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, Special Issue 4, April 2015*

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

Reducing Overlay Networking Transmission Detection in Wireless Sensor Networks

D.J.Samatha Naidu, Dr.A.Prasad

Assistant Professor, Dept of MCA, APGCCS, New Boyanapalli, Rajampet, Kadapa, India

Associate Professor & HOD, Dept of computer science, vikrama simhapuri university, Nellore, india

ABSTRACT*:* In this paper existing work problems are identified due to the sensor nodes lack tamper-resistant hardware and are subject to the node clone attack. In this paper here it present two distributed detection protocols, Probabilistic directed forwarding technique along with random initial direction and border determination. The performance based final results uphold the parameters of a protocol design and show its efficiency on communication overhead and satisfactory detection probability. By using distributed hash table which also forms choke overlay network and provides keyword base routing, backup caching will be used to detect the other uses probabilistic directed technique will help to sends the network to overcome the problem.

KEYWORDS*:* network model ,general detection guidelines, performance metrics, advisory model.

I. INTRODUCTION

All The WSN is built of "nodes" –. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimension. In proposed work, probabilistic directed forwarding technique along with random initial direction and border determination. By using distributed hash table with session key, which also forms choke overlay network and provides keyword base routing, backup caching will be used to detect the other uses probabilistic directed technique will help to sends the network to overcome the problem.

II. RELATED WORK

Wireless Sensor Networks (WSNs) [2] provide an interesting research domain because they represent a class of massively distributed systems in which nodes are required to work in a cooperative and self-organized fashion to overcome scalability problems. Additionally, WSNs are facing strong resource limitations as a large number of sensor nodes with strong CPU, energy, and bandwidth restrictions need to be operated to build stable and operational networks. This includes the need to solve problems with high dynamics introduced by joining and leaving nodes.

Algorithm: Verification of Cord node join algorithm

Require: One node must be pre-programmed as initial node, i.e. it gets position S; all nodes in the cord periodically send hello messages.

1: **if** NeighbourPosition = S **then**
2: MyPosition S
3: Successor Neighbour
4: Predecessor NULL
5: **if** NeighbourSuccessor = NULL **then**
6: NewNeighbourPosition E
7: **else**
8:NewNeighbourPosition position(S,NeighbourSuccessorPosition)
9: **end if**
10:SendUpdatePredecessor(Neighbour, newNeighbourPosition)
11: **else if** NeighbourPosition = E **then**
12: MyPosition E
13: Successor NULL

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, Special Issue 4, April 2015

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

14: Predecessor Neighbour
15:NewNeighbourPosition position(NeighbourPredecessorPosition, E)
16:SendUpdateSuccessor(Neighbour, NewNeighbourPosition)
17: **else if** Neighbour1 is predecessor to Neighbour2 **then**
18:MyPositionposition(Neighbour1Position, Neighbour2Position)
19: Predecessor Neighbour1
20: Successor Neighbour2
21: SendUpdateSuccessor(Neighbour1)
22: SendUpdatePredecessor(Neighbour2)
23: **else**
24: CreateVirtualNode(Neighbour)
25: **end if**

III. PROPOSED RELATED WORK

A. Prevention

The identity-based cryptography is used in their protocol such that nodes private keys are bounded by both their identities of relevant locations. By similar arguments, they review key distribution protocols for sensor networks, and it can be claimed that some of them prevent node clone as well. For example, in schemes [4], [5] based on initial trust which assume that it takes adversaries a certain amount of time to compromise nodes after their deployment, valid keys only can be established during that safety period, and hence forth compromising nodes will not grant adversaries extra advantages, including the ability to cloned nodes. Those prevention schemes might be useful .

B. Centralized Detection

In a simplest centralized detection approach, each node maintains buffer to store a list of its neighbor nodes and their locations to a base station, which then can find cloned nodes. The SET protocol [8] manages to reduce the communication cost of the approach above by constructing exclusive subsets such that each node belongs to one and only one disjointed subset, and the subset nodes information is reported to the base station by a subset leader. The basic idea is that the keys employed in random key pre distribution scheme should follow a certain pattern, and those keys whose usage exceeds a threshold can be thought to be suspicious.

C. Distributed Detection

The straightforward node-to-network broadcasting [1] is a quite practical way to distributive detect the node clone, in which every node collects all of its neighbors identities along with their locations and broadcasts to the network. The main problem in this approach is its extremely high communication overhead provided two probabilistic detection protocols in a completely distributed, balanced manner. Randomized multicast scheme distributes node location information to randomly selected nodes as inspectors, exploiting the birthday paradox to detect cloned nodes, Moreover, the communication cost in the randomized multicast is similar to that in the node-to-node broadcasting. For the procedure of choosing random inspectors, both scheme simply that every node is aware of all other nodes' existence, which is a very strong assumption for large-scale sensor networks and thus limits their applicability. **[6]** and**. *[7]*** proposed several clone detection schemes.

