ISSN 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 1, March 2012

Random Routing Algorithms for Wireless Sensor Networks

P.B.Manoj[1], Sai Sandeep Baba[2]

Asst. Prof, Dept. of ECE, AMC Engg. College, Banglore[1],
Asst. Prof, Dept. of ECE, AMC Engg. College, Bangalore[2],

ABSTRACT— ***Compromised node and denial of service are two key attacks in wireless sensor networks (WSNs). In this paper, we present data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. We observe that the classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once the adversary acquires the routing algorithm, it can compute the same routes known to the source, hence, making all information sent over these routes vulnerable to its attacks. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. In this paper three routing algorithms are presented with simulation results.***

Keywords— Randomized multipath routing, adhoc networks, wireless sensor network, secure data delivery

I. Introduction

Of the various possible security threats encountered in a wireless sensor network (WSN), in this paper, we are specifically interested in combating two types of attacks: compromised node (CN) and denial of service (DOS) [22]. In the CN attack, an adversary physically compromises a subset of nodes to eavesdrop information, whereas in the DOS attack, the adversary interferes with the normal operation of the network by actively disrupting, changing, or even paralyzing the functionality of a subset of nodes. These two attacks are similar in the sense that they both generate black holes: areas within which the adversary can either passively intercept or actively block information delivery. Due to the unattended nature of WSNs, adversaries can easily produce such black holes [1].Severe CN and DOS attacks can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology. A conventional cryptography-based security method cannot alone provide satisfactory solutions to these problems. This is because, by definition, once a node is compromised, the adversary can always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it. Likewise, an adversary can always perform DOS attacks (e.g., jamming) even if it does not have any knowledge of the underlying cryptosystem.

II. Network Model

Wireless Ad hoc network is infrastructure less network. Communication in such type of network is either single hop or multi hop. A node can transmits or receive data to /from a node which lies in its vicinity. A node can transmit data to a longer distance if it has sufficient energy level. In wireless Ad hoc network a node is not only transmitting its own data but it also forward data of other nodes. Resources available in scarce at a node may halt the data transmission either temporarily or permanently. All the nodes in the wireless Ad hoc network are battery operated and the life time of the network depends upon the available battery power of a node. A node after data transmission may reach to a threshold level. If the battery power of a node reaches to threshold value, then node is not in position to either accept the data or send the data to other nodes in the network. In this situation a node is excluded from the available path.

Similarly if such types of nodes are in large number then more number of paths will not be available to send the data to other nodes and it may be possible that network is of no use. The position of a node in wireless Ad hoc network is not fixed. Mobility of nodes are very high. The range of data transmission of every node is not fixed it changes according to the position of node. The coverage area is different for different node. Consider a node 'i' wants to transmit data to a node ‘j’. Node 'i' can transmit data directly to ‘j’ if and only if they are in transmission range of each other and node ' i' has sufficient battery power for data transmission. Source node can also send its data with the help of other intermediate nodes, which lies in its vicinity. In Fig 1 the total area of a network is 'r' and let say the transmission range of inner circle node is 'rl'. Where (rl <r). The nodes which are situated 'rl' distance from each other can transmit data directly to each other without any interference.

ISSN 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 1, March 2012

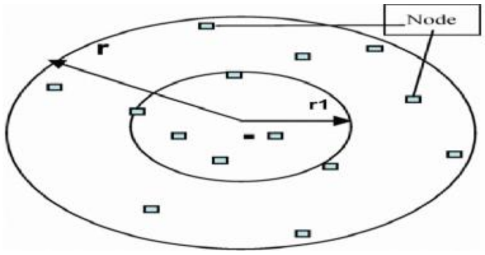


Fig. 1: Illustration of Transmission area.

The node situated at the periphery i.e. the distance between two nodes is 'r' then it is the maximum distance between 2 nodes. Here two cases arises either a node transmit data directly destination, if it has sufficient battery power or it can send the data with the help of intermediate nodes. Whenever a node wants to transmit data beyond its range, data may collide due interference problem.

