ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR

International Journal OF Engineering Sciences & Management Research

RANDOMIZATION OF PATH FOR SECURE DATA COLLECTION IN WIRELESS SENSOR NETWORK

Milet Thottan*, Namitha G.P., Sayan Mukherjee, Sneha.S, S.Rajeswari
Student of B.E.(Information Science),Department of Information Science, New Horizon College of Engineering, India
Student of B.E.(Information Science),Department of Information Science, New Horizon College of Engineering, India
Student of B.E.(Information Science),Department of Information Science, New Horizon College of Engineering, India
Student of B.E.(Information Science),Department of Information Science, New Horizon College of Engineering, India
Assistant Prof., Department of Information Science,New Horizon College of Engineering, India

KEYWORDS: Randomized multipath routing, Purely Random Propagation, Directed Random Propagation, Non Repetitive Random Propagation, Multicast Tree-Assisted Random Propagation.

ABSTRACT
Multiple paths can be created between source and destination nodes in a network by multi-path routing. If the file contents is sent in a deterministic way the adversary might acquire the complete information hence it would lead to loss of data so we divide the file into N packets and traverse them through various random paths. This can be implemented using the following modules namely Purely Random Propagation, Directed Random Propagation, Non Repetitive Random Propagation, Multicast Tree-Assisted Random Propagation. We implement a cross layer strategy mechanism which enables the user to get an acknowledgment on packet receival and black hole acknowledgment on packet loss.

INTRODUCTION
A wireless sensor network (WSNs)[5] is prone to many attacks like denial of service (DOS) and compromised node (CN) [4]. To enhance the security of a WSN, we propose a model where we can make sure that there is no data loss. When we have to send confidential data from a source to destination there are chances that it can go into wrong hands. In order to avoid this we divide the particular file into N packets and each packet is sent through different paths. So even if the external user gets a part of the file it is not possible to get the entire information.

We propose 4 different ways of sending the packets in the network namely Purely Random Propagation (PRP) [1],[2],[3], Directed Random Propagation(DRP)[1],[2],[3], Non Repetitive Random Propagation(NRRP)[1],[2],[3], and Multicast Tree-assisted Random Propagation (MTRP) [1],[2],[3]. We also have a cross layer feedback mechanism where a message is received to the sender when the packet reaches destination. By having this mechanism we can make sure that there is no data loss in the network and also get to know if the message has been hacked. If hacked, the data is sent again through a different path so the destination can have the entire information. The proposed model can increase the efficiency of the network by randomizing the path and collecting the data at the destination. Randomizing is a process of sending the N packets through different path each time.The user himself is not aware of the path being created.The path generated is unique for each and every packet.This can increase the efficiency of the system.The different ways are explained in the later sections.

PURELY RANDOM PROPAGATION
In this type randomizing the source generates a random number which is the port number of the intermediate node(router),once the packet reaches the node,it again generates a random number which leads to the next node. The process continues until the time to live(ttl) value reaches 0 and finally reaches the destination.The algorithm for PRP is as shown below..
Step 1: Start
Step 2: Select IP Address and Browse File Name.
Step 3: Split file into packets and convert data from char to byte format.
Step 4: Create a single random number.
randomInt=randomGenerator();
Step 5: Assign port no to each random no. and send packet to that router
Step 6: In the router repeat Step 5 and 6.
Step 7: Receive Acknowledgment on packet receival.
Step 8: On Back repeat from step 5,6 again.
Step 9: At destination, collect all the packets.
Step 10: Stop

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

DIRECTED RANDOM PROPAGATION

In this type of randomizing the source creates the random path i.e a series of numbers are generated and each number corresponds to the port number of the intermediate nodes. Each node will have information about the next two hops.For example: If the path generated at the source is 1234. The packet travels from node 1-node 2-node 3-node 4.Now node 1 will have information of node 2 and node 3 and node 2 will have information about node 3 and node 4.The algorithm supporting this method is as follows.

Step 1: Start
Step 2: Select IP Address and Browse File Name.
Step 3: Split file into packets & convert data from char to byte format.
Step 4: Each node has info about next 2 nodes.
Step 5: Send the packets in order
Step 6: Upon reaching next node, ACK is sent to its sender
Step 7: Repeat from step 6 until all packets reach destination.
Step 8: Merge packets and original file is obtained.
Step 9: Stop.

