IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 1, Feb-Mar, 2014
ISSN: 2320 - 8791
www.ijreat.org

Sense And Transfer Packet For Multihop Wireless Network Using Chord Algorithm

Befeena Francis[1], R.Aroul Canessane[2]

[1]M.E Student, Computer Science & Engineering, Sathayabama University, Chennai.
[2]Associate Professor, Faculty of Computer Science & Engineering, Sathayabama University, Chennai.

***Abstract*: Our work behind this paper is to propose the a clone node detection protocol with different transaction on network circumstances and presentation. Originally the chord algorithm is used to detect the clone node based on distributed hash table(DHT). Each and every node in the network is assigned to the unique key. The witness should check the data before the transformation starts. If the witness node identifies the similar key in another node, then it mark as a clone node. Furthermore, the similar function in the distributed detection protocol carry out in the distributed hash table and it is easy and cheap to implement. Through this method, it requires to know the neighbor node identification(ID's) and node Location. Finally, the paper construct the DHT to detect the clone node with high security level and hold strong resistance against attackers. The experimental result prove that it consumes minimal memory storage and high detection probability.**

Keywords: DHT, Distributed Detection Protocol,

1. INTRODUCTION

A Wireless Sensor network(WSN) [1] is a compilation of sensor node with limited resources that work together in order to achieve a mutual goal.Sensor nodes, which works in different zone, such as battlefields and observation zones. Wireless Sensor Network shows the potential technology for spatial and temporal resolution.

The critical nature of sensor network applications is that any loss of sensor resource due to a malicious attack will cause significant damage to the entire network. The sensor node network develops many intelligent attackers operating in their surroundings nodes. It make the damage node to subvert from the network. The damage node cannot enter into the network, the witness node block the clone no security solutions need for sensor networks have to operate with minimal energy usage, even as securing the network. So the basic security requirements of WSN are accessibility, privacy, integrity and communication. The Security of wireless sensor networks isat risk to the clone node, and several distribute protocols have been developed to detect this attack [2]. So they require two strong assumptions be practical for major randomly deployed sensor networks. An attacker can capture a few nodes, and identifications, and use those materials to clone many nodes out of all other sensor hardware. These cloned nodes that can freely join the sensor network and then make the enlarge the attacker's capacities to manipulate the network maliciously.

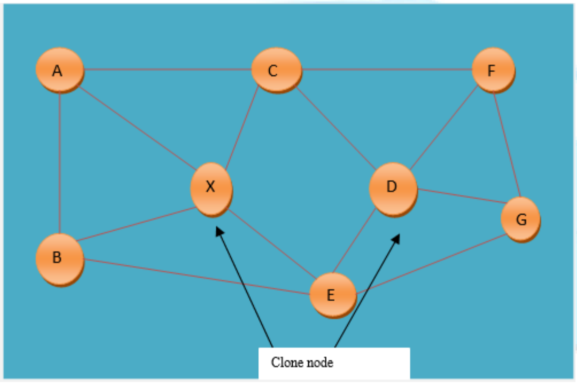
To overcome these issue witness nodes is used to detect the clone node and chord algorithm is used to verify the neighbor nodes information of the request node. So that by verifying the ID's and Location, we can detect the clone node. For this purpose, we have to create the list of the neighbor node information for each node so that the server/witness node can verify the node's request. Based on this the paper which proposes a clone detection method on the DHT with chord algorithm that is the unique feature of early detection.

II RELATED WORK

Several approaches have been proposed in literature for clone detection with high security level and holds strong resistance against adversary's attacks.

Rui Zhang et al, proposed the algorithm for clone detection. This algorithm called Randomized Multicast is used for detecting node replication attacks that takes a different approach for selecting witness for a node. In this approach which we call localized multicast, the witness node for a node identity are randomly selected from the nodes for a node identity are randomly selected from the nodes that are located within a geographically limited region [3].

AyouB Ait Lahcen et al, proposed for load balancing with replicas in DHT based p2p network.SCOPE uses RPTs (Replica Partition Trees) for strictly managing the replica location and thus support consistency of data in the network. Since SCOPE assumes p2p networks with DHTs, it must be difficult to support efficient range queries. In addition, the number of messages were only considered as load and the costs for data sending should be also considered a Keith M. Martin et al, proposed a framework for classifying different sensor network environments from the point of view of key establishment requirements. Fitting existing schemes within this framework permits a clearer comparison of schemes appropriate for particular network environments. Furthermore this framework enables the identification of application environments to which inadequate attention [5].