Roles	Trusted	Duty
Initiator	Yes	Start a round of detection
Observer	No	Claim neighbors IDs and locations
Inspector	No	Buffer and check messages for detection
Witness	No	Broadcast detection evidence

Table 1: Roles in Detection Protocols

D .Network Model

They consider a large-scale, homogeneous sensor network consisting of *n* resource-constrained sensor nodes. In existing DD approaches, each legitimate node is allocated a unique ID and a corresponding private key by a trusted third party. Consequently, no node can lie to others about its identity. Let K_α and $K\alpha\text{-}1$ denote the public and private keys of node, respectively, and $\{M\}_{K\alpha}\text{-}1$ represent the signature of *M* signed by node α. They also assume that every sensor node can

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, Special Issue 4, April 2015

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

determine its geographic location *L* and current relative time via a secure localization protocol and a secure time synchronization scheme, respectively..

E. General Detection Guidelines

Relying on the identity-based cryptography, secure localization, and secure time synchronization used in our network model. In this sense, the neighbors of a node are its observers. Subsequently, some nodes will be selected as inspectors to examine claiming messages for the purpose of clone detection. If an inspector successfully finds a clone, it becomes a observer, which will broadcast necessary evidence to inform all connected nodes revoking the cloned nodes. While the initiator is trusted, the other roles (observer, inspector, and witness) might be compromised by the adversary and behavior maliciously. The four roles in our protocols are summarized in Table.

F. Performance Metrics

Metrics are used to measure a protocol's performance analysis and evaluate its practicability.

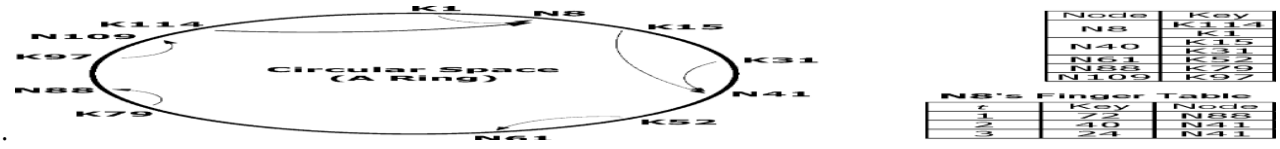
Detection probability and security level, As a primary security requirement, a practical detection scheme should detect the occurrence of the attack with high probability. Thus, the detection probability is the most important security metric for a probabilistic clone detection scheme. On the other hand, if a detection protocol is deterministic in the sence that cloned nodes are always caught by witnesses, and it is also a fully symmetric approach in which nodes are equally likely to become witnesses prior to a round of detection procedure, they will use the number of witnesses to evaluate the security level because more witnesses improve protocol resilience against the adversary's potential attacks to witnesses

G.. Adversary Model

The adversary definitely wants to conceal the existence of clone. In their settings, this enemy is allowed to interfere with a detection protocol as follows. 1.The bad cloned nodes may not appear in the regular detection procedures. 2.The nodes controlled by the adversary may fake, drop, or manipulate claiming messages that they forward. Third, the adversary can capture some nodes accordingly, but it would take time, and the total number of nodes that an adversary can compromise is limited. The adversary may also try to abuse a detection protocol to frame innocent nodes as cloned such that they will be expelled from the network. This can be lead a framing delay attack. DHT-Based detection protocol. The principle of our first distributed detection protocol is to make use of the DHT mechanism to form a decentralized caching and checking system that can effectively detect cloned nodes.

H .Distributed Hash Table

Chord network example, where the key space is 7-bit, seven records with different keys are stored in five nodes, and the successor table size g=2. For node N8, its direct predecessor is N109, and its two successors are N41 and N61. Likewise, the key of a record is the result of the hash function. Specifically, the finger table for a node with Chord coordinate contains information of nodes that are respectively responsible for holding the t keys: $(y+_2{}^b\text{-}i) \bmod 2^b$ for i€[1,t] .If two nodes are within the inner and outer side of ring-segments with their relay ratio distance, they are each other's predecessor node value and successor by the order of their coordinates, with respect to predefined . In theory, a Chord node only needs to know its direct predecessor and figure table. every node additionally maintains a successor table, containing its successors., the last node successor], node proceeds with the figure table and finds that the next forwarding node should be because 97€ .



Node	Key
N8	K1
N40	K15
N61	K31
N85	K79
N109	K97

N8's Finger Table

i	Key	Node
1	2	N85
2	10	N40
3	24	N41

Figure 2 : Virtual Ring network

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, Special Issue 4, April 2015

