IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 07-10
www.iosrjournals.org

Randomly Directed Exploration Protocol with Maximum Throughput and Packet Delivery Ratio

Neenu George [1], T.K.Parani[2]

[1,] *(ECE Department, Dhanalakshmi Srinivasan College of Engineering/ Anna University, India.)*
[2,] *(ECE Department, Dhanalakshmi Srinivasan College of Engineering/ Anna University, India.)*

Abstract: *Wireless sensor networks consist a large number of sensor nodes and physical attack suffered by the wireless sensor network is node clone attack. A node clone detection protocol randomly directed exploration is used to detect node clones using forwarding technique based on probability. The simulation is done using NS2 for detection probability, communication cost and storage consumption. An efficient network always is of both security and quality of services. Along with node clone detection the quality of service multicast routing protocol (MQOSPF), is used to provide the quality of services packet delivery ratio and throughput.*

Keywords- *node clone, NS2, quality of service multicast routing protocol, randomly directed exploration, wireless sensor networks (wsn),*

1. INTRODUCTION

A wireless sensor network (wsn) is an emerging new technology which monitors physical or environmental conditions by spatially distributed autonomous sensors. It is built of large number of nodes and each node act as sensor. The main problem deal with wsn is that it is easy to hack [1]. Between those hacker's attacks, the serious and dangerous one a node clone attack. In this attack the adversary may capture some nodes in the network when they are in hostile environment and extract the secret credentials data and information from nodes, reprograms or modifies the data and creates replicas or clones of such nodes in the network. Then these compromised nodes plays active in network and thus the adversary may gain the control over the network Therefore in this paper, an effective novel node clone detection protocol is proposed to detect the node clones. Distributed detection protocol, named randomly directed exploration (RDE) in which probabilistic directed forwarding technique along with random initial direction and border determination [2].

1.1 Previous works

The earliest method to detect node clones was prevention schemes and key plays the main role which provided to nodes by mobile trusted agents. The private key of node comprises of location and identity. But the problems arise here are attackers may takes some time to compromise the nodes (compromising time) in the network. As the compromising time decreases the number of clone nodes increases, thus badly affects the security of the network. And also prevention scheme is applicable to only some specific applications. The assumption made on trusted agents is not too strong [3] .In the centralized detection method a base station is connected to each node. Each node sends a list of its neighbor nodes and locations to base station. The communication cost is limited by constructing subsets of nodes. Even though communication cost is reduced the lifetime expectancy of the network is decreased due to the communication burden of the nodes near to the base station [4].

2. RANDOMLY DIRECTED EXPLORATION

To overcome the problems a new node clone detection protocol introduced namely randomly directed exploration. Here the each node only needs to know and buffer a neighbor list having all neighbors ID and locations. During detection round each node constructs claiming message with signed version of neighbor list and then deliver messages to others which will compares with its own neighbor list to detect node clone. If there exists any node clone, one witness node successfully catches the clone and notifies the entire network by broadcasting [5].

2.1 Detection round

Initially the node clone detection round is activated by the initiator. At the right mentioned action time, each node creates its own neighbor list (ID of neighbor and location). The claiming message by node is constructed by:

$$M_\alpha = \text{ttl}, \text{id}\alpha, L\alpha, \text{neighbor list} \quad (1)$$

2.2 Algorithm 1

rde-processmessage Mα: An intermediate node processes a message
1: verify the signature of Mα
2: compare own neighbor-list with that in Mα

3: if found clone then
4: broadcast the evidence;
5: ttl<=ttl-1
6: if ttl ≤ 0 then
7: discard Mα
8: else
9: next node<=get next node (Mα) {See Algorithm 2}
10: if next node =NIL then
11: discard Mα
12: else
13: forward Mα to next node

2.3 Algorithm 2

get next node (Mα): To determine the next node that receives the message

1: determine ideal angle then target zone and finally priority zone
2: if no neighbors within the target zone then
3: return NIL
4: if no neighbors within the priority zone then
5: next node<= the node closest to ideal angle
6: else
7: next node<= a probabilistic node in the priority zone
8: return next node.