V. Manjula et al, proposed to concentrate on anidentical attack called replication attack where if one or more nodes illegally destroy an identity of specificnode and it will replicate all the nodes in the network. Reason for choosing this attack is that it can form the basis of a variety attack such as routing attacks and link layer attack also called as denial of service attacks which affects the availability of the network.Therefore the fundamental problem in sensor network detection of node replication attack [6].

Zhijunli et al, proposed key-based caching and checking system, which is constructed to catch cloned nodes based on distributed hash table. The border determination mechanism is employed to further reduce communication payload[7].

Section I of this paper is a background introduction. Section II discusses a brief literature review of clone node detection method. Section III describe existing work. Se ctionIV(1) Network construction, IV(2) Chord algorithm, IV(3) Witness node distribution IV(4) Verification of random number, IV(5) Verification of user ID, IV(6) Block the repeated data packet, IV(7) Clone node detection. Concluding remarks and scope for furt are given section(V).

4.1: Clone Node Detection

III. EXISTING WORK

The wireless sensor networks are at a risk to the node clone, and several distributed protocol to detect this attack. So they require too strong assumption to be practical for major randomly deployed sensor networks. An adversary can capture a few nodes, extract code and all secret credentials, and use those materials to clone many nodes out of off-the-shelf sensor hardware. Those cloned nodes that can freely join the sensor network and then continously make enlarge the attackers capacities to manipulate the network maliciously.

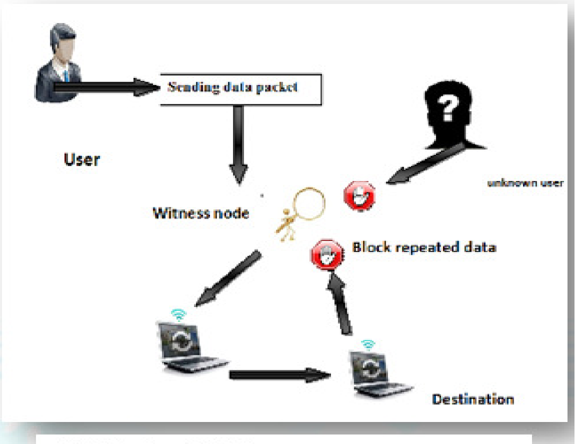


Fig: 2 System Architecture

IV. PROPOSED WORK

The clone node detect protocol with different functionality on network conditions and performance. Initially, it is based on a distributed hash table (DHT) in which chord algorithm is used to detect the clone node, every node is assigned to the unique key, before it transmit the data it has to give its key which would be verified by the witness node. Continue to the initial stage, the distribution detection protocol, which is same as DHT, but it is easy and cheaper implementation. Here every node only needs to know the neighbor-list containing all neighbor ID's and location. So the clone node can detect with high security level and hold a strong resistance against adversary's attack.

IV (1). NETWORK CONSTRUCTION

To construct and maintain the efficient, dynamic network topology is a very important task in wireless sensor network. Instead of transmitting with the maximal power, nodes in a multihop wireless network collaboratively determine their transmission power and define the network topology by forming the proper neighbor relation under certain □riteria. This is in contrast to the traditional network, in which each node transmits with its maximal transmission is built implicitly by relating protocols without considering the power issue. A desirable network topology not only reduces energy consumption and prolong network lifetime, but also improve spatial reuse and mitigate the medium-access control (MAC) [8] level contention. In a network, nodes are interconnected with admin, which is monitoring all the other nodes. All nodes are sharing their information with each others as shown in fig .2

IV CHORD ALGORITHM

A chord which assigns the distributed hash table with key-values to compare the values with different node. Chord specifies how key are assigned to nodes and how a node can find out the values for a given key by locating the node responsible for that key.

ID's and key values are assigned as n-bit. It identifies using consistent hashing. The chord-algorithm is based on hashing function for consistent hashing. Consistent hashing is integral to the strength and performance of chord, because both the keys and IP address (IDs) are uniformly distributed in the same identifier space. Consistent hashing is also necessary to join the node and leave the network without distribution. Using the chord lookup protocol, node key is arranged in a circle (based on network range) that has at most 2^n nodes. The circle can have IDs/keys ranging from 0 to 2^n-1.