III. Purely Random Propagation Routing

To diversify routes, an ideal random propagation algorithm would propagate shares as dispersive as possible. Typically, this means propagating the shares farther from their source. At the same time, it is highly desirable to have an energy-efficient propagation, which calls for limiting the number of randomly propagated hops. A share may be sent one hop farther from its source in a given step, but may be sent back closer to the source in the next step, wasting both steps from a security standpoint. To tackle this issue, some control needs to be imposed on the random propagation process.

In PRP, shares are propagated based on one-hop neighbourhood information. More specifically, a sensor node maintains a neighbour list, which contains the ids of all nodes within its transmission range. When a source node wants to send shares to the sink, it includes a TTL of initial value N in each share. It then randomly selects a neighbour for each share, and unicasts the share to that neighbour. After receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than 0, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node) and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing it toward the sink using normal min-hop routing. The WANDERER scheme [2] is a special case of PRP with N 1/41. The main drawback of PRP is that its propagation efficiency can be low, because a share may be propagated back and forth multiple times between neighbouring hops.

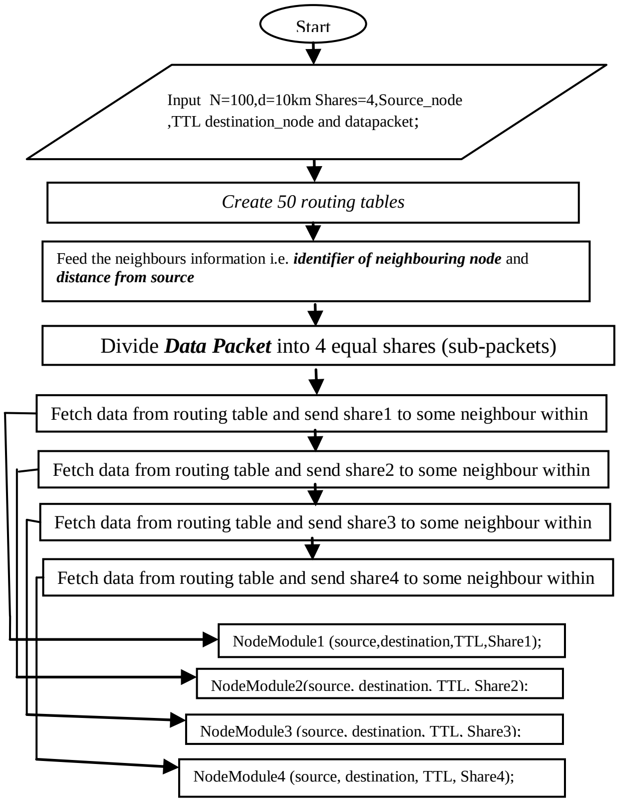

Start
Input N=100,d=10km Shares=4,Source_node ,TTL destination_node and datapacket;
Create 50 routing tables
Feed the neighbours information i.e. identifier of neighbouring node and distance from source
Divide Data Packet into 4 equal shares (sub-packets)
Fetch data from routing table and send share1 to some neighbour within
Fetch data from routing table and send share2 to some neighbour within
Fetch data from routing table and send share3 to some neighbour within
Fetch data from routing table and send share4 to some neighbour within
NodeModule1 (source,destination,TTL,Share1);
NodeModule2(source. destination. TTL. Share2):
NodeModule3 (source. destination. TTL. Share3):
NodeModule4 (source, destination, TTL, Share4);

Fig. 2: Global PRP Algorithm

Fig. 2 describes a situation where global PRP is used to divide the packets into shares and transmit them over randomly dispersed route.

PRP Routing algorithm details are described in the following figure.

