast**: claim message
13: claim message←{Neighbor ID, Neighbor Location, witness ID, witness Location}
14: **intention node receives** claim message
15: **inspect claim message** (Destination act as an inspector)
16: **return** NIL (reach destination)
17: else if
18: forward msg to next node with Id
19: same ID at different Location
20: Inspector found clone and become a witness
21: **Broadcast** evidence message
22: evidence message ←cloned node {ID, Loc}
23: detect clone node
24: **finish procedure**

Algorithm 2: DHT using Random Key Distribution approach

1: **Input:** Detected clone node
2: Inspector become witness and detect clone node **(use Algorithm 1)**
3**: If** found clone **then**
4: Witness **broadcast** evidence msg← {ID, Loc, and Nonce}
5: insert keys to all nodes
6: Bloom filter← count the number of times the key is used
7: Inspector receives filter
8: verify the count within predefined threshold value
9: **if** (key value > threshold value) **then**
10: found cloned key
11: **else**
12: forward keys to next node with msg
13: **if** neighbor within the target zone **then**
14**: return** NIL (reach destination)
15: **if** no neighbor within the target zone **then**
16: onward msg to various in-between nodes
17: transitional act as spiteful node **then**
18: checker should not onward msg to that exacting hateful node
19: clone keys and nodes recognized by Bloom filter and witness
20: superintendent forward msg to correct node
21: **Output:** honorable broadcast of replica node in sequence.

5 PERFORMANCE ANALYSIS

The following metrics are employed for the performance analysis.

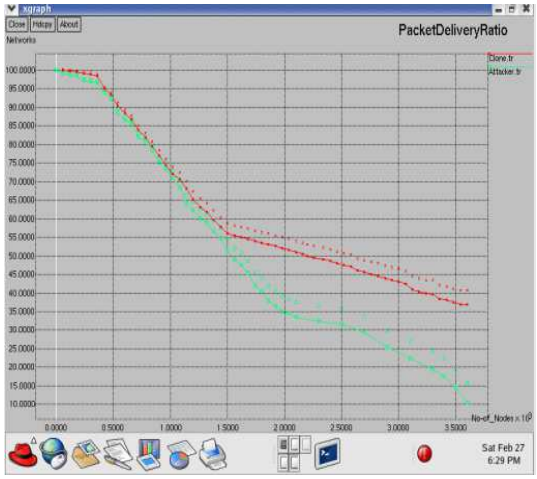
A) Packet Delivery Ratio
B) Throughput Analysis

A) PACKET DELIVERY RATIO

The Packet delivery analysis is used to very important factor to measure the performance of the network. The performance of these protocol is based on the depends on the various parameter. The packet delivery ratio is the total number of received at destination divide by the total number of seed packets. The performance is better and packet delivery ratio is high.

Table 1: Packet delivery ratio

S.No	No of Nodes (x-axis)	Packet Delivery Ratio (y-axis)
1	20	72.50
2	40	67.50
3	60	62.00
4	80	60.00
5	100	59.50



Screenshot 1: Packet delivery ratio

B) THROUGHPUT ANALYSIS

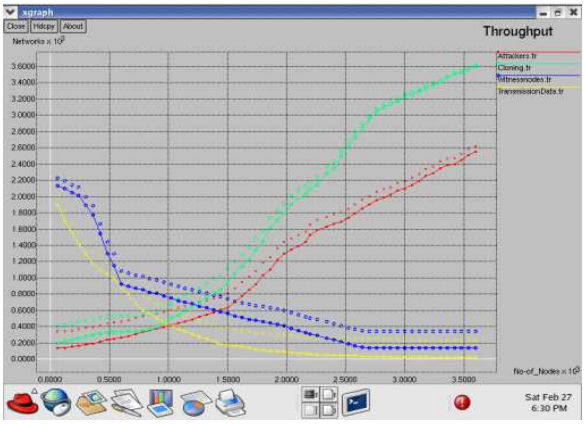
The average throughput is used to receive packet size divided by stop time and start time.

Average throughput = (received size) / (stop time – start time) *(8 /1000).

Where received size = store received packets, stop time = simulation stop time, start time = simulation start time.

Table 3: Throughput analysis

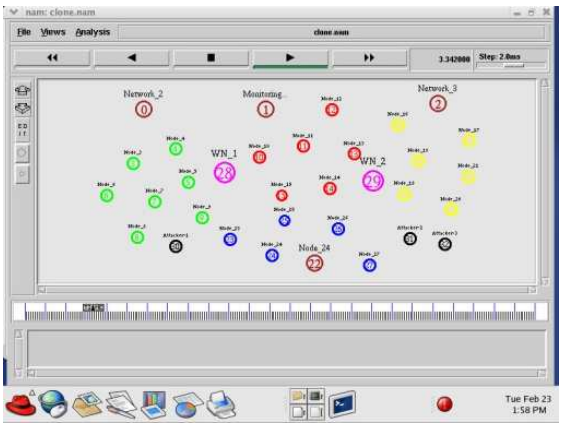
S.No	*No of Nodes (x-axis)*	*Throughput analysis (y-axis)*
1	*20*	1.78
2	*40*	1.62
3	*60*	1.53
4	*80*	1.45
5	*100*	1.32