Chord always maps a key into a node. A n-bit identifier is assigned as Keys and nodes. For nodes, IP address of specific node is an identifier in the distributed hash table. A keyword is an identifier for key in distributed hash tables. similarly for a file name too. The actual identification of nodes and keys are the IP address and Location ID. Key K is the node whose identifier of Key. If there is N node is responsible for node. Generally, K/N keys are used for when a new node joins or leaves the network. The pseudo code to find the successor node of an identifier:

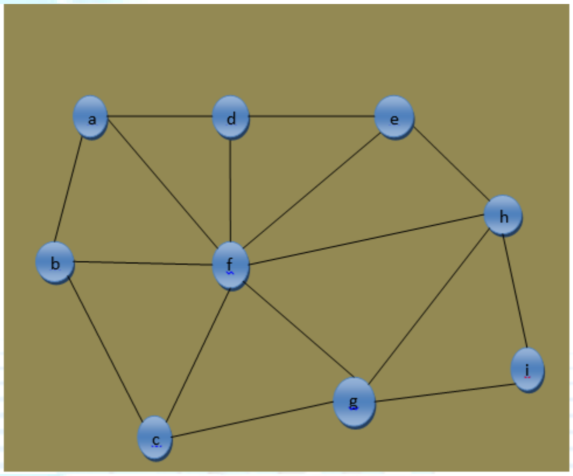


Fig:3 Node Distribution to Share ID's and Location

```
// To find the successor of the id for node n
N find_successor (id)
If (id € (n, successor))
Return successor;
Else
//Forward the inquiry around the circle
no= closest-preceding_node (id);
returnno.find_successor(id);
```

```
//the highest predecessor of id look for the local table

n.closest-preceding_node(id)

for i=m down to1

if(finger[i]€(n,id))

return finger[i];return n;
```

IV (3) WITNESS NODE DISTRIBTION

The selection of the witness is used to detect the clone node. The design is based on the this clone detection protocol. We will call “witness” as a node which is used to identify the clone node and block the attacker. If the admin knows the future witness before the detection protocol executes, the adversary would subvert these nodes so that the attack goes undetected or block the node. we have identified two kinds of production

1. ID-based prediction
2. Location-based prediction

We say that a protocol for replication attack detection is ID-oblivious. If the protocol does not provide any information on the ID of the sensors that will be the witness of a clone node attack during the next protocol run(ID based prediction). Similarly, if a protocol is area-based, if the probability does not depend on the geographical position of nodes in the network. Clearly, when a protocol is neither ID-oblivious nor area-based, then a smart admin can have good chance of succeeding, it is able to use this information to subvert the nodes that most probably, will be the witness as shown in fig:3

IV (4) VERIFICATION OF RANDOM NUMBER

Random key pre-distribution [10] scheme is implemented in the sensor network. That is, each node is assigned a number randomly with time stamp from Group leader. Then the Group leader will transmit a random number (Encrypted with RSA algorithm) which was generated with respect to that Time Stamp to the witness node. Witness node will now check the random number key distribution which is generated with the user information. If both the data are same then the witness node will confirm that this node is authentic.

4.5 CHECKIING OF USER ID

Each node is assigned with an ID for an individual node. Once it is registered into the network and also an ID for the whole group then Location ID is generated for each and every location. That Node ID and Location ID are also appended to witness node (Encrypted with RSA algorithm). Then the witness node will now check node ID + Location ID which is generated with the user information. If both the data are matched, then witness node will confirm that this node with the location is genuine.

4.6 BLOCK THE REPEATED DATA PACKET

Collision problem will occur while sending the same data packet between the nodes. So in this module using Chord algorithm, it will block the repeated data between the nodes. The witness node will scan all node data if it finds any repeated data, immediately it blocks through ID as shown in Fig:4.