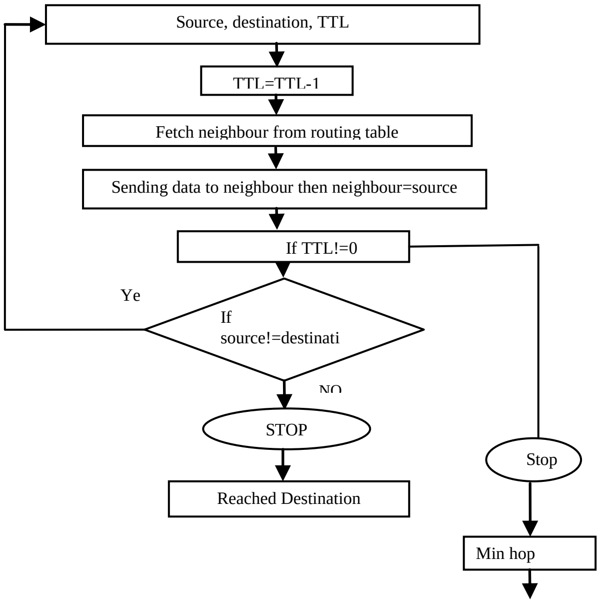


Fig. 3: Detail Summary of PRP Algorithm

The PRP module as in Fig. 3 contains sub-modules which has the responsibility of routing all single Share using Purely Random Propagation Scheme.

IV. Non repetitive Random Propagation (NRRP)

NRRP is based on PRP, but it improves the propagation Efficiency by recording the nodes traversed so far. Specifically, NRRP adds a "node-in-route" (NIR) field to the header of each share. Initially, this field is empty. Starting from the source node, whenever a node propagates the share to the next hop, the id of the upstream node is appended to the NIR field. Nodes included in NIR are excluded from the random pick at the next hop. This non repetitive propagation guarantees that the share will be relayed to a different node in each step of random propagation, leading to better propagation efficiency.

V. Directed Random Propagation (DRP)

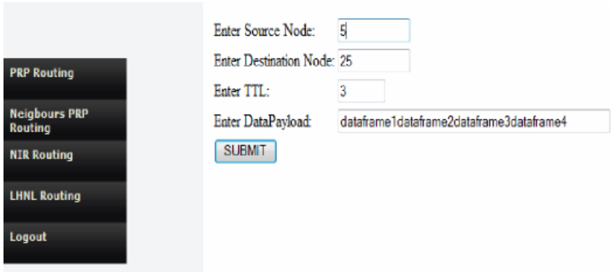
DRP improves the propagation efficiency by using two hop neighbourhood information. More specifically, DRP adds a "last-hop neighbor list" (LHNL) field to the header of each share. Before a share is propagated to the next node, the relaying node first updates the LHNL field with its neighbor list. When the next node receives the share, it compares the LHNL field against its own neighbor list, and randomly picks one node from its neighbors that are not in the LHNL. It then decrements the TTL value, updates the LHNL field, and relays the share to the next hop, and so on. Whenever the LHNL fully overlaps with or contains the relaying node's neighbor list, a random neighbor is selected, just as in the case of the PRP scheme According to this propagation method, DRP reduces the chance of propagating a share back and forth by eliminating this type of propagation within any two consecutive steps. Compared with PRP, DRP attempts to push a share outward away from the source, and thus, leads to better propagation efficiency for a given TTL value.

VI. Simulation Results

In this section the simulation results with route traces are presented

Case (1): Routing Using PRP

Input Data

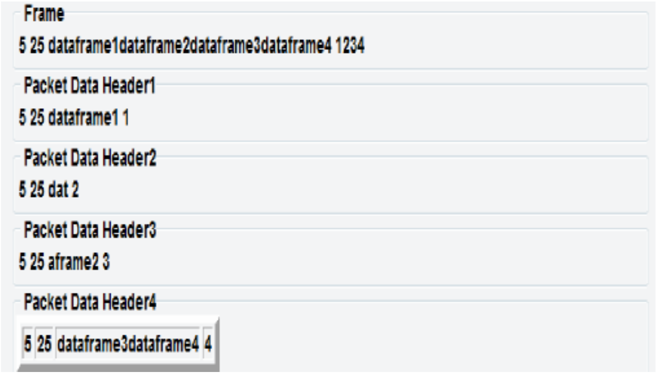


Enter Source Node: 5
Enter Destination Node: 25
Enter TTL: 3
Enter DataPayload: dataframe1dataframe2dataframe3dataframe4

Fig. 4: Input to PRP routing algorithm ***Output***

Fig. 4 shows the user interface where the source node, destination node, TTL is given as input developed in using java

