International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 7 Issue 1 –MARCH 2014.

DISTRIBUTED HASH TABLE PROTOCOL DETECTION IN WIRELESS SENSOR NETWORKS

Mr. M. Raghu (Asst.professor)
Dr .Pauls Engineering College

Ms. M. Ananthi (PG Scholar)
Dr. Pauls Engineering College

Abstract- Wireless sensor networks are the weakest to the node clone, and several distributed protocols have been proposed to detect this attack. So, they require too strong assumptions to be practical for large scale, randomly deployed sensor networks. In this paper, to propose two novel node clone detection protocols with different tradeoffs on network conditions and performance. The first one is based on a distributed hash table (DHT) in which chord algorithm is used to detect the cloned node, every node is assigned with unique key, and before it transmits the data it has to give its key which would be verified by the witness node. If the same key is given by another node then the witness node identifies the cloned node. The second one based on distributed detection protocol which is same as DHT, but it is easy and cheaper implementation. Here every node only needs to know the neighbour-list containing all neighbour Ids and its locations. Hence the simulation results uphold the protocol design and show its efficiency on communication overhead and satisfactory detection probability.

I. INTRODUCTION

In wireless sensor network there are wide range of application areas and specific design challenges are obtained. The concept of the sensor networks is based on the sensing, CPU, radio is equal to thousands of potential applications. It seems like straight forward combination of modern technology. Therefore it is necessary to synthesize the interconnected web that will emerge as they deployed, while meeting strict requirements of size, cost and power consumption.

Sensor network application classes [3]:

Collection of data: The collection of data application is characterized by the large number of nodes for transmitting and receiving the data into a set of base stations, and then the particular data will be stored. The distance between the adjacent nodes will be minimal yet the distance across the entire the network that will be more significant. The important characteristics of data collection is based on lifetime, precise synchronization, low data rates and some related topologies. The data can be transmitted in order to improve the network efficiency.

Monitoring the security: Security monitoring application is characterized by using the composed nodes that are placed at fixed locations. A small difference between the security monitoring and the environmental monitoring is that not actually collecting the data. Actual data transmission will consume more network energy.

Tracking of node scenarios: A node tracking the sensor network is used to track the object through the region of space or address is to be monitored by the network. It is essential that the network be able efficiently detect the clone node. It keeps on tracking the node until the new nodes that enter the network.

With the large number of cloned nodes under command, the adversary may even gain control of the whole network. Therefore the node will exacerbate most of the sensor networks**.**

II. PREVIOUS WORK

In previous work they are using two novel clone detection protocols. These detection protocols are based on different network performance and conditions. First one is Distributed hash table protocol and another one is randomly directed exploration protocol. Both the protocol performance on memory consumption and a security metric deducted through the simulation results.

The results shows that the DHT based protocol can detect with the high security level and low performance. Here probabilistic directed technique is used as the network incurs randomness for the communication and performance will be low. In terms of the simulation results the output performs the communication cost, while the detection probability is obtained. For that it acquires the low performance and adversary attacks.

A. Distributed detection

In Distributed detection protocol is same as distributed hash table (DHT), but it is easy and cheaper implementation. Here every nodes only needs to know the neighbour-list. In neighbour nodes we have the neighbour ID and locations of the user. For that we can detect the clone with high security.

B. centralized detection

It is simplest approach, here each and every node sends their neighbour ID and locations to the base station, which they find the cloned nodes. Here so many protocols are used to detect the clone nodes. The protocols are SET, secret key extraction, random

key predistribution etc. The SET protocol is to reduce the communication cost. However these protocols require the authenticated subset covering protocol to be performed and then it increases the burden the communication performance. The concern of this approach it has high false negative and positive rates.

III. DISTRIBUTED HASH TABLE

Distributed hash table protocol is the improved version of the previous work because in DHT we are using the chord algorithm. Here every node is assigned a unique secret key , before it transmit the data, the key is verified by the witness node. Distributed Detection is same as DHT, but it is easy and cheaper functioning. By using the secret key we can find the authorized user. In somecases the unauthorized user can access the network, by using chord algorithm we can detect the cloned node.

