International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

Secure Data Collection in Wireless Sensor Networks using Randomized Dispersive Routes

T.L.Priyadarsini, Asst.Prof,
Dept.of Computer Science and Engineering, VNRVJIET, Telangana, India

---

Abstract- ***The Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs).We study routing mechanisms that circumvent (bypass) black holes formed by these attacks. We argue that existing multi-path routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. In this paper, we develop mechanisms that generate randomized multipath routes. Under our design, the routes taken by the "shares" of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the routes generated by our mechanisms are also highly dispersive and energy-efficient, making them quite capable of bypassing black holes at low energy cost. Extensive simulations are conducted to verify the validity of our mechanisms. Instead of selecting paths from a pre-computed set of routes, our aim is to compute multiple paths in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically infeasible. A naive algorithm of generating random routes, such as Wanderer scheme (a pure random-walk algorithm), only leads to long paths (containing many hops, and therefore, consuming lots of energy) without achieving good dispersiveness. Due to security considerations, its required that the route computation be implemented in a distributed way, such that the final route represents the aggregate decision of all the nodes participating in the route selection. Randomized route selection algorithm only incurs a small amount of communication overhead. As a result, a small number of colluding/compromised nodes cannot dominate the selection result.***

Key Words: *Energy-Efficient, Colluding, Black Holes.*

1. INTRODUCTION

1.1. Black Holes Attack

Of the various possible security threats that may be experienced by a wireless sensor network (WSN), in this paper we are specifically interested in combating two types of attacks: the compromised-node (CN) attack and the Denial-of-Service (DoS) attack. The CN attack refers to the situation when 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 WSN by actively disrupting, changing, or even destroying the functionality of a subset of nodes in the system. 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. 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. At the same time, an adversary can always perform certain form of DOS attack (e.g., jamming) even if it does not have any knowledge of the crypto-system used in the WSN.

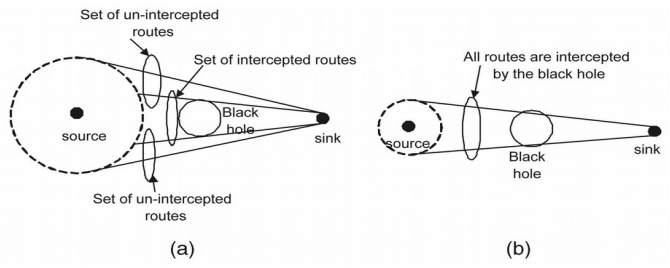
1.2. Solution for this kind of attacks:

One remedial solution to these attacks is to exploit the network's routing functionality. Specifically, if the locations of the black holes formed by the compromised (or jammed) nodes are known a priori, then information can be delivered over paths that circumvent (bypass) these holes, whenever possible. In practice, due to the difficulty of acquiring such location information, the above idea is implemented in a probabilistic manner, typically through a two-step process: secret sharing and multi-path routing.

First, an information (e.g., a packet) is broken into First, an information (e.g., a packet) is broken into M shares (i.e., components of a packet that carry partial information) using a (T,M)-threshold secret-sharing mechanism such as the Shamir's algorithm. The original information can be recovered from a combination of at least T shares, but no information can be guessed from less than T shares. Then, multiple routes from the source to the destination are computed according to some multi-path routing algorithm. These routes are node-disjoint or maximal node-disjoint subject to certain constraints (e.g., minhop routes). The M shares are then distributed across these routes and delivered to the destination, following different paths.

1.3. Main contributions are as follows:

As we consider a three-phase approach for secure information delivery in a WSN: secret sharing of information, randomized propagation of each information share, and normal routing (e.g., min-hop routing) toward the sink. More specifically, when a sensor node wants to send a packet to the sink, it first breaks the packet into M shares, according to a ðT; MÞ-threshold secret sharing algorithm, e.g., Shamir's algorithm. Each share is then transmitted to some randomly selected neighbor. That neighbor will continue to relay the share it has received to other randomly selected neighbors, and so on. In each share, there is a TTL field, whose initial value is set by the source node to control the total number of random relays. After each relay, the TTL field is reduced by 1.When the TTL value reaches 0, the last node to receive this share begins to route it toward the sink using min-hop routing. Once the sink collects at least T shares, it can reconstruct the original packet. No information can be recovered from less than T shares. The effect of route depresiveness on bypassing black holes is illustrated in Fig 1, where the dotted circles represent the ranges the secret shares can be propagated to in the random propagation phase. A larger dotted circle implies that the resulting routes are geographically more dispersive. Comparing the two cases in Fig 1, it is clear that the routes of higher dispersiveness are more capable of avoiding the black hole. Clearly, the random propagation phase is the key component that dictates the security and energy performance of the entire mechanism.