Output Data

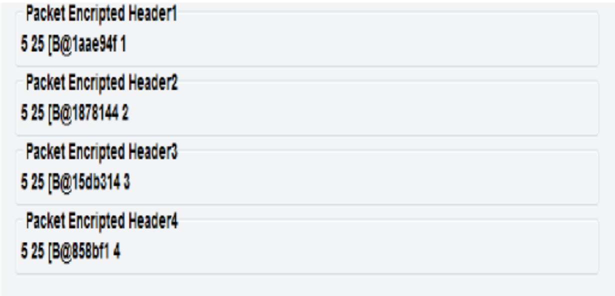


```
Frame
5 25 dataframe1dataframe2dataframe3dataframe4 1234
Packet Data Header1
5 25 dataframe1 1
Packet Data Header2
5 25 dat 2
Packet Data Header3
5 25 aframe2 3
Packet Data Header4
5 25 dataframe3dataframe4 4
```

Fig. 5: PRP Packet Formation

Fig. 5 shows the PRP Algorithm frame formation and division of entire frame into four different packets.

Output of PRP Algorithm Packet Formation with Encryption

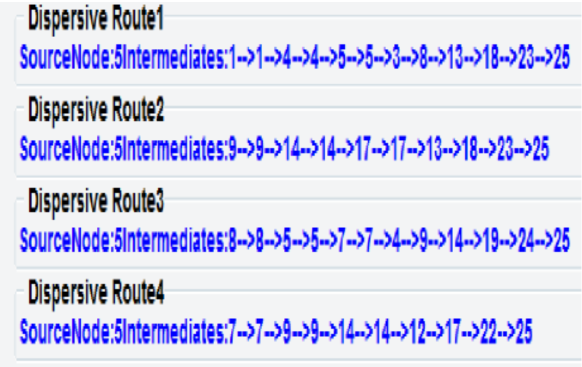


```
Packet Encripted Header1
5 25 [B@1aae94f 1
Packet Encripted Header2
5 25 [B@1878144 2
Packet Encripted Header3
5 25 [B@15db314 3
Packet Encripted Header4
5 25 [B@858bf1 4
```

Fig. 6 : PRP Algorithm Encryption Output using Triple DES

Fig. 6 shows packet formation output containing source Ip=5, Destination Ip=25 and various packets and data payload encrypted using Triple DES algorithm.

Output of PRP Algorithm Trace Routes

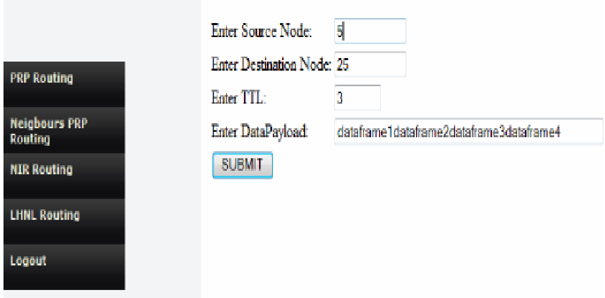


```
Dispersive Route1
SourceNode:5Intermediates:1-->1-->4-->4-->5-->5-->3-->8-->13-->18-->23-->25
Dispersive Route2
SourceNode:5Intermediates:9-->9-->14-->14-->17-->17-->13-->18-->23-->25
Dispersive Route3
SourceNode:5Intermediates:8-->8-->5-->5-->7-->7-->4-->9-->14-->19-->24-->25
Dispersive Route4
SourceNode:5Intermediates:7-->7-->9-->9-->14-->14-->12-->17-->22-->25
```

Fig. 7: PRP Algorithm Dispersive routes output

Fig. 7 gives the dispersive routes to send the packets from source node 5 to the destination node 25.

Case (2): NRRP Routing Algorithm

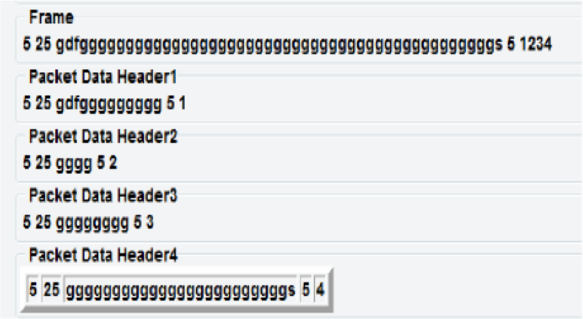


Enter Source Node: 5
Enter Destination Node: 25
Enter TTL: 3
Enter DataPayload: dataframe1dataframe2dataframe3dataframe4

Fig. 8: Input to NRRP routing algorithm

Fig. 8 shows the user interface where the source node, destination node, TTL is given as input.