2.4 Performance parameters

2.4.1Detection Probability

The RDE protocol's detection probability is determined by the number of nodes that are reached when randomly drawing lines where each has a random initial angular and fixed number of nodes along this direction with the border limitation. Let h denote the reachable node number; □, it is a function of (an initial angular),ttl (the number of maximum hops), and v (the number of the claiming messages[5]. Therefore, for a network with n nodes, the detection probability shown in fig 1(a) is given by:

$$P_{RDE}=h\ (ttl, \square, v)/n \qquad (2)$$

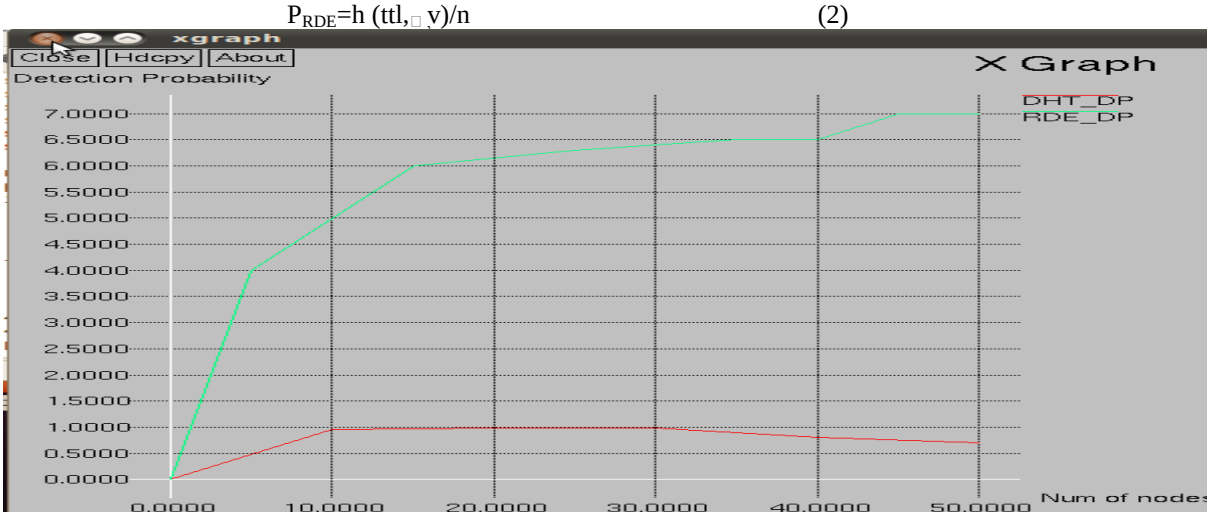

Figure 1(a) storage consumption of randomly directed exploration compared with previous methods

2.4.2Storage Consumption

The RDE protocol is exceedingly memory-efficient. No additional memory is required to suppress broadcasting flood since it does not rely on broadcasting. The protocol does not demand to buffer claiming messages for intermediate nodes, all memory requirement lies on the neighbor-list[1]. Therefore, the protocol consumes almost minimum memory shown in fig 1 (b).