Screen shot 2: Throughput analysis

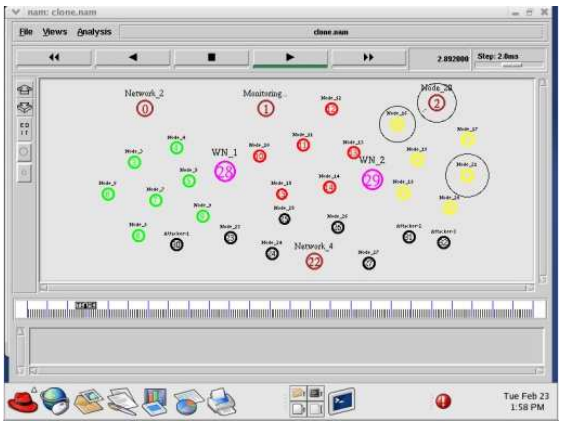
6 SIMULATION RESULT

The simulations results show that first of all form a cluster. There\are four clusters are formed. The every node senses the sensor field and initializes the location of sensor nodes. All sensor nodes get the communications. The dependency on their nearest position connected to each other. This process done in all cluster is shown below:



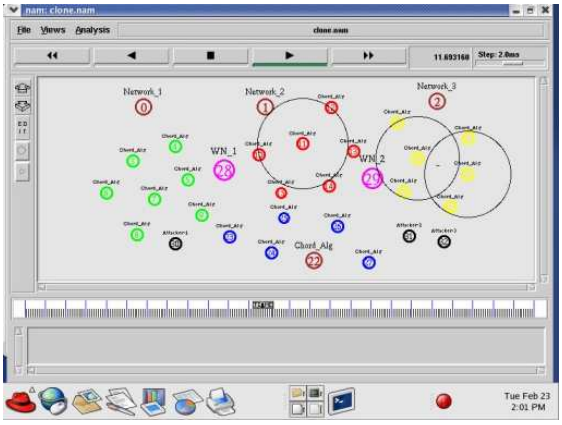
Screenshot 4: Number of Sensor Node.

In next step of nodes are connected to each other the process of sending time and receiving time of pending request. The some node is missed due to their long distance. The figure shown below:



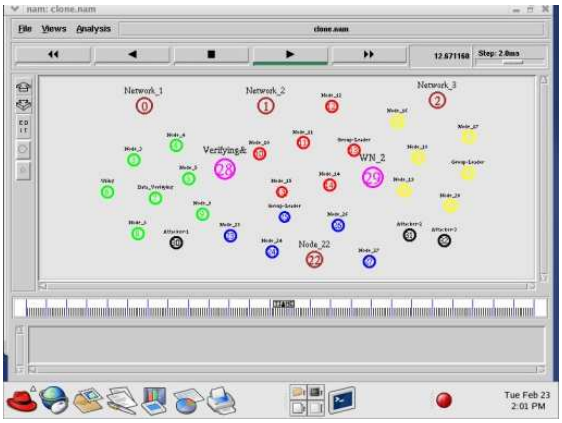
Screenshot 5: Sensor Node Connected to Each other.

In next step every sensor node are connected to the cluster head. All data are sending to the cluster head.



Screenshot 6: Sends Data to Cluster Head.

The cluster head can send information to base station. The figure shows below:



Screenshot 7: Cluster Head Send Data to baseestation.

7 CONCLUSION

There are three exposure protocols are used: One is based on a RDE, other is distributed hash table, and third one is chord. The DHT protocol gives high sanctuary for all types of sensor networks. We have implemented the CHORD algorithm and RED protocol to classify replica harass in wireless sensor networks. By implementing this technique we are able to classify the attacks more competently than the existing approaches.

Also we are encrypting the data packet during broadcast will also increase the security level. Since we are implementing the level-wise security for retrieve the data from other node in the network will be more useful in armed applications.

REFERENCES

[1] B. Parno, A. Perrig, and V. Gligor, —Distributed detection of node replication attacks in sensor networks, in Proc. IEEE Symp. Security Privacy, 2005, pp. 49–63.

[2] H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, Looking up data in P2P systems, Commun. ACM, vol. 46, no. 2, pp. 43–48, 2003.

[3] Y.Zhang,W.Liu,W. Lou, and Y. Fang, Location- based compromise tolerant security mechanisms for wireless sensor networks, IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 247–260, Feb. 2006.

[4] S. Zhu, S. Setia, and S. Jajodia, —LEAP: Efficient security mechanisms for large-scale distributed sensor networks, in Proc. 10th ACM CCS, Washington, DC, 2003, pp. 62–72.
[5] R. Anderson, H. Chan, and A. Perrig, —Key infection: Smart trust for smart dust, in Proc. 12th IEEE ICNP, 2004, pp. 206–215.
[6] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, —A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks, in Proc. 8thACMMobiHoc,Montreal, QC, Canada, 2007, pp. 80–89.
[7] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, —Efficient distributed detection of node replication attacks in sensor networks, in Proc. 23rd ACSAC, 2007, pp. 257–267.
[8] H. Choi, S. Zhu, and T. F. La Porta, —SET: Detecting node clones in sensor networks, in Proc. 3rd Secure Comm, 2007, pp. 341–350.
[9] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, —On the detection of clones in sensor networks using random key predistribution, IEEE Trans. Syst.s, Man, Cybern. C, Appl. Rev., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.
[10] L. Eschenauer and V. D. Gligor, —A key management scheme for distributed sensor networks, in Proc. 9th ACM Conf. Comput. Commun. Security, Washington, DC, 2002, pp. 41 47.