Randomized Multipath Routes for Secure Data Delivery in Wireless Sensor Networks

Saranya.V
Assistant Professor
Department of Information Technology
Sri Krishna College Of Engineering & Technology, Coimbatore, Tamil Nadu , India

Suriya S.
UG Scholar
Department of Information Technology
Sri Krishna College of Engineering & Technology
Coimbatore, Tamil Nadu, India

Rakini M.
UG Scholar
Department of Information Technology
Sri Krishna College of Engineering & Technology
Coimbatore, Tamil Nadu, India

Abstract- There are two key attacks in wireless sensor networks (WSNs)Compromised node and denial of service . In this project, the data delivery mechanisms that came with high probability circumvent black holes formed by these attacks can be studied. It's argued that 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. In this project mechanisms that generate randomized multipath routes are developed. These designs can identify attacker based on the loss of packets on the particular node. Whenever the attacker is identified, it randomly changes the routing path between sources to destination. By doing this black holes and loss of packets can be minimized. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes.

Keywords – WSN, black holes, adversary, randomized routes, energy efficient.

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are-directional, also enabling control of Sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance, today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node Might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes"(demo video) of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding[1-2].

The various possible security threats encountered in a wireless sensor network (WSN), here its specifically interested in combating two types of attacks: compromised node (CN) and denial of service (DOS).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. 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[3].

One remedial solution to these attacks is to exploit the network's routing functionality. Specifically, if the locations of the black holes are known a priori, then data can be delivered over paths that circumvent (bypass) these holes, whenever possible. The multiple routes from the source to the destination are computed according to some multipath routing algorithm to argue that three security problems exist in the above counter-attack approach. This approach is no longer valid if the adversary can selectively compromise or jam nodes. This is because the route computation in the above multipath routing algorithms is deterministic in the sense that for a given topology and given source and destination nodes, the same set of routes is always computed by the routing algorithm. As a result, once the routing algorithm becomes known to the adversary, the adversary can compute the set of routes for any given source and destination. Then, the adversary can pinpoint to one particular node in each route and compromise (or jam) these nodes. Such an attack can intercept all packets, rendering the above counter-attack approaches ineffective.

The proposed a randomized multipath routing algorithm that can overcome the above problems. In this algorithm, 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 several different paths 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 not possible. Because routes are now randomly generated, they may no longer be node-disjoint. However, the algorithm ensures that the randomly generated routes are as dispersive as possible, i.e., the routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole. Considering the stringent constraint on energy consumption in WSNs, the main challenge in this design is to generate highly dispersive random routes at low energy cost[4].

The rest of the paper is organized as follows. Proposed algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. Proposed Algorithm

Randomized multipath routes in Proposing system can overcome the existing problems. 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. Adversary cannot easily pinpoint and compromise the packets because of large no of random routes.

2.1 ROUTING PROTOCOLS

2.1.1 DYNAMIC SOURCE ROUTING PROTOCOL

Dynamic Source Routing (DSR) is designed to allow nodes to dynamically discover a source route across multiple network hops to any destination in a network. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which to forward the packet. The sender explicitly lists this path in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination node. A key advantage of source routing is that intermediate hops do not need to maintain routing information in order to route the packets they receive, since the packets themselves already contain all necessary routing information. An example of a packet moving through a network with source routing is illustrated in figure 2.1