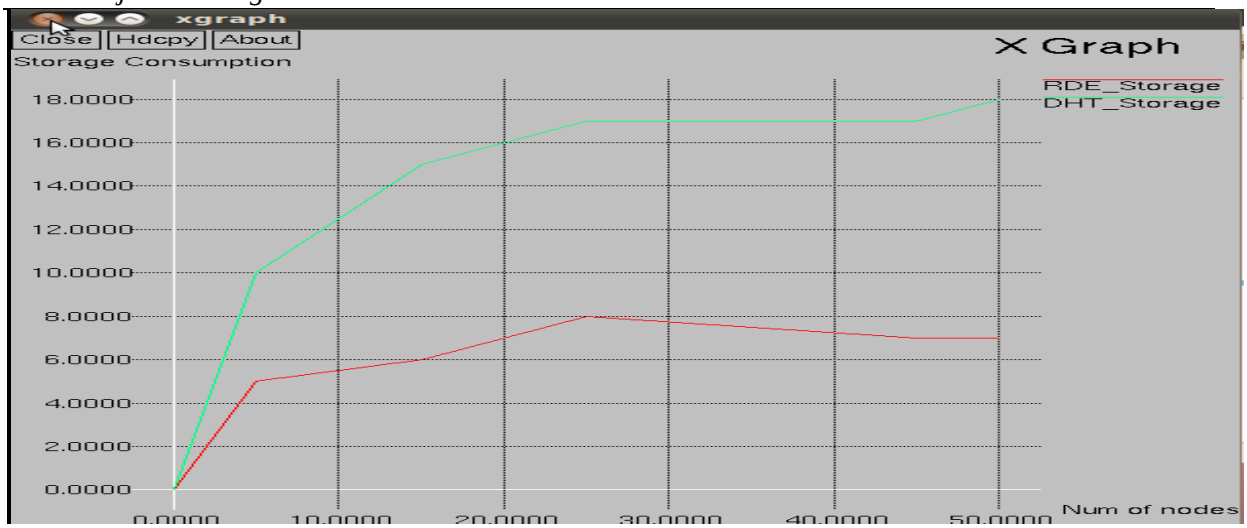

Figure 1(b) detection probability of randomly directed exploration compared with previous methods

3. MULTICAST QOS PATH FIRST PROTOCOL

The network time and space can be reduced by forming self organizing networks and it should support quality of service (QoS). To describe the routing information accurately in these networks is difficult or even impossible. In this paper, self-organizing behaviors are introduced based on bio-inspired networking and a QoS multicast routing scheme based on NS2 is devised to find a QoS multicast path [6]. The MQOSPF Protocol (Multicast extension to QOSPF), is a simple multicast extension version of QOSPF protocol, which uses a scope-limited advertising scheme to limit both control and storage overheads.

1. Look up the best feasible path for a join request.
2. QMRP search.
3. Set up forwarding state and advertise LSA.
4. RIB precomputation[7]

3.1throughput

In communication networks, throughput is the average rate of *successful* message delivery over a communication channel. This data pass through a certain network node. The throughput is usually measured in data packets per second or bits per second (bit/s or bps) or data packets per time slot. The system throughput is the sum of the data rates that are delivered to all terminals in a network. Throughput is essentially similar to consumption. The capacity of the network can be increased by exploiting multi-user diversity and , if delay is not constrained, a source can split the packets of a session and send them too many different neighbors and these neighbors then forward the packets onto the destination when they move into its transmission range[1]. Figure 2(a) explains the throughput improvement.

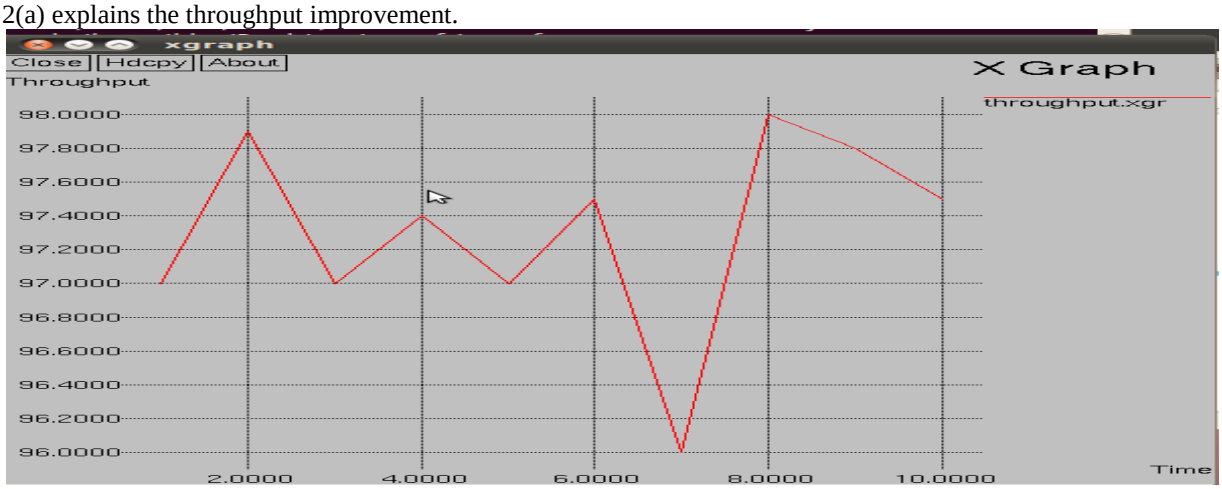

Figure 2(a) throughput

3.2 Packet delivery ratio

The ratio of number of delivered packets to the destination is PDR. The greater value of packet delivery ratio means better performance of protocol. The packets are to be transmitted thru multiple paths. So the delivery ratio and throughput are to be improved [1]. This illustrates the level of delivered data to the destination. Figure 2(b) shows increase in PDR.

