ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Network Security by Detecting Clone Node Using RSA Bitmap and DHT

Dr. R. Udayakumar [1], P. Gayathri [*2]

[1] Associate Professor, Department of Information Technology, Bharath University, Chennai, Tamil Nadu, India

[2]Assistant Professor, Department of Information Technology, Bharath University, Chennai, Tamil Nadu, India

[*] Corresponding Author

ABSTRACT: Wireless Sensor Network which is susceptible to the node clone, and quite a few distributed protocols have been planned to notice this attack. However, they need too strong assumptions to be practical for large-scale, randomly organized sensor networks. In this the data send by the source will be send in an image format as bitmap format. By using RSA algorithm the input is converted into bitmap format, the input data will be assigned with key so that the security will be strong only the destination will know the key and the source will decrypt the image and get the file. In this paper, we put forward two novel node clone detection protocols with dissimilar tradeoffs on net work conditions and performance. First one is based on a distributed hash table (DHT), by which a completely decentralized, key-based caching and inspection system is demonstrated to obtain cloned nodes capably. The protocol presentation on efficient storage space consumption and high security level is theoretically deducted through a probability model, and the resulting equations, with essential adjustments for real application, are supported by the simulations. To address this concern, our second distributed detection protocol, named randomly directed exploration, presents high-quality communication performance for solid sensor networks, by a probabilistic bound for forwarding method all along with random initial direction and border determination. . The simulation results support the protocol design and demonstrate its effectiveness on communication overhead and satisfactory detection probability.

KEYWORDS: Wireless Sensor Network, Distributed detection, distributed hash table, node clone attack, randomly directed exploration, RSA Algorithm.

I. INTRODUCTION

Wireless Sensor Network has gained a enormous deal of notice in the past decade due to their wide variety of application areas and frightening design challenge. Sensor nodes are usually short of tamper-resistance hardware components; thus, an opponent can arrest a few nodes, remove code and all secret credentials, and utilize those resources to clone many nodes out of off-the-shelf sensor hardware. Those cloned nodes that appear legitimate can freely join the sensor network and then increase the adversary's capacities to influence the network maliciously. With a large number of cloned nodes under command, the adversary may even increase control of the whole network. Furthermore, the node clone will aggravate most of inside attacks against sensor networks. In this paper, we present two novel, practical node clone detection protocols with different tradeoffs on network conditions and performance. First proposal is based on a distributed hash table (DHT), by which a fully decentralized, key-based caching and inspection system is constructed to catch cloned nodes. In accordance with our analysis, the comprehensive Simulation results show that the DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks. Our second protocol, named randomly directed exploration, is planned to provide highly well-organized communication presentation with adequate detection probability for dense sensor networks. In the protocol, initially nodes send claiming messages containing a neighbor-list along with a maximum hop limit to randomly selected neighbors; then, the subsequent message transmission is synchronized by a probabilistic directed technique to roughly maintain a line property through the network as well as to incur enough randomness for improved performance on communication and resilience aligned with adversary. In adding, border determination mechanism is working to further decrease communication payload. During forwarding, intermediate nodes search claiming messages for node clone detection. By design, this protocol consumes almost negligible memory, and the simulations illustrate that it outperforms all other detection protocols in terms of message cost, while the exposure probability is satisfactory. Main aim is to detect the clone node that is accessing with the original node's information; Clone node will attack the whole network using the malicious code. In this witness node which acts as the intermediate node will note down the ID, Random no, Time stamp of destination node and will check with the node which send the Information.[1]