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

IV IMPLEMENTATION

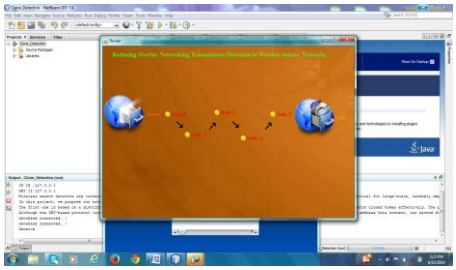


Fig 1: IP Verification page

Description: Attach the file and then send it to the server

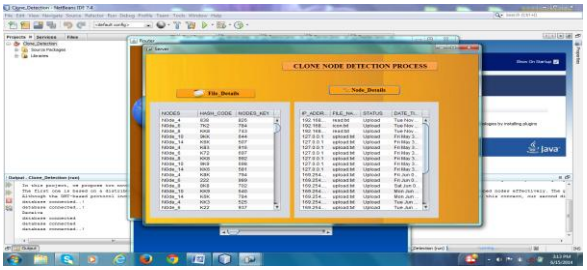


Fig 2 : File details and corresponding Node details

Description: It verifies the nodes by using the network model

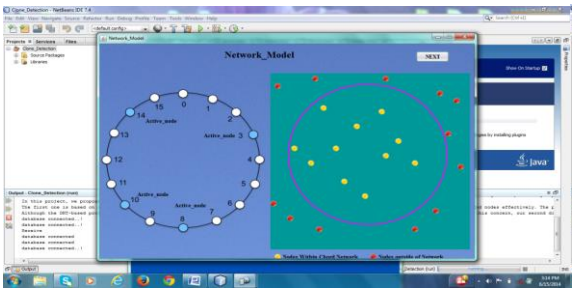


Fig 3 : Network Model

`Description: And it also verifies using rde model and click on next button

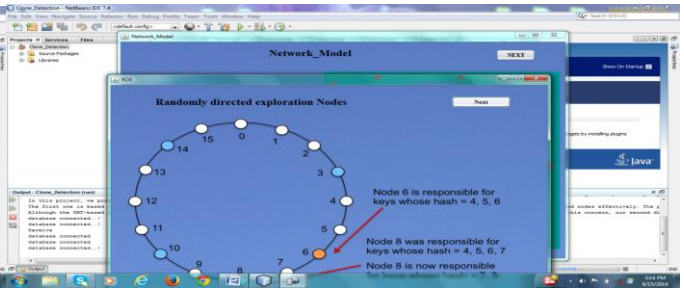


Fig 4 Randomly Directed Exploration Nodes

Description: Then it display the file details and node details.

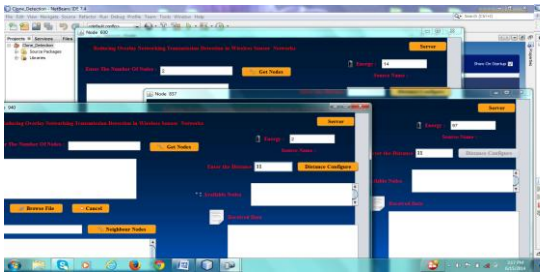


Fig 5 : Appropriate Nodes

Description: Then it displays the 2 appropriate nodes and enter the same clone node occurance

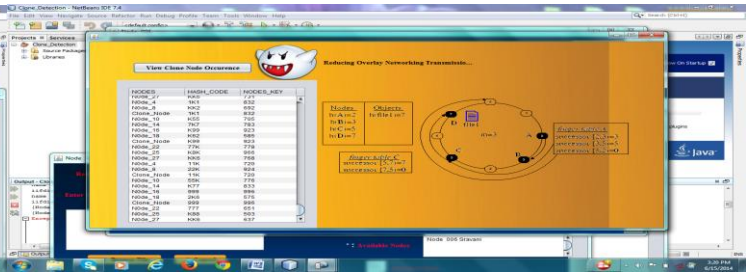


Fig 6: Clone Node Occurance

Description: Then it display the cloned node details. To view the clone node tails click pasted it in the neighbour nodes. And browse the same uploaded file and

V. CONCLUSION AND FUTURE WORK

Sensor nodes lack tamper-resistant hardware and are subject to the node clone attack. In this paper, we present 2 DD protocols: through this protocol centralized ring based proceeded node value with successor node value can be calculated based on hash table, which forms a real time overlay network calculations had been provides the session key-based routing, buffer caching, and error checking facilities for clone node detection and satisfies the detects the abnormalities of node delay. **Future work,** In addition, border determination mechanism is employed to further reduce communication payload.

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, Special Issue 4, April 2015

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

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, 2008.
3. 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.
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, 2008, 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. 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.
7. H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in Proc. 3rd SecureComm, 2007, pp. 341–350.

BIOGRAPHY

D.J.Samatha Naidu received MCA Degree(2005) in Computer Applications from SV University. In 2008 received MPhil degree in Computer Science from the university of MKU, India. In 2010 received the M.Tech Degree in Computer Science and Engineering. At present PhD scholar of Computer Science Vikrama Simhapuri University, espectively. She is currently working as Assistant Professor at APGCCS College. Her research interest includes Computer Networks, Wireless and Sensor networks, software testing. She has published more than 40 papers in related national and international conference proceedings and 18 International journals are published. She is a life member for ISTE, member for IACSIT, IAENG, CSTA, ACM, IAMJSTE.

Dr.A.Prasad has obtained M.Sc(Mathematics), M.Phil(Engineering Mathematics). M.Tech(Computer Science and Technology) and Ph.D(Computer Science & Systems Engineering) from Andhra University, Vishapatanam. He is working as Associate Professor and HOD Department of Computer Science. Vikrama Simhapuri University Nellore, Andhra Pradesh, India with more than 18 years of rich experience in Teaching and Research. He has published 25 and above papers in National and International Journals Conference Proceedings.