Output of PRP Algorithm Packet Formation

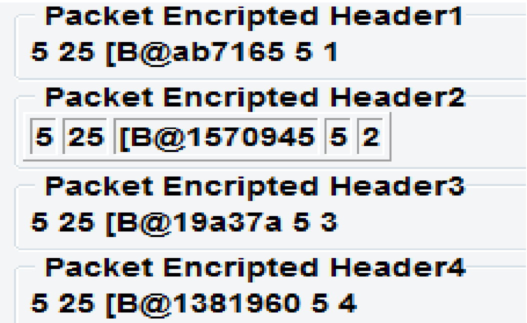


```
Frame
5 25 gdfggggggggggggggggggggggggggggggggggggggggggggggggggggs 5 1234
Packet Data Header1
5 25 gdfgggggggg 5 1
Packet Data Header2
5 25 gggg 5 2
Packet Data Header3
5 25 ggggggg 5 3
Packet Data Header4
5 25 ggggggggggggggggggggggggs 5 4
```

Fig. 9: NRRP Packet Formation

Fig. 9 shows the NRRP Algorithm frame formation and division of entire frame into four different packets the only difference with PIR is. Here the NIR field will also be added.

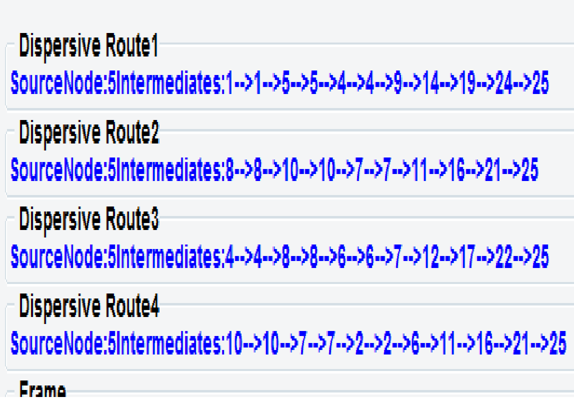
Output of NRRP Algorithm Packet Formation with Encryption



```
Packet Encripted Header1
5 25 [B@ab7165 5 1
Packet Encripted Header2
5 25 [B@1570945 5 2
Packet Encripted Header3
5 25 [B@19a37a 5 3
Packet Encripted Header4
5 25 [B@1381960 5 4
```

Fig. 10: PRP Algorithm Encryption Output using Triple DES

In Fig. 10 packet formation of NRRP algorithm with encrypted packet data payload is described using triple DES algorithm.



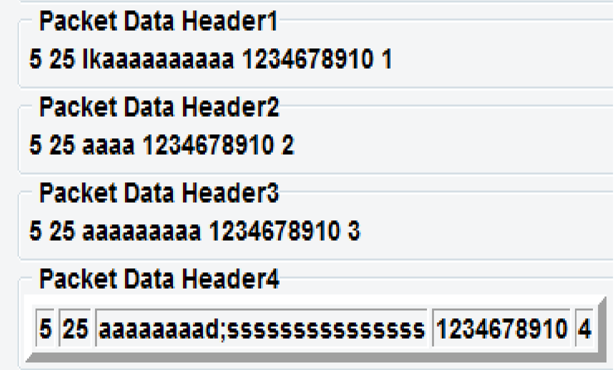
```
Dispersive Route1
SourceNode:5Intermediates:1-->1-->5-->5-->4-->4-->9-->14-->19-->24-->25
Dispersive Route2
SourceNode:5Intermediates:8-->8-->10-->10-->7-->7-->11-->16-->21-->25
Dispersive Route3
SourceNode:5Intermediates:4-->4-->8-->8-->6-->6-->7-->12-->17-->22-->25
Dispersive Route4
SourceNode:5Intermediates:10-->10-->7-->7-->2-->2-->6-->11-->16-->21-->25
Frame
```

Fig. 11: NRRP Algorithm

Fig. 11 gives the dispersive routes to send the packets from source node 5 to the destination node 25.