(a) Higher dispersiveness.(b)lower dispersiveness.

Fig 1 Implication of route dispersiveness on by passing the black hole.

2. RANDOM PROPAGATION OF INFORMATION SHARES

To diversify routes, an ideal random propagation algorithm would propagate shares as depressively 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. The challenge here lies in the random and distributed nature of the propagation: 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. We explore the potential of random dispersion for information delivery in WSNs. Depending on the type of information available to a sensor; we develop four distributed schemes for propagating information "shares":

1. Purely random propagation (PRP),
2. Directed random propagation (DRP),
3. Non repetitive random propagation (NRRP), and
4. Multicast tree assisted random propagation (MTRP).

PRP utilizes only one-hop neighborhood information and provides baseline performance. DRP utilizes two-hop neighborhood information to improve the propagation efficiency, leading to a smaller packet interception probability. The NRRP scheme achieves a similar effect, but in a different way: it records all traversed nodes to avoid traversing them again in the future. MTRP tries to propagate shares in the direction of the sink, making the delivery process more energy efficient.

Theoretically evaluate the goodness of these dispersive routes in terms of avoiding black holes. We conduct asymptotic analysis (i.e., assuming an infinite number of nodes) for the worst-case packet interception probability and energy efficiency under the baseline PRP scheme. Our results can be interpreted as the performance limit of PRP, and a lower-bound on the performance of the more advanced DRP, NRRP, and MTRP schemes. Our analysis helps us better to understand how security is achieved under dispersive routing. Based on this analysis, we investigate the trade-off between the random propagation parameter and the secret sharing parameter. We further optimize these parameters to minimize the end-to-end energy consumption under a given security constraint. Conducting extensive simulations to study the performance of the proposed schemes under more realistic settings. Our simulation results are used to verify the effectiveness of our

design. When the parameters are appropriately set, all four randomized schemes are shown

to provide better security performance at a reasonable energy cost than their deterministic counterparts. At the same time, they do not suffer from the type of attacks faced by deterministic multipath routing as described in following fig 3.

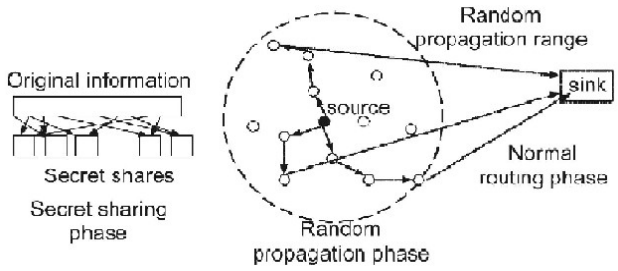


Fig 2 Randomized dispersive routes in a WSN

2.1 Purely random propagation -PRP (Baseline Scheme):

In PRP, shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor 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 neighbor for each share, and unicasts the share to that neighbor. 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 ¼1.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 neighboring hops. As shown in the analysis and simulations in subsequent sections, increasing the TTL value does not fully address this problem. This is because the random propagation process reaches steady state under a large TTL, and their distributions will no longer change even if the TTL becomes larger which can be seen in fig 1.

2.2 Directed random propagation (DRP)

DRP improves the propagation efficiency by using two-hop neighborhood 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 LHN"'L 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.

2.3 Non repetitive Random Propagation

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 no repetitive propagation guarantees that the share will be relayed to a different node in each step of random propagation, leading to better propagation efficiency.

2.4 Multicast Tree-Assisted Random Propagation

MTRP aims at actively improving the energy efficiency of random propagation while preserving the dispersive ness of DRP. The basic idea comes from the following observation of Fig 2. Among the three different routes taken by shares, the route on the bottom right is the most energy efficient because it is the shortest end-to-end path. So, in order to improve energy efficiency, shares should be best propagated in the direction of the sink. In other words, their propagation should be restricted to the right half of the circle in Fig 2. Conventionally, directional routing requires location information of both the source and the destination nodes, and sometimes of intermediate nodes.