NON-REPETITIVE RANDOM PROPAGATION

In this method the mechanism is similar to PRP except that we have an array to hold the traversed path so that the visited port is not used again while generating the random number.The algorithm supporting is given below
Step 1: Start
Step 2: Select IP Address and Browse File Name.
Step 3: Split file into packets and compress
data from char to byte format.
Step 4: Create a single random number.
randomInt=randomGenerator();
Add this number to the traversed array, so that the number is not generated again in a path..
Step 6: Assign port no to each random number and send packet to that router
Step 7: In the router repeat Step 5 and 6.
Step 8: Receive Acknowledgment on packet receival.
Step 9: On Back repeat from step 5,6 again.
Step 10: When all packets reaches destination merge the packets and file is obtained.
Step 11: Stop

MULTICAST TREE ASSISTED RANDOM PROPAGATION

This model we suggest of creating M number of paths and evaluating the cost of the path.The cost efficient path is selected from the generated paths and the data is send through it.By using this method we can make the network energy efficient.The algorithm is as follows.
Step 1:Start
Step 2:Select IP Address and Browse File Name.
Step 3:Split file into packets and convert data from char to byte format.
Step 4: Create a random path.
randomInt=randomGenerator();
a=randomInt%10
b=randomInt/10;
c=b%10;
d=b/10;
Step 5:Assign port no to each random no.
Step 6:Calculate cost of each path and choose the cost effective path and send the packets one by one.

Step 7:Receive Acknowledgment on packet receival.
Step 8:On Back repeat from step 5 again.
Step 9:When all packets reaches destination merge contents and file is obtained.
Step 10:Stop.

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

IMPLEMENTATION AND PROOF OF CONCEPT

In this section we provide the proof of the procedure.
Step 1:We select the ip address and file name and send the contents.

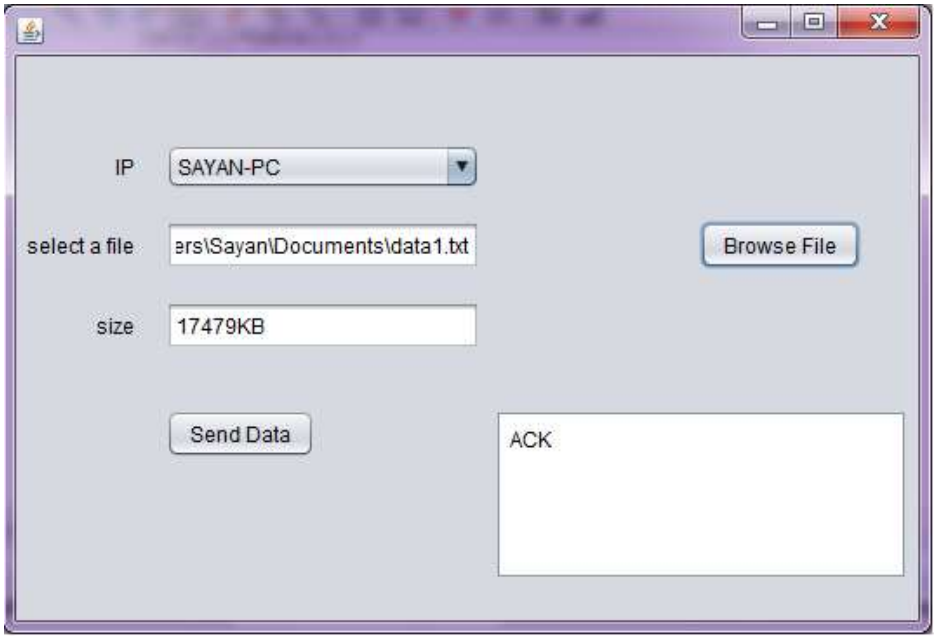

Fig 1:Start the process

If the first packet has reached the destination successfully we get ACK message else we get BNACK message.