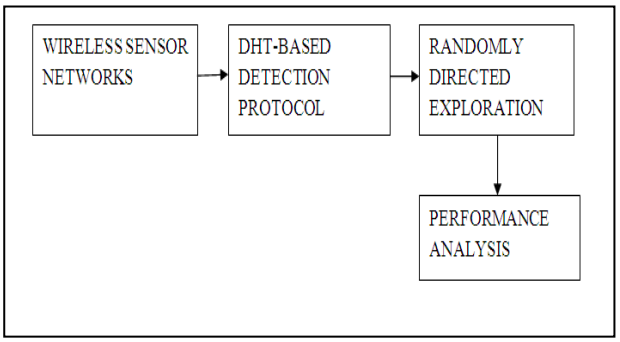


Figure 3.1 Block Diagram

In this block diagram it shows that the wireless sensor network is used to sense the network. In terms of DHT is to assign a secret key to each and every node. And then randomly directed exploration is intended to provide highly well-organized communication performance. And then performance analysis is based on the average number of nodes to be transmitted, average number of node cache table sizes, average number of spectator.

DHT is a class of distributed decentralized system that provides the lookup services to a hash table;(key, value)pairs are stored in DHT. In DHT there are several services are available. There are distributed file system, domain name services, instant messaging, multicast, and also peer to peer file sharing and content distribution systems.

It has a table partitions the key space and distributes the set of nodes in the network. For any new content of node is added to the network, a hash function (k) is calculated and the message is sent to the next node. Then the message is forwarded to the node until it reaches the next node or destination.

The pair (k, data) is stored to the next node. If the message is not forwarded to the next node, again the message will be forwarded through the node is responsible for k. And then it stored the data it can scale the large number of nodes whether the message is successful or failures.

By the design of DHT, it takes the responsibilities of mapping the keys among all the nodes in an efficient and balanced way.

IV. CHORD ALGORITHM

Chord Algorithm is used for problem addressing protocol in distributed look up. The chord consists of nodes which every node is located at one point. It supports just an operation is given by a key which refers the chord that maps onto the node. The advantage of using chord is simple, provable correctness, provable performance.

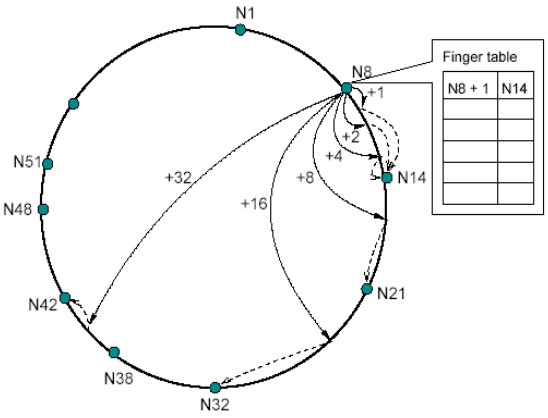
The chord is used to achieve pseudo-randomness on output consisting of a hash function (H) is used to map an arbitrary input into a m-bit, which can be convinced as a ring.

4.1 Construction Of Chord Ring

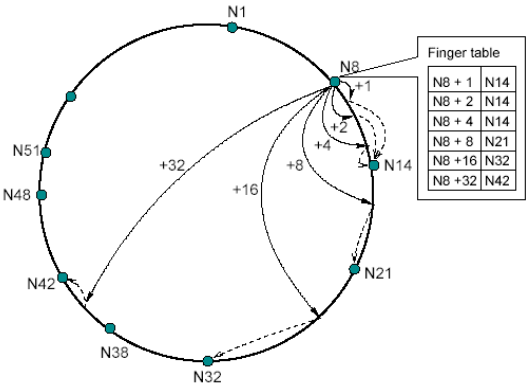
- The standard hash function assigns each node and each key an m-bit identifier using SHA-1
  a. m = any number is enough to make collisions improbable.
  b. Key identifier = SHA-1(key)
  c. Node identifier = SHA-1(IP address)
- Key identifier and Node identifier are uniformly distributed.
- That exists in the same ID space.