Examples of location based routing are the Greedy Perimeter Stateless Routing (GPSR) and Location-Aided Routing (LAR). Location information mainly relies on GPS in each node, or on some distributed localization algorithms. The high cost and the low accuracy of localization are the main drawbacks of these two methods, respectively. MTRP involves directionality in its propagation process without needing location information. More specifically, it requires the sink to construct a multicast tree from itself to every node in the network. Such tree construction is not unusual in existing

protocols, and is typically conducted by flooding a "hello" message from the sink to every node.

2. Wanderer algorithm

Parametric Gossiping was proposed in to overcome the percolation behaviour by relating a node's retransmission probability to its hop count from either the destination or the source. A special form of Gossiping is

2.5. Different algorithms used for analysis the PRP Scheme

1. SPREAD algorithm

SPREAD algorithm in attempts to find multiple most-secure and node-disjoint paths. The security of a path is defined as the likelihood of node compromise along that path, and is labeled as the weight in path selection. A modified Dijkstra algorithm is used to iteratively find the top- K most secure node-disjoint paths.

2. Wanderer algorithm

Parametric Gossiping was proposed in to overcome the percolation behaviour by relating a node's retransmission probability to its hop count from either the destination or the source. A special form of Gossiping is the Wanderer algorithm, whereby a node retransmits the packet to one randomly picked neighbor. When used to counter compromised-node attacks, flooding, Gossiping, and parametric Gossiping actually help the adversary intercept the packet, because multiple copies of a secret share are dispersed to many nodes.

3. Shamir's algorithm for secret sharing of information

Consider a three-phase approach for secure information delivery in a WSN: secret sharing of information, randomized propagation of each information share, and normal routing (e.g., min-hop routing) toward the sink. More specifically, when a sensor node wants to send a packet to the sink, it first breaks the packet into M shares.

3. TOPOLOGY CONSTRUCTION

In this module, we construct a topology structure. Here we use mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user. While getting each of the nodes, their associated port and ip address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user. While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.