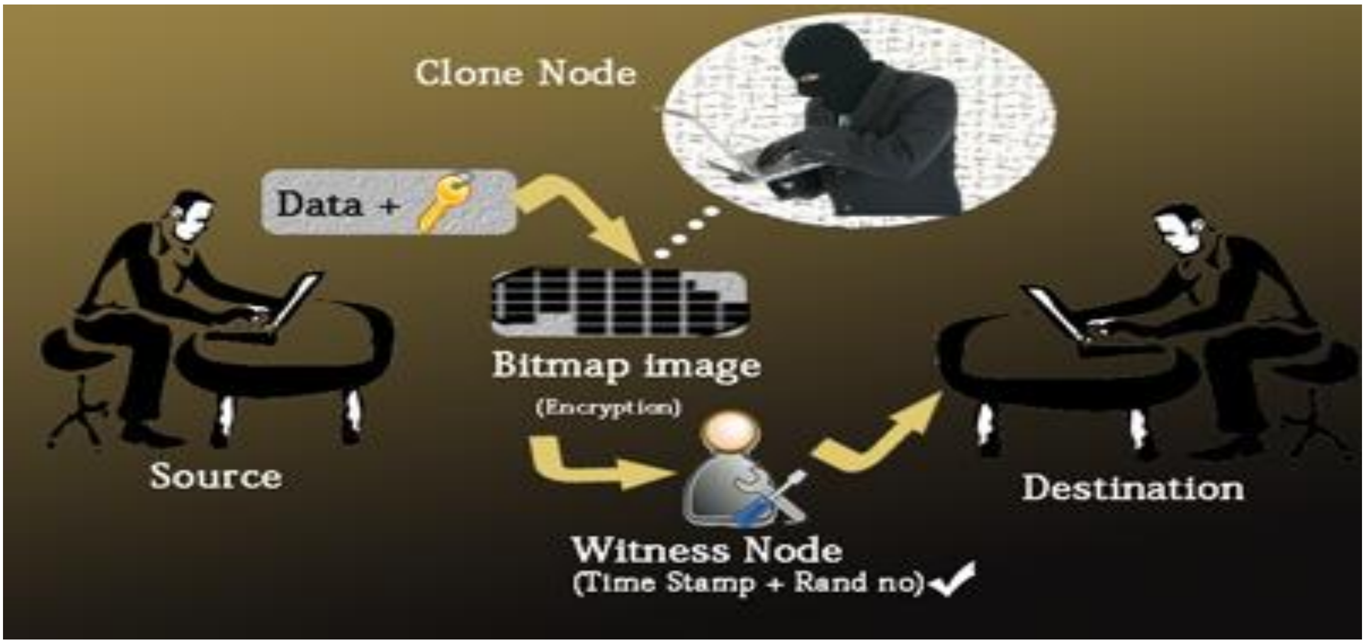


Fig 1: Detection of clone node attack in network

II. DHT-BASED DETECTION PROTOCOL

DHT distributed detection protocol is to make utilize of the DHT mechanism to figure a decentralized caching and checking system that can successfully detect cloned nodes. Essentially, DHT enables sensor nodes to distributive construct an overlay network and provide an capable key-based routing within the overlay network. A message linked with a key will be broadcast through the overlay network to attain a destination node that is solely determined by the key.[2] The source node does not require identifying or knowing which node a message's destination is the DHT key-based routing take care of transport details by the message's key. More importantly, messages with a same key will be stored in one destination node. We assign four roles initiator, Observer, inspector and witness.[3]

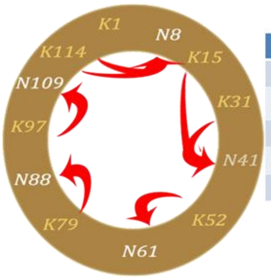
TABLE I
Assigning Four roles

Roles	Trusted	Duty
Initiator	Yes	Start a round of detection
Observer	No	Claim Neighnours ID and loc
Inspector	No	Buffer and check messages for detection
Witness	No	Broadcast Detection evidence

The initiator broadcast the action message with a random seed.[6] Then, every observer constructs a claiming message for each neighbor node, which is referred to as an examinee of the observer and the message, and transfer the information with probability separately.[4] In the protocol, a message's DHT key that examines it's routing and destination is the hash value of concatenation of the seed and the examinee ID. By means of the DHT mechanism, a claiming message will finally be transmitted to a deterministic destination node, which will cache the ID-location pair and check for node clone detection, acting as an inspector. [5]