$$PDR=\sum \text{Number of packets receive}/\sum \text{number of packets send} \quad (3)$$

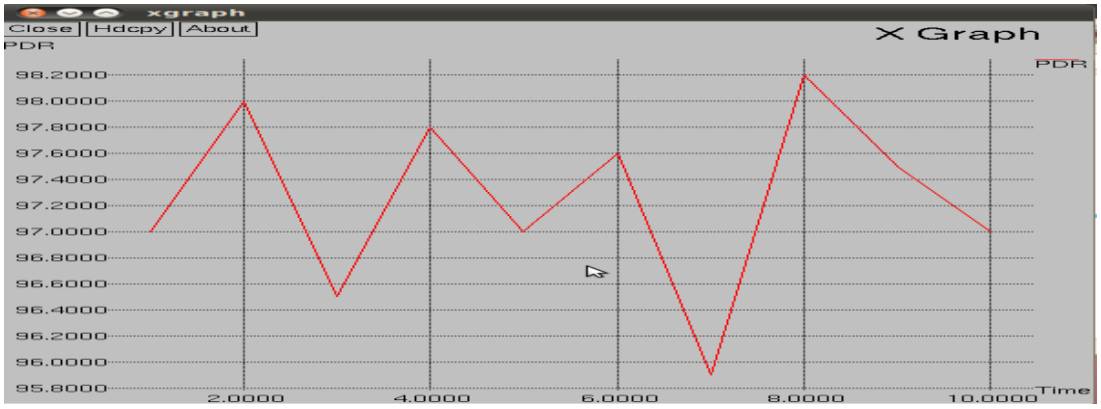

Figure 2(b) Packet Delivery Ratio

4. RESULTS AND CONCLUSIONS

Sensor nodes lack tamper-resistant hardware and are subject to the node clone attack. So a distributed detection protocol is presented which uses probabilistic directed technique to achieve efficient communication overhead for satisfactory detection probability. From the analysis, the randomly directed exploration protocol outperforms all other distributed detection protocols in terms of communication cost and storage requirements. The efficiency of a network comprises of both security and quality of services. The quality of services, namely throughput, packet delivery ratio of the network is improved by implementing an algorithm named QoS multicast routing protocol. So this multicast routing protocol for the QoS provides more efficiency and performance to the network. Thus the proposed method is applicable the military field.

5. ACKNOWLEDGEMENT

I wish to sincerely thank to Mr. M.Tamilarasu M.E, Head of the Department, Department of Electronics and Communication Engineering, Dhanalakshmi Srinivasan College of Engineering, Coimbatore for giving me constant inspiration and motivation to accomplish this work. I extend sincere thanks to Ms.T.K.Parani M.E**,** Internal Guide, Department of Electronics and Communication Engineering for her valuable guidance and suggestions. I express my heartfelt thanks to My Parents and friends for their support throughout my career.

REFERENCES

[1]. www.wikipedia.com
[2]. Zhijun Li, Member, IEEE, and Guang Gong, (2013),".On the Node Clone Detection in Wireless Sensor Networks", in proc *5th IEEE transactions,Volume 40*,no.11,pp 17-23
[3]. C.Bekara And M.L.Maknavicius(2007),"A new protocol for securing wsn against node replication attacks,"in *third IEEE International Conference on wireless and mobile computing, networking and communications*,pp59-59
[4]. B. Parno, A. Perrig, and V. Gligor(2005), "Distributed detection of node replication attacks in sensor networks," in Proc. *IEEE Symp. Security Privacy*, pp. 49–63.
[5]. Zhijun Li And Guang Gong, (2009)"Randomly directed exploration: an efficient node clonedetection protocol in wireless sensor network" ,in proc 5 *th IEEE Trans.Volume 11*,pp34-4.
[6]. Peng Zhang, Raimo Kantola, Zhansong Ma (2009),"Design And Implementation Of a New Routing Simulator" ,in proc.*IEEE IPANA.communication Volume 45*.no.9 pp 345-354.
[7]. Chih-Jen Tseng Chyou-Hwa Chen(2012), "Multicastextensions to QOSPF",in proc NSC 93-2213 e *Volume 23*,no.8 pp. 149-005