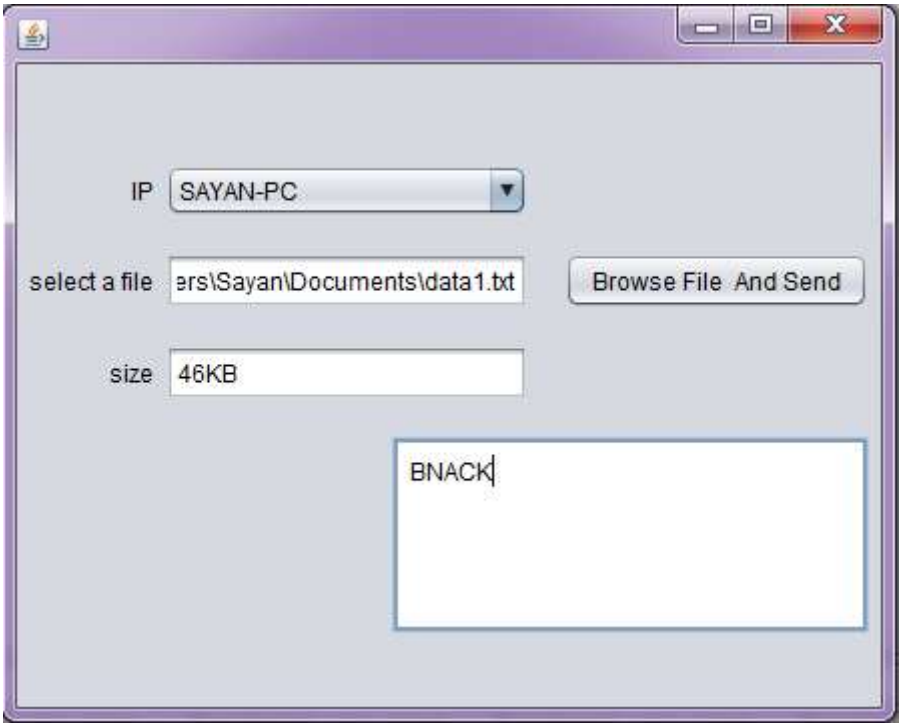

Fig 2: Packet didn't reach the destination

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

Step 2:Split the file into different packets and sending contents through the path created. If a BNACK occurs the path is generated again.

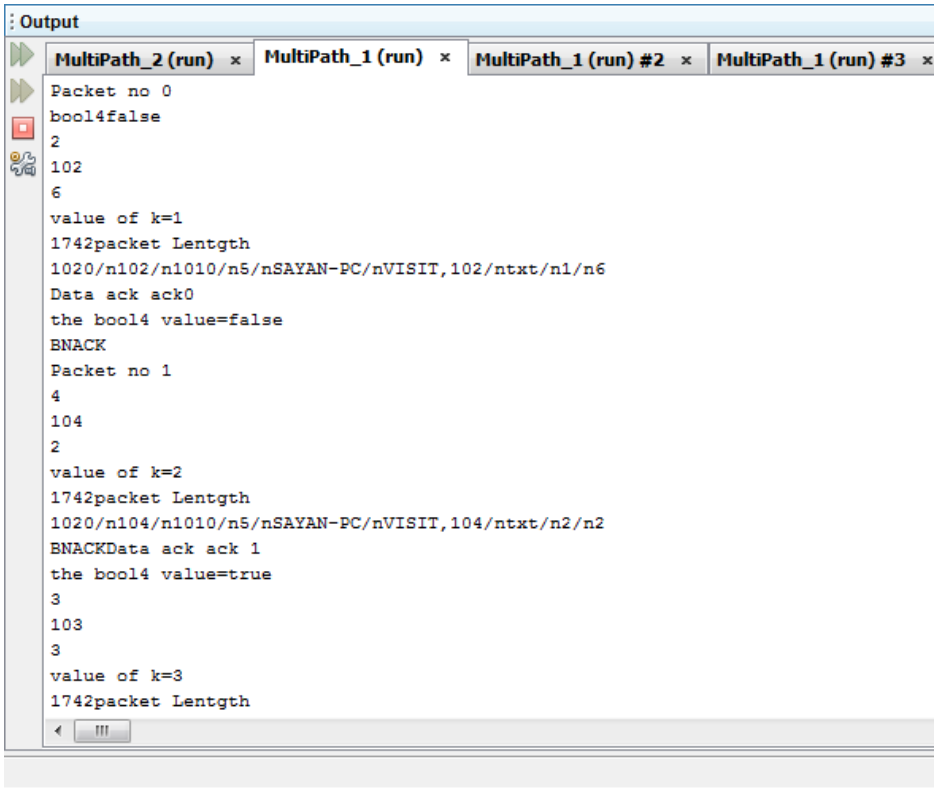

Fig 3: Packet division with prp

Step 3:Different ways of routing like nrrp,prp,mtrp and nrrp.