Distributed Hash Table

A distributed hash table is a decentralized distributed system that provides a key-based lookup service alike to a hash table: (key, record) pairs are store in the DHT, and any participating node can professionally store and recover records linked with specific keys. By design, DHT distributes responsibility of maintain the mapping from keys to records among nodes in an efficient and balanced way, which allows DHT to scale to large networks and be suitable to serve as a facility of distributed node clone detection. There are several different types of DHT proposals, such as CAN, Chord, and Pastry. Generally, CAN have least efficiency than others in terms of communication cost and scalability, and it is not often employed in real systems. By difference, Chord is widely used, and we choose Chord as a DHT implementation to demonstrate our protocol. However, our protocol can easily migrate to build upon Pastry and there alike security and performance results.[7]



Node	Key
N8	K114,K1
N40	K15,K31
N61	K52
N88	K79
N109	K97

t	Key	Node
1	72	N88
2	40	N41
3	24	N41

Fig. 2 Chord network

A demonstration of a Chord system with little parameters is given in Fig. 1. In this system, if node N8 needs to query a record with key K97, it initial looks up its successor table. Since 97 is not in (109, 61], namely (direct predecessor, the last successor], node proceeds with the finger table and finds that the subsequently forwarding node should be N88 because 97 (72: the first item in finger table corresponding to, 109: direct predecessor). When N88 receive this query about, by inspection its successor table with two nodes of N109 and N8, it determines the end node should be, N109 as (88: itself, 109: the first successor].[9] When node N109 get the query, it know itself be the destination because 97 (88: direct predecessor, 109: itself].By this routing mechanism, on average (g/g+1) of queries in the direction of a destination pass from side to side one of g predecessors. For node N109 as the destination, its two predecessors are N88 and N61, and the latter's straight predecessor is N41 the line from N41 and N109 has the length of 109-41 and is divided by N61 and N88 into three segments with lengths of, and. Therefore, the probability of a query passing through N61 and N88 are 20/68 and 27/68, correspondingly.[10]

Applications employing DHTs

FAROO

FAROO is a worldwide web search engine depends on peer-to-peer technology. It uses a distributed crawler that stores search data on users' computers instead of a central server. Whenever a consumer visits a website, it is routinely indexed and distributed to the network. Ranking is complete by comparing usage statistics of users, such as web pages visited, amount of occasion exhausted on each page, and check out whether the pages were bookmarked or printed.[8]

Coral Cache

The Coral Content Distribution Network, sometimes called Coral Cache or Coral, is a free peer-to-peer content distribution network. Coral use the bandwidth of a world-wide network of web proxies and name servers to mirror web content, frequently to keep away from the Slashdot Effect or to reduce the load on websites servers in general.

Algorithm 1:

```
var query = 'somequery'; // random seed will be given
var rootnode = N97;// Node which we have to find out
var successor = N61; // Next node which is the neighbor node
var predecessor = N109; // Node which is subsequent to main node
if (rootnode == successor || rootnode == predecessor){ // Checks whether the successor and predecessorNIL;    break;
//come out of loop
}Else {    var forwardingNode = N88;
   var nodes[] = {N109, N8};
   for(int i = 1;i<=2; i++)
   {    if(nodes[i] == forwardingNode)
{    forwardingNode = query;
         var destinationNode = nodes[i];//contains N109
         var numQueries = g/(g+1);
         var Probability = 27/68;        }}}
```

Output:

1) This node is the destination node of the claiming message.
2) The destination node is one of the successors of the node.

In this case, the average witness number can be obtained by

$$\rho=1+g\ (1-(1-pr)\ m)^{2}$$

g predecessor nodes of the destination may become witnesses if and only if they receive at least two claiming messages associated with different cloned nodes.[11]

Algorithm 2:

```
var signature = mAlpha;
if(idBeta == CacheTable)
{if(idBeta == clone || idBeta == witness)
   broadcast the evidence;    else   buffer mAlpha into CacheTable
 }
```

III. RANDOMLY DIRECTED EXPLORATION

In RDE, the messages broadcast over a Chord overlap network incur considerable communication cost, which may not be preferred for some sensor networks that are very sensitive to energy consumption.[12] To complete this challenge, we suggest the randomly directed exploration (RDE), which tremendously reduce communication cost and presents optimal storage cost with adequate detection probability. Every node only wants to know and buffer a neighbor-list containing all neighbors IDs and locations. For both detection procedures, every node construct a claiming message with signed version of its neighbor-list, and then try to deliver the message to others which will compare with its own neighbor-list to notice clone. First, a claiming message needs to provide maximal hop limit, and at first it is send to a random neighbor.[13] Then, the message succeeding transmission will approximately preserve a line. The line transmission property helps a message go through the network as fast as possible from a locally optimal perspective.[14]