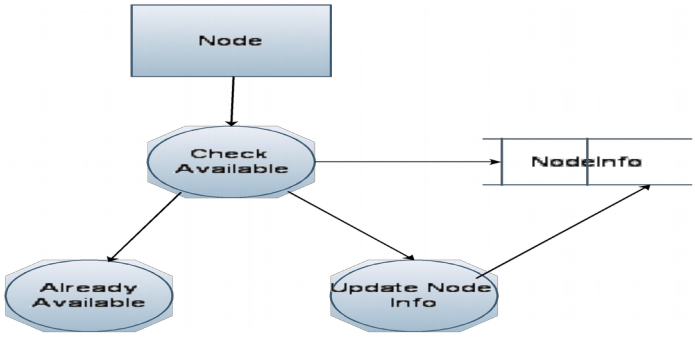


Fig 3 Topology construction

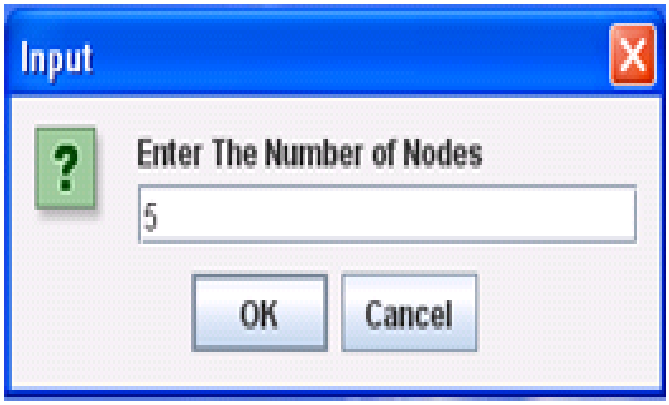


Fig 4 Enter the number of nodes to traverse the data

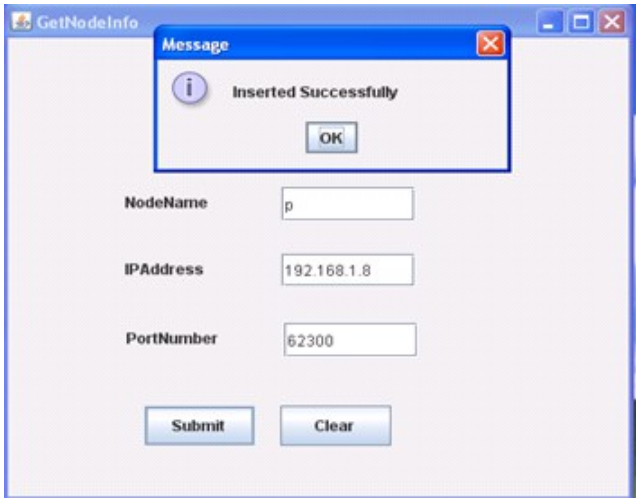


Fig 5 Nodes added along with IP address & Port number

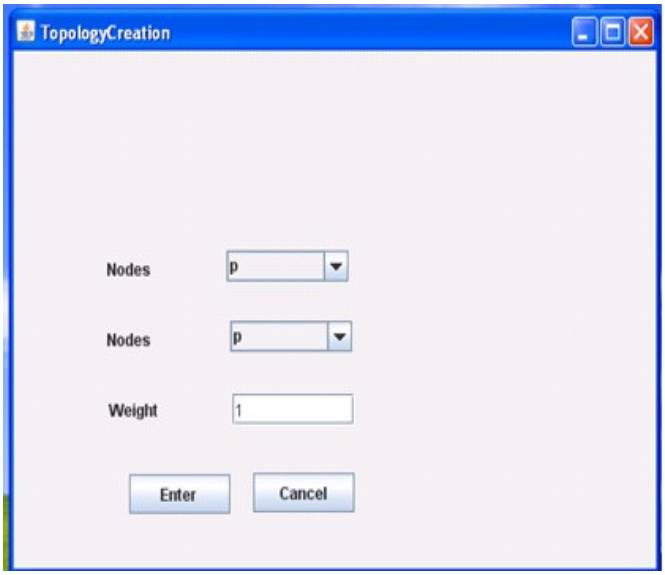


Fig 6 Topology Construction is done

4. RANDOMIZED MULTIPATH ROUTING

We achieve randomized multipath routing that can overcome the Compromised Node attack Denial of Service attack. Here multiple paths are computed in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically not possible.

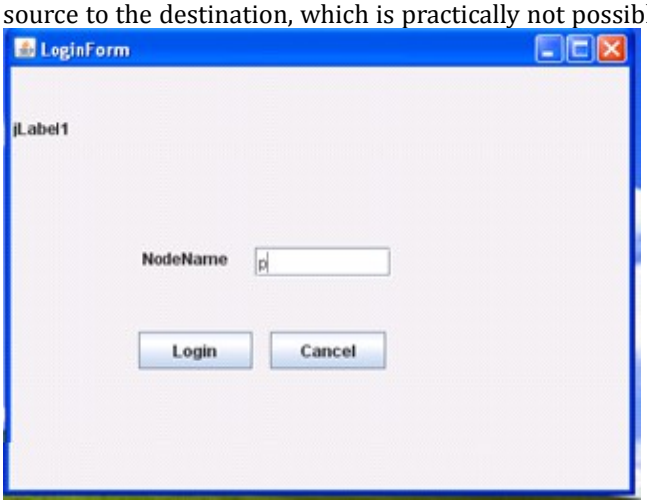


Fig 7 Randomized Multipath Routing: Perform login for every node is done

5. RANDOM PATH

In this module after performing node login for every node, the destination node is being selected so as to transmit the data. Firstly the path selection done for choosing the destination node is based on the number of hop positions from the source node. So the comparison of repeated paths with the new generated paths will done using next hop count table, if they seemed equal it selects the destination node again else it will update the next hop table with the new hop count found. The procedure is illustrated in the following fig 8.