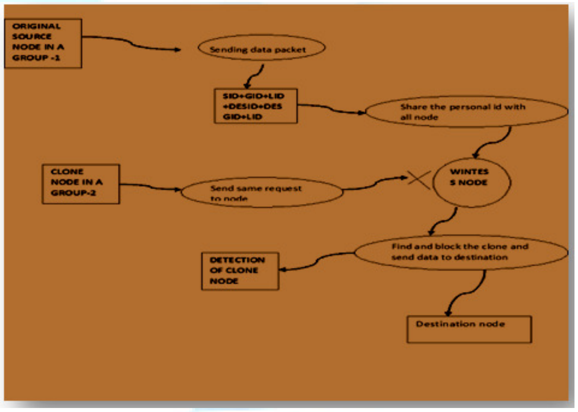

ORIGINAL SOURCE NODE IN A GROUP -1
Sending data packet
SID+GID+LID +DESID+DES GID+LID
Share the personal id with all node
CLONE NODE IN A GROUP-2
Send same request to node
WINTES S NODE
Find and block the clone and send data to destination
DETECTION OF CLONE NODE
Destination node

Fig:4 Block the repeated data

NODE DETECTION AND DATA TRANSFER

Only the detection node confirms the sender node, the data send to the detection, which is genuine. If the user specified information and internal information are varied than the witness node will identify that cloning or some malpractice has occurred and the packets are discarded by the witness node.

V CONCLUSION

Based on the Distributed Hash Table (DHT) in which Chord algorithm is used to detect the clone node. This method is used to construct the network with chord algorithm and with the witness node distribution, it can detect the clone node with the witness node distribution. Here every node should know their neighbor node ID’s and Location ID. Finally, the construct the DHT to detect cloned node with high security level and hold a strong resistance against adversary’s attacks. The experimental results prove that it consumes minimal memory storage and high detection probability.

REFERENCE

[1] PrabirBarooh, Cut Detection in Wireless Sensor Network, IEEE transaction in parallel and distributed system (2012).

[2] Scott C. -H. Huang* , Peng-jun Wan* , Xiaohuajia* , Hongwei Du* , weiping Shang, Minimum-Latency Broadcast Scheduling in Wireless Ad Hoc Networks, IEEE publication in the IEEE INFOCOM 2007 proceedings.

[3] ui Zhang, Yanchao Zhang, KuiRen, Distributed Privacy-Preserving Access Control in Sensor Networks, IEEE proceedind, Aug.2012(vol.23 no.8).

[4] AyoubAitLahcen[a,b] , Didier Parigot[a] , A Light Weight Middleware fro Developing p2p Application with Component and Service-Based Principles , published in “CSE’12 IEEE international computional science and engineering , pathos(2012).

[5] Keith M.Artin2 Maura Paterson1,3 , An Application-Oriented Frame work for Wireless Sensor Network Key Establishment , Electronic Notes in Theoretical computer science 192(2008) 31-41.

[6] V.Manjula[1] and Dr.C.Chellapan[2] , Replication Attack Mitigations for Static And Mobile Security and Its Applications(IJNSA) , vol.3 , No.2 , march 2011.

[7] ZhijunLi ,Guang Gong , On the Node Clone Dtection in Wireless Sensor Network , IEEE/ACM Transactions on Networking.

[8] F.Iannello, O.Simeone and Spaginolini, Medium Access Control Protocol for Wireless Sensor Network with Energy Harvesting(2011).

[9] Guruprasad Khataniar[1] and Diganta Goswami[2],SPH:A Hierarchial Protocol to Improve Performance of Peer-to-Peer Systems,(2012).

[10] Leonardo B.Oliveira[a,*], Adrian Ferreira[c], Marco A.Vilaca[c], Hao Chi Wong[b], Marshall Bern[b], Ricardo Dahab[a], Antanio A.F.Loureiro[c], SecLEACH-On the Security of Clustered Sensor Network(2007).

[11] Scott.C, -H.Huang, Peng-jun Wan, Jing Deng, and Yunghsiang S.H, Broadcast Scheduling in Interference Environment, IEEE transaction(2008).

[12] Rajiv Gandhi, Yoo-Ah Kim, Seungjoon Lee, Jiho Ryu, and Peng-jun wan, Appromation algorithm for Data broadcast in Wireless Network, IEEE transaction in(2009).

[13] Wei Wang, Boon-Hee Soong, Collision-Free and and Low Latency Scheduling Algorithm for Broadcast operation in Wireless Ad-hoc Networks, IEEE publication in(2007).

[14] Scott.C, -H.Huang, Peng-jun Wan, Xiahua jia, Hongwei Du, Low Latency Broadcast in Scheduling in Ad-hoc Network, IEEE publication in(2006).

[15] Jae joon-Lee, Bhaskar, Krishnamachari, C.-C.Jay Kua, Determining Localized Tree Construction Scheme Based on Sensor Network Lifetime, Hindawi publication corporation(2010).