Algorithm 3:

```
var signature = mAlpha;
if(signature == mAlphaNeighbour)
{broadcast the evidence;}else { var ttl = ttl-1;
   if(ttl <= 0){    discard mAlpha;    }
   else{    var nextNode = getnextnode(mAlpha);
      if(nextNode == '')       {
      discard mAlpha;       }
      else       {       mAlpha = nextNode;      }}}
```

IV. CONCLUSION

In this paper, we present two distributed detection protocols: One is based on a distributed hash table, which form a Chord overlay network and provide the key-based routing, caching, and inspection facilities for clone detection, and the additional uses probabilistic directed technique to attain efficient communication overhead for acceptable detection probability. While the DHT-based protocol provides high safety level for all kinds of sensor networks by one deterministic witness and extra memory-efficient, probabilistic witnesses, the randomly directed exploration presents exceptional communication performance and negligible storage consumption for solid sensor networks.

In real time application we can use this in banking security purpose in order to identify the duplicate accessing of data (ie. hacking), In Military security purposes for the secure transformation of data and weapons details.

REFERENCES

[1] Zhijun Li, Guang Gong"On the Node Clone Detection in Wireless Sensor Networks" in IEEE/ACM transactions on networking, 2013,

[2] Krishnamoorthy P., Jayalakshmi T., "Preparation, characterization and synthesis of silver nanoparticles by using phyllanthusniruri for the antimicrobial activity and cytotoxic effects", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(11) (2012) pp.4783-4794.

[3] 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.

[4] 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.

[5] Madhubala V., Subhashree A.R., Shanthi B., "Serum carbohydrate deficient transferrin as a sensitive marker in diagnosing alcohol abuse: A case - Control study", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 7(2) (2013) pp.197-200.

[6] Y. Zhang,W. Liu,W. Lou, andY. 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.

[7] 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.

[8] Khanaa V., Thooyamani K.P., Saravanan T., "Simulation of an all optical full adder using optical switch", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6)(2013) pp.4733-4736.

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

[10] Nagarajan C., Madheswaran M., "Stability analysis of series parallel resonant converter with fuzzy logic controller using state space techniques", Electric Power Components and Systems, ISSN : 1532-5008, 39(8) (2011) pp.780-793.

[11] 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.

[12] 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.

[13] Bhat V., "A close-up on obturators using magnets: Part I - Magnets in dentistry", Journal of Indian Prosthodontist Society, ISSN : 0972-4052 , 5(3) (2005) pp.114-118.

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

[15].M.Sundararajan & R.Pugazhanthi," Human finger print recognition based biometric security using wavelet analysis", Publication of International Journal of Artificial Intelligent and Computational Research, Vol.2. No.2. pp.97-100(July-Dec 2010).

[16].M.Sundararajan & E.Kanniga," Modeling and Characterization of DCO using Pass Transistor", proceeding of Springer – Lecturer Notes in Electrical Engineering-2011 Vol. 86, pp. 451-457(2011). ISSN 1876-1100.(Ref. Jor- Anne-II)

[17].M.Sundararajan & C.Lakshmi, "Wavelet based finger print identification for effective biometric security", Publication of Elixir Advanced Engineering Informatics-35(2011)-pp.2830-2832.

[18].M.Sundararajan, "Optical Instrument for correlative analysis of human ECG and Breathing Signal" Publications of International Journal of Biomedical Engineering and Technology- Vol. 6, No.4, pp. 350-362 (2011). ISSN 1752-6418.(Ref. Jor-Anne-II)

[19].M.Sundararajan, C.Lakshmi & D.Malathi, "Performance Analysis Restoration filter for satellite Images" Publications of Research Journal of Computer Systems and Engineering-Vol.2, Issue-04- July-December-2011-pp 277-287