Case3: Routing Algorithm DRP

Output of DRP Algorithm Packet Formation

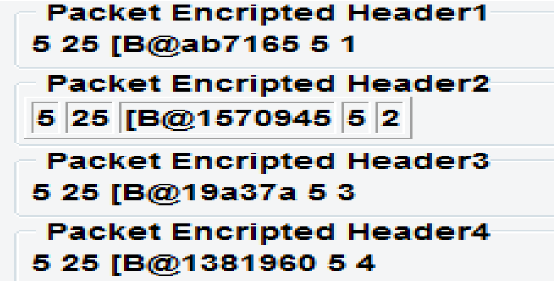


```
Packet Data Header1
5 25 Ikaaaaaaaaaa 1234678910 1
Packet Data Header2
5 25 aaaa 1234678910 2
Packet Data Header3
5 25 aaaaaaaaa 1234678910 3
Packet Data Header4
5 25 aaaaaaaad;ssssssssssssssss 1234678910 4
```

Fig. 12: NRRP Packet Formation

Fig. 12 shows the DRP Algorithm frame formation and division of entire frame into four different packets the only difference with PIR is. Here the LHNL field will also be added.

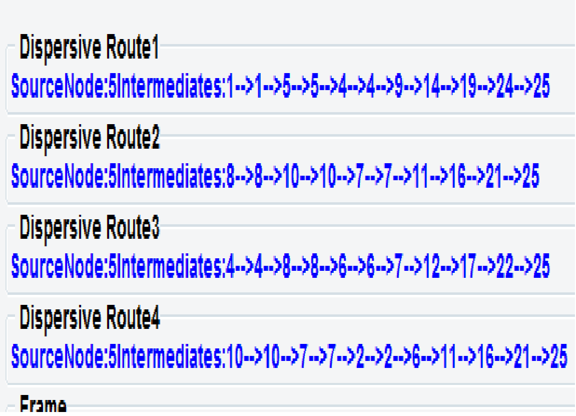
Output of DRP Algorithm Packet Formation with Encryption



```
Packet Encripted Header1
5 25 [B@ab7165 5 1
Packet Encripted Header2
5 25 [B@1570945 5 2
Packet Encripted Header3
5 25 [B@19a37a 5 3
Packet Encripted Header4
5 25 [B@1381960 5 4
```

Fig. 13: PRP Algorithm Encryption Output using Triple DES

In Fig. 13 packet formation of DRP algorithm with encrypted packet data payload is formed using triple DES algorithm



```
Dispersive Route1
SourceNode:5Intermediates:1-->1-->5-->5-->4-->4-->9-->14-->19-->24-->25
Dispersive Route2
SourceNode:5Intermediates:8-->8-->10-->10-->7-->7-->11-->16-->21-->25
Dispersive Route3
SourceNode:5Intermediates:4-->4-->8-->8-->6-->6-->7-->12-->17-->22-->25
Dispersive Route4
SourceNode:5Intermediates:10-->10-->7-->7-->2-->2-->6-->11-->16-->21-->25
Frame
```

Fig. 14: DRP Algorithm

Fig. 14 gives the dispersive routes to send the packets from source node 5 to the destination node 25 using DRP Routing algorithm.

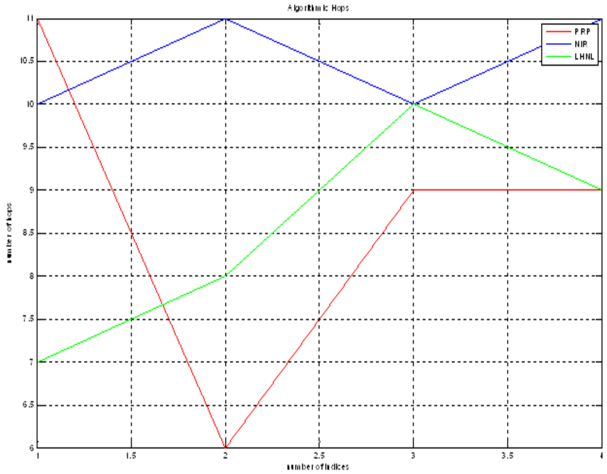


Fig. 15: Number of Hops in PRP, NRRP and DRP Algorithms

Fig. 15 shows the number of algorithmic hops taken for a data payload from the source to destination for all the three algorithms