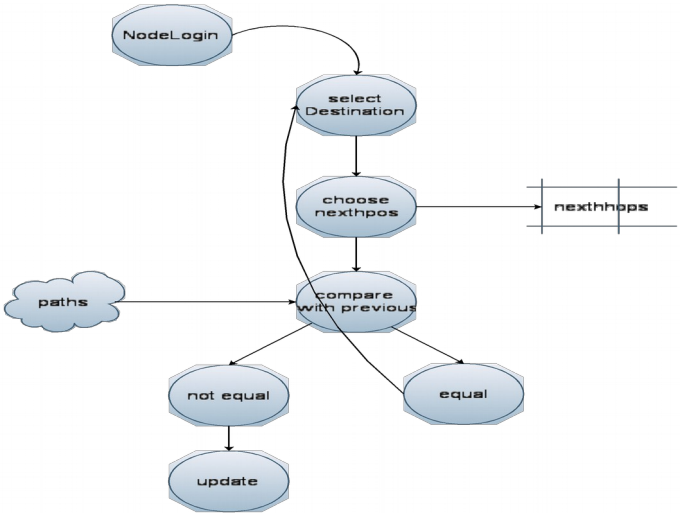


Fig 8 To perform random path selection

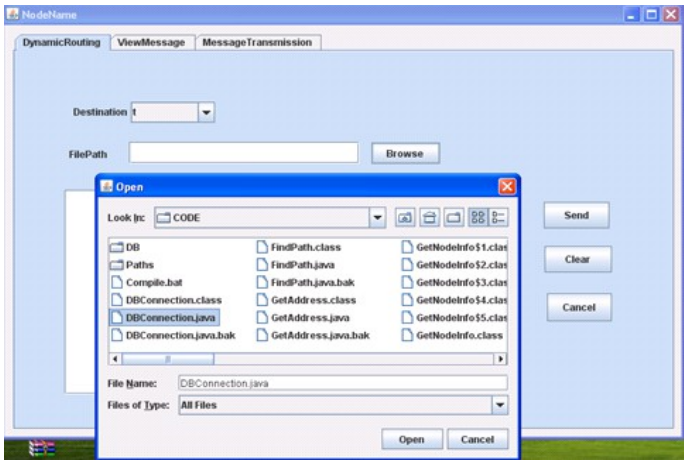


Fig 9 Selecting random path-To transfer data from paths choose a data file

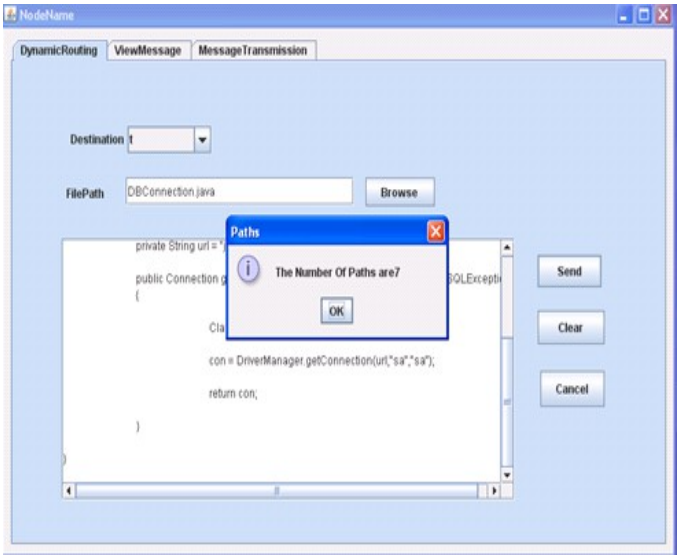


Fig 10 Selecting random path- Total Number of paths from source p to destination t

6. SECURE DELIVERY OF PACKETS

In this module we can maintain the routing table; here we add one more column to maintain the packet delivery ratio. In this one we can maintain how many packets are transmitted over each path. It will be useful for to identify any path can handle number packets. To reduce unnecessary retransmissions and improve energy efficiency, the Gossiping algorithm was proposed as a form of controlled flooding, whereby a node retransmits packets according to a pre-assigned probability. It is well known that the Gossiping algorithm has a percolation behavior, in that for a given retransmission probability, either very few nodes receive the packet, or almost all nodes.