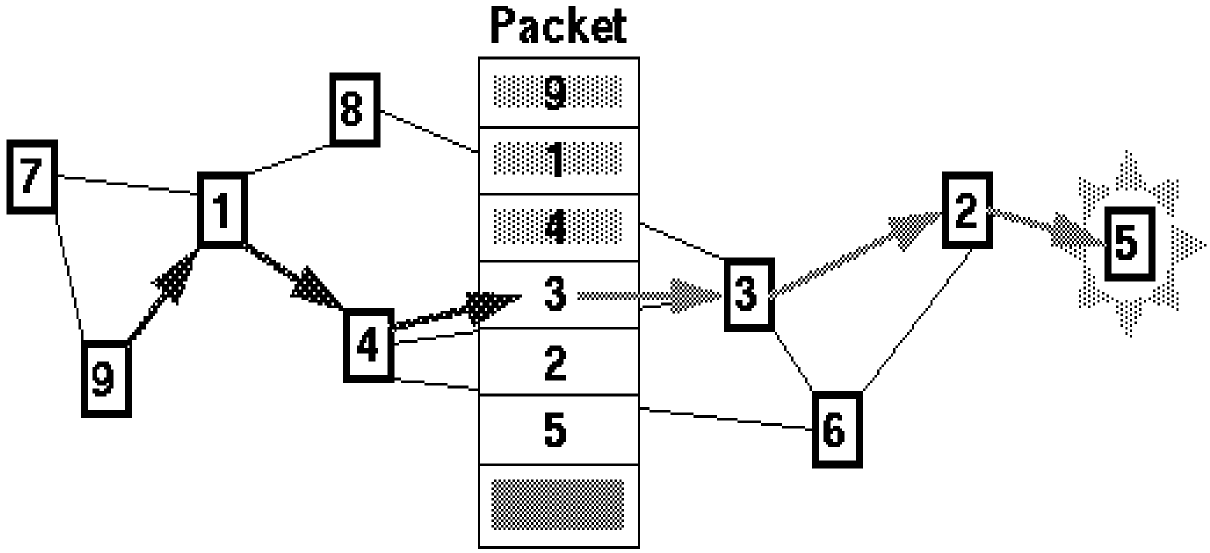


Figure 2.1 a packet being source routed from node 9 to node 5.

DSR is broken down into three functional components: routing, route discovery and route maintenance. Routing has already been described above and is relatively trivial. Route discovery is the mechanism by which a node wishing to send a packet to a destination obtains a path to the destination. Route maintenance is the mechanism by which a node detects a break in its source route and obtains a corrected route.

III.EXPERIMENTAL RESULTS

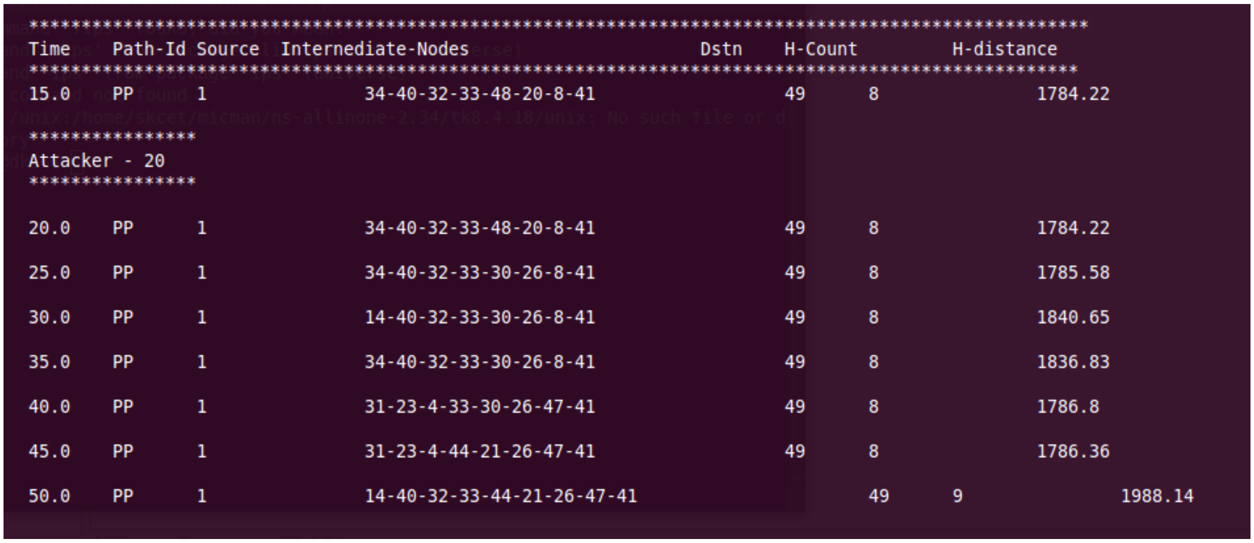
3.1 ROUTE DISCOVERY

To perform route discovery, a source node broadcasts a route request packet with a recorded source route listing only itself. The route request packet also contains a unique sequence number generated by the source. Each node that hears the route request adds its own address to the source route in the packet, and then rebroadcasts the packet. The route request packet propagates hop-by-hop outward from the source node until either the destination node is found or until another node is found that can supply a route to the target.

To prevent route request packets from being broadcast around in loops, nodes will not forward route requests if they are already listed as a hop in the route. To reduce congestion and duplication, each node maintains a small cache of recently received route request < sequence numbers / source address > pairs and does not propagate copies of a route request packet after the first.

All source routes learned by a node are kept (memory permitting) in a route cache, which is used to further reduce the cost of route discovery. A node may learn of routes from virtually any packet the node forwards or overhears. When a node wishes to send a packet, it examines its own route cache and performs route discovery only if no suitable source route is found.