4.2 Scalable Node Localization

- Each node n contains a routing table with up to m entries.



- i^{th} entry in the table at n ode n contains the first node s that succeeds n by at least 2^{i-1}
- S = Successor $(n+2^{i-1})$
- S is called the i^{th} finger of node n.
- Each node stores information only small number of nodes (m).
- A table generally does not contain enough information to directly determine the successor of an arbitrary key k



4.3 Node joins and stabilization

- All successor pointers must be to update.
- The stabilization protocol running periodically

V. SIMULATION RESULTS

The simulation results show that the DHT based detection protocol using chord algorithm is used to detect the clone node. In the node creation several number of nodes available. In that node clone First we have to analyse the failure node. On that failure node we have to identify the cloned node based on the user ID and their locations. Hence it has same ID or same region based on that we have to identify the duplicate node. At the same time the duplicate node is known to be cloned node.

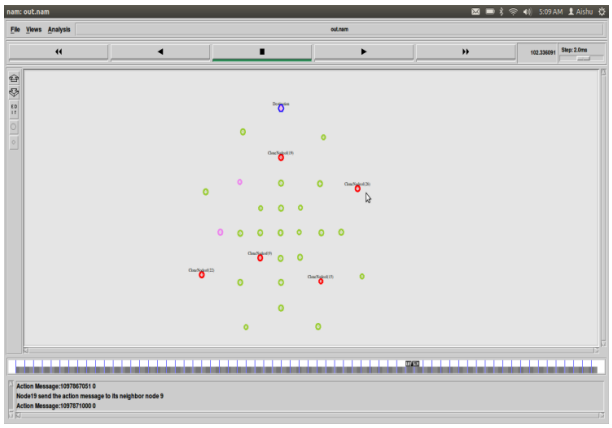


Figure.5.1 Analysis of failure node and detection of clone node.

A claiming message will be forwarded to the destination node. The destination node is one of the successor nodes. Here the analysis of failure node and to detect the clone node using the chord overlay network in the specification of the sensor networks. For that it has the high security and efficient storage consumption of the DHT interfaces. The interfaces are the routing interface, client interface and storage interface. Among the design challenges are the routing efficiency, management overhead and dynamics.

VI. PERFORMANCE EVALUATION

Performance of DHT-based detection protocol is calculated in terms of packet delivery ratio and end to end delay ratio.

Packet Delivery Ratio

Packet delivery ratio defined by the number of delivered data packet to the destination. This simulation is to measure the protocol performance based on different network conditions and sizes. For each rounds of transmitting the messages a random seed is generated, and then the two nodes having the same set of ID that is the process of two nodes are cloned nodes. The average number of messages sent per node is based on the time period which is the node is independent to the network and it matches the chord.

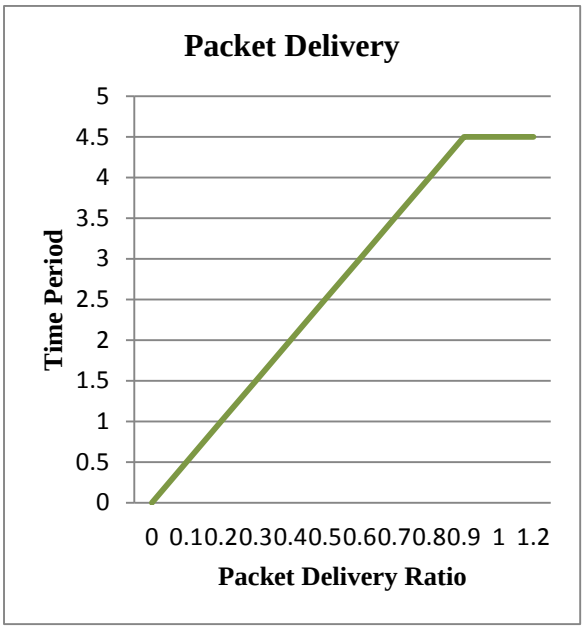


Figure.6.1 Packet Delivery Ratio is used to determine the performance is stable.