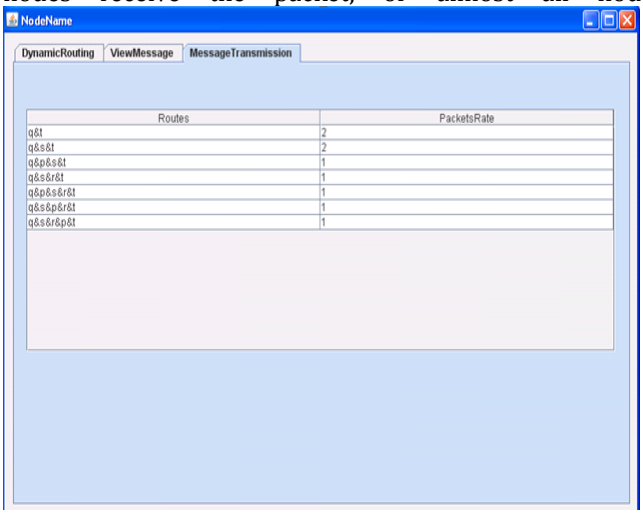


Fig 11 Secure delivery of packets -Displaying the paths from different nodes

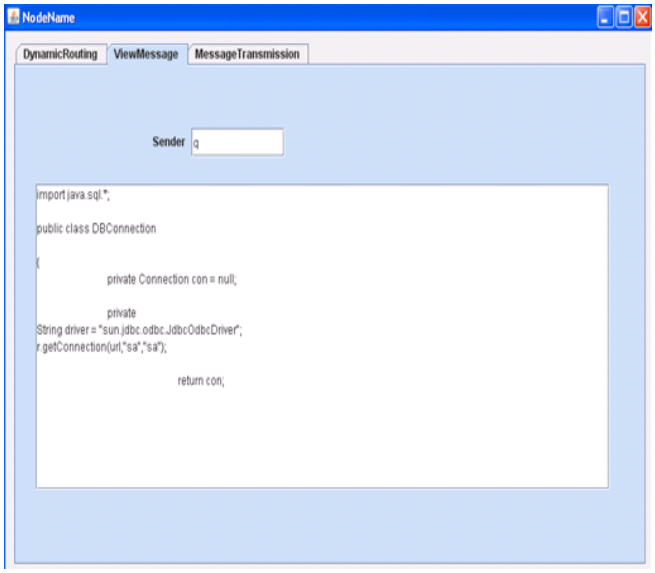


Fig 12 Successful transmissions of packets in a secured way

7. CONCLUSIONS

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 algorithms to as low as 10_3, which is at least one order of magnitude smaller than approaches that use deterministic node-disjoint multipath routing. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy. Specifically, the energy consumption of the proposed randomized multipath routing algorithms is only one to two times higher than that of their deterministic counterparts.

The proposed algorithms can be applied to selective packets in WSNs to provide additional security levels against adversaries attempting to acquire these packets. By adjusting the random propagation and secret sharing parameters (N and M), different security levels can be provided by our algorithms at different energy costs.

8. ACKNOWLEDGEMENT

I am thankful to Management and Principal of VNR Vignana Jyothi Institute of Engineering and Technology for providing their support and facilities such as labs, soft wares etc. needed to carry out this work.

9. REFERENCES

[1] Base paper: "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes" by Tao Shu, Student Member, IEEE, Marwan Krunz, Fellow, IEEE, and Sisi Liu, Student Member, IEEE

[2] INFORMATION PROCESSING AND ROUTING IN WIRELESS SENSOR NETWORKS © World Scientific Publishing Co. P.Ltd

[3] "Introduction to Wireless Sensor Networks" by Robert Berger

[4] 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.

[5] 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.

[6] "Wireless sensor networks" by John A. Stankovic, Depts. Computer science, University of Virginia

[7] Laiali Almazaydeh, Eman Abdelfattah, Manal Al- Bzoor, and Amer Al- Rahayfeh, "PERFORMANCE EVALUATION OF ROUTING PROTOCOLS IN WIRELESS SENSOR .NETWORKS" By Department of Computer Science and Engineering, University Of Bridgeport

[8] "Understanding Packet Delivery Performance In Dense Wireless Sensor Networks" By Jerry Zhao, Ramesh Govidan , Department of Computer science, University of Southern California.

[9] Mobile wireless network by Mischa Schwartz, Cambridge University Press