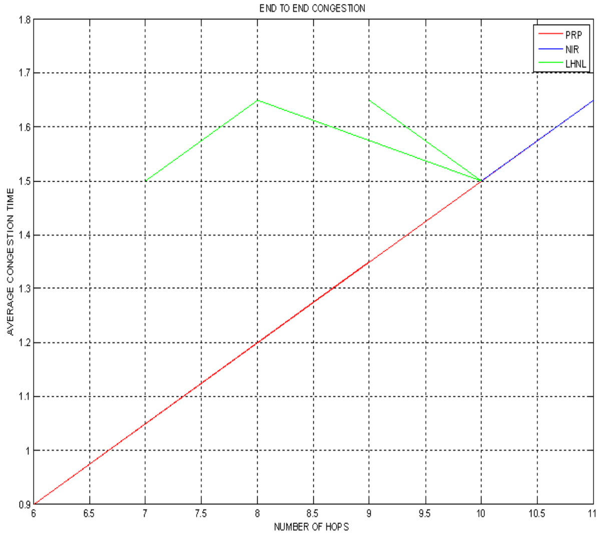


Fig. 16: End to End Congestion in PRP, NRRP and DRP Algorithms

In Fig. 16 the marking level makes sure that there are very few congestion related losses, most of the packet losses seen by the user are indeed due to network losses.

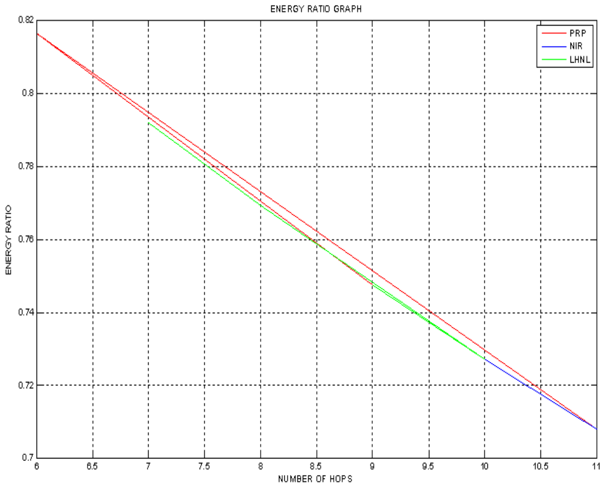


Fig. 17: Energy ratio of PRP, NRRP and DRP Algorithms

Fig. 17 shows that energy savings are obtained when arbitrary number of nodes are placed between source S and destination D, and these nodes are used to retransmit the message.

VII. CONCLUSION

Our analysis and simulation results have shown the effectiveness of the randomized dispersive routing in combating CN and DOS attacks. By appropriately setting the secret sharing and propagation parameters, the packet interception probability can be easily reduced by the proposed algorithm which is at least one order of magnitude smaller than approaches that use deterministic node-disjoint multipath routing. From the simulation results one can conclude that in PRP routing algorithm is less efficient because the packet can transverse back and forth. In NRRP the dispersive routes will avoid back and forth propagation because of NIR fields storage. DRP routing algorithm works even better because of comparison of two LHNL fields.

VIII. REFERENCES

[1] 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.

[2] C.L. Barrett, S.J. Eidenbenz, L. Kroc, M. Marathe, and J.P. Smith, "Parametric Probabilistic Sensor Network Routing," Proc. ACM Int'l Conf. Wireless Sensor Networks and Applications (WSNA),pp. 122-131, 2003.

[3] M. Burmester and T.V. Le, "Secure Multipath Communication in Mobile Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, pp. 405-409, 2004.