End To End Delay

The average time taken by a data packet to arrive in the destination.

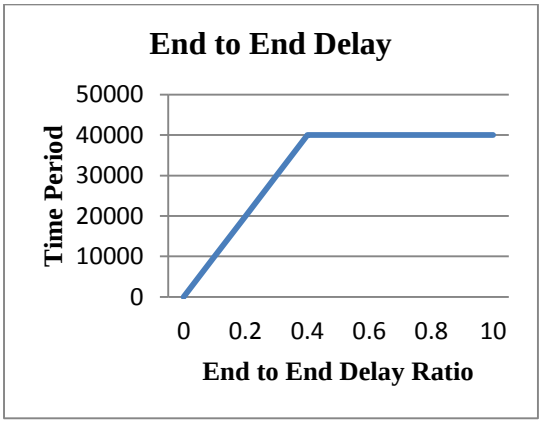


Figure.6.2 Delay ratio

∑ (arrive time-send time) / ∑ number of correction.

In the end to end delay is difficult to bound for sensor networks, where nodes can be generate or propagate data when the delay is occurred. Here the total numbers of packets are dropped during the simulation.

Number of packet send – Number of packets received

VII. CONCLUSION

Sensor nodes lack to fiddle in the hardware and are subject to the node clone attack. Here two distributed detection protocols one is based on a distributed hash table , which is fully decentralized and it performs a chord overlay network and provides the key-based routing, caching and checking facilities for clone detection , and the other uses probabilistic directed technique to achieve good communication performance. Meanwhile the DHT-based protocol provides high security level for all kinds of sensor networks by one deterministic observer and additional memory-efficient, probabilistic witnesses, the randomly directed exploration presents outstanding communication performance and minimal storage expenditure for dense sensor networks.

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] R. Anderson, H. Chan, and A. Perrig, “Key infection: Smart trust for
Smart dust,” in *Proc. 12th IEEE ICNP*, 2004, pp. 206–215.

[4] 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.

[5] H. Choi, S. Zhu, and T. F. La Porta, “SET: Detecting node clones in sensor networks,” in *Proc. 3rd SecureComm*, 2007, pp. 341–350.

[6] I. Stoica, R.Morris, D. Liben-Nowell, D. R. Karger,M. F.Kaashoek, F. Dabek, and H. Balakrishnan, “Chord: A scalable peer-to-peer lookup protocol for internet applications,” *IEEE/ACM Trans. Netw.*, vol. 11, no. 1, pp. 17–32, Feb. 2003.

[7] A. I. T. Rowstron and P. Druschel, “Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems,” in *Proc. IFIP/ACM Int. Conf. Distrib. Syst. Platforms Heidelberg*, 2001, pp. 329–350.

[8] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *Proc. 1st Int. Conf. Simulation Tools Tech. Commun.,Netw. Syst. Workshops*, Marseille, France, 2008, pp. 1–10.

[9] A. Awad, C. Sommer, R. German, and F. Dressler, "Virtual cord protocol (VCP): A flexible DHT-like routing service for sensor networks," in *Proc. 5th IEEE MASS*, 2008, pp. 133–142.

Ms.M. Ananthi has received the B.tech degree in information technology in 2012.Currently she is pursuing her M.E degree in Computer And Communication Engineering in Dr.Pauls engineering College, Pulichapallam, Villupuram district, Tamilnadu .Her area of interest re Network Security in Wireless Sensor Networks.