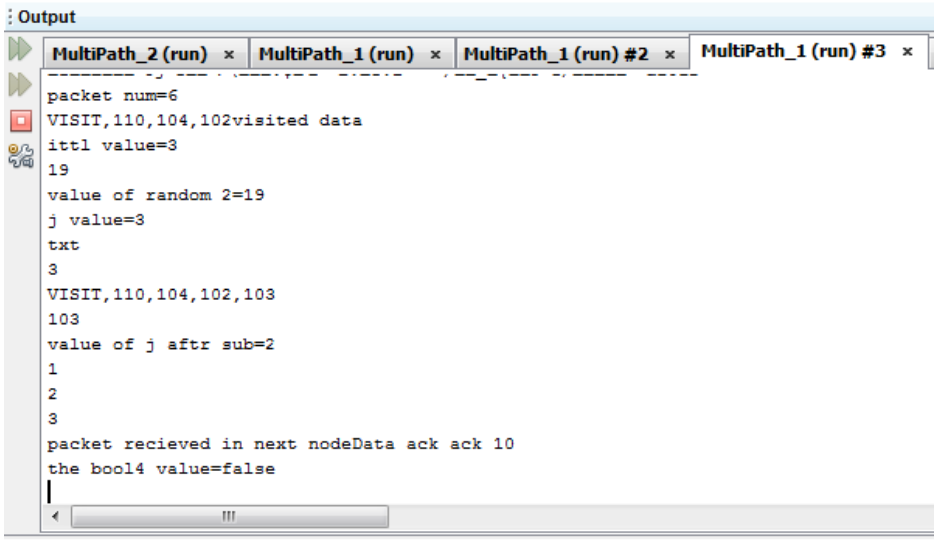

Fig 4:Visited Array in NRRP

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

Fig 5: Different paths in MTRP

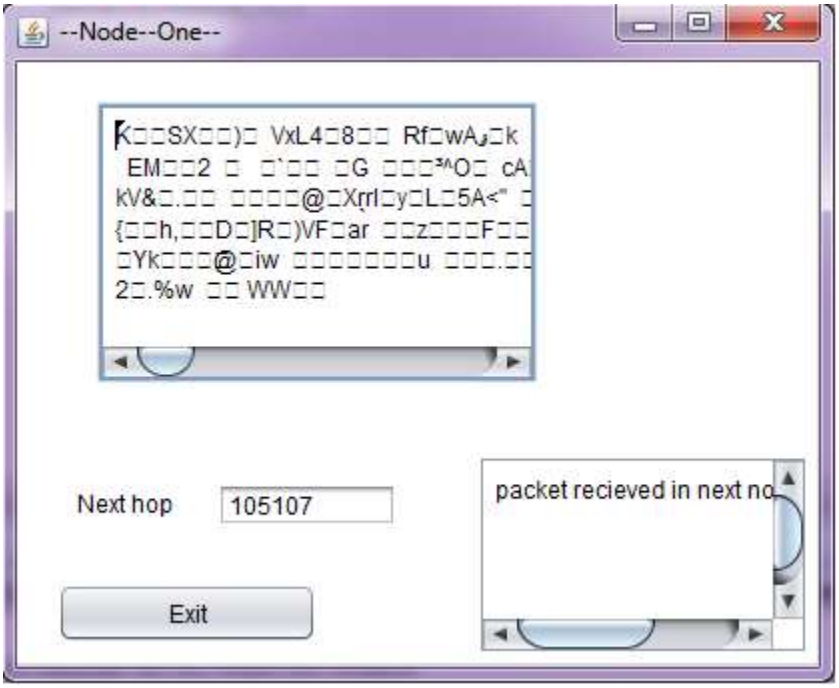

Fig 6:DRRP with the information of the next two hops.

CONCLUSION

In this paper we provide a general framework for securing the data sent through a WSN. With the help of this procedure we can secure data in the presence of security attacks such as CN and DOS. In our implementation procedure we have limited the number of intermediate routers and black holes,but in reality the scenario is different and harder. We will enhance the security[6] of the system further by using an encryption algorithm. In our future work we will try to revise our implementation procedure to fit the real world.

REFERENCES

1. *Multipath routing and secure data collection in WSNs by P.Sudhashini, G.Prema,A.Fairosebanu, Vol 2, issue 7, July 2013.*

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

2. *Random routing algorithms for WSNs by P.B.Manoj, Sai Sandeep Baba,Vol 1, issue 1, March 2012.*
3. *Secure data collection in WSNs using randomized dispersive routes by University of Arizona.*
4. *A framework for identifying compromised nodes in sensor networks by Qing Zhang,Ting Yu, North Carolina State University*
5. *I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40,no. 8,pp. 102-114, Aug. 2002*
6. *P.C. Lee, V. Misra, and D. Rubenstein, "Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks," IEEE/ ACM Trans. Networking, vol. 15, no. 6, pp.1490-1501, Dec.2007*