[4] T. Claveirole, M.D. de Amorim, M. Abdalla, and Y. Viniotis,"Securing Wireless Sensor Networks Against Aggregator Compromises," IEEE Comm. Magazine, vol. 46, no. 4, pp. 134-141, Apr. 2008.

[5] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The DynamicSource Routing Protocol for Multihop Wireless Ad Hoc Networks,"Ad Hoc Networking, C.E. Perkins, ed., pp. 139-172,Addison-Wesley, 2001.

[6] P.C. Lee, V. Misra, and D. Rubenstein, “Distributed Algorithms for Secure Multipath Routing,” Proc. IEEE INFOCOM, pp. 1952-1963, Mar. 2005.
[7] 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.
[8] S.J. Lee and M. Gerla, “Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks,” Proc. IEEE Int’l Conf. Comm. (ICC), pp. 3201-3205, 2001.
[9] X.Y. Li, K. Moaveninejad, and O. Frieder, “Regional Gossip Routing Wireless Ad Hoc Networks,” ACM J. Mobile Networks and Applications, vol. 10, nos. 1-2, pp. 61-77, Feb. 2005.
[10] W. Lou and Y. Kwon, “H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks,” IEEE Trans. Vehicular Technology, vol. 55, no. 4, pp. 1320- 1330, July 2006.
[11] W. Lou, W. Liu, and Y. Fang, “Spread: Enhancing Data Confidentiality in Mobile Ad Hoc Networks,” Proc. IEEE INFOCOM, vol. 4, pp. 2404-2413, Mar. 2004.
[12] W. Lou, W. Liu, and Y. Zhang, “Performance Optimization Using Multipath Routing in Mobile Ad Hoc and Wireless Sensor Networks,” Proc. Combinatorial Optimization in Comm. Networks,pp. 117-146, 2006.
[13] M.K. Marina and S.R. Das, “On-Demand Multipath Distance Vector Routing in Ad Hoc Networks,” Proc. IEEE Int’l Conf Network Protocols (ICNP), pp. 14-23, Nov. 2001.
[14] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, “SecMR—a Secure Multipath Routing Protocol for Ad Hoc Networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, Jan. 2007.
[15] N.F. Maxemchuk, “Dispersity Routing,” Proc. IEEE Int’l Conf.Comm. (ICC), pp. 41.10-41.13, 1975.
[16] P. Papadimitratos and Z.J. Haas, “Secure Routing for Mobile Ad Hoc Networks,” Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), 2002.
[17] P. Papadimitratos and Z.J. Haas, “Secure Data Communication in Mobile Ad Hoc Networks,” IEEE J. Selected Areas in comm., vol. 24, no. 2, pp. 343-356, Feb. 2006.
[18] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, “SPINS: Security Protocols for Sensor Networks,” Proc. ACM MobiCom,2001.SHU ET AL.: SECURE DATA COLLECTION IN WIRELESS SENSOR NETWORKS USING RANDOMIZED DISPERSIVE ROUTES 953
[19] B. Vaidya, J.Y. Pyun, J.A. Park, and S.J. Han, “Secure Multipath Routing Scheme for Mobile Ad Hoc Network,” Proc. IEEE Int’l Symp. Dependable, Autonomic and Secure Computing, pp. 163-171,2007.
[20] A.D. Wood and J.A. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

Biography

Mr. P. B. Manoj received his masters degrees in Information technology from Visvesvaraya Technological University, Belgaum, Karnataka, India. His research interests include mobile wireless networks, sensor networks, parallel and clustering computing, and performance modeling and evaluation. He has authored/co-authored several technical papers In the areas of computer networking, performance evaluation, and parallel and distributed computing. He is currently an Assistant Professor in the Department of Electronics and Communication Engineering ,AMC Engineering college,VTU,Karnataka.

Mr. Sai Sandeep Baba received his master’s degree in Digital Electronics and Communications from Visvesvaraya Technological University, Belgaum, Karnataka, India. His research areas interests include mobile wireless networks, GSM,CDMA. He has authored/coauthored several technical papers. He has presented papers in several national, international conferences and international journals in the areas of computer networking, performance evaluation, and parallel and distributed computing. He is currently an assistant professor in the Department of Electronics & Communication Engineering ,AMC Engineering college,VTU,Karnataka.