Table-1 Shortest Path Identification



```
****************************************************************************************************
Time     Path-Id Source  Internediate-Nodes                      Dstn     H-Count         H-distance
****************************************************************************************************
15.0     PP      1               34-40-32-33-48-20-8-41                  49       8               1784.22

****************
Attacker - 20
****************

20.0     PP      1               34-40-32-33-48-20-8-41                  49       8               1784.22

25.0     PP      1               34-40-32-33-30-26-8-41                  49       8               1785.58

30.0     PP      1               14-40-32-33-30-26-8-41                  49       8               1840.65

35.0     PP      1               34-40-32-33-30-26-8-41                  49       8               1836.83

40.0     PP      1               31-23-4-33-30-26-47-41                  49       8               1786.8

45.0     PP      1               31-23-4-44-21-26-47-41                  49       8               1786.36

50.0     PP      1               14-40-32-33-44-21-26-47-41                      49       9               1988.14
```

Further, when a node receives a route request for which it has a route in its cache; it does not propagate the route request, but instead returns a route reply to the source node. The route reply contains the full concatenation of the route from the source (from the request packet), and the route leading to the destination (from the route cache).

3.2 ROUTE MAINTENANCE

Conventional routing protocols integrate route discovery with route maintenance by continuously sending periodic routing updates. If the status of a link or node changes, the periodic updates will eventually reflect the change to all other nodes, presumably resulting in the computation of new routes. However, using route discovery, there are no periodic messages of any kind from any of the mobile nodes. Instead, while a route is in use, the route maintenance procedure monitors the operation of the route and informs the sender of any routing errors.

.

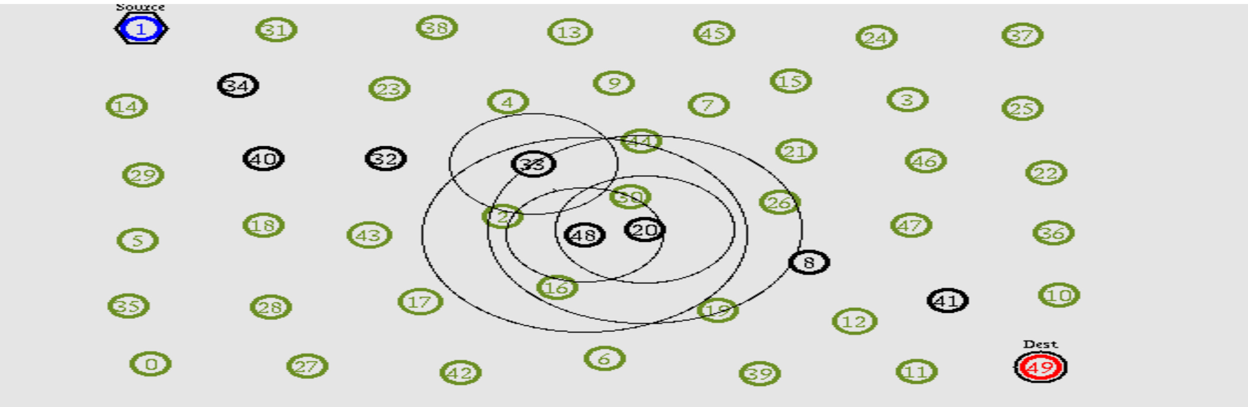


Figure 1 Establishing The Path Between Sources To Destination

If a node along the path of a packet detects an error, the node returns a route error packet to the sender. The route error packet contains the address of the node at both ends of the hop in error. When a route error packet is received or overheard, the hop in error is removed from any route caches; all routes which contain this hop must be truncated at that point.

There are many methods of returning a route error packet to the sender. The easiest of these, which is only applicable in networks which only use bidirectional links, is to simply reverse the route contained in the packet from the original node. If unidirectional links are used in the network, the DSR protocol in presents several alternative methods of returning route error packets to the sender.

Route maintenance can also be performed using end-to-end acknowledgments rather than the hop-by-hop acknowledgments described above. As long as some route exists by which the two end nodes can communicate, route maintenance is possible. In this case, existing transport or application level replies or acknowledgments, or explicitly requested network level acknowledgments, may be used to indicate the status of the node's route to the other node.

- *ADVANTAGES*

Reactive routing protocols have no need to periodically flood the network for updating the routing tables like table-driven routing protocols do. Intermediate nodes are able to utilize the Route Cache information efficiently to reduce the control overhead. The initiator only tries to find a route (path) if actually no route is known (in cache). Current and bandwidth saving because there are no hello messages needed (beacon-less).

- *DISADVANTAGES*

The Route Maintenance protocol does not locally repair a broken link. The broken link is only communicated to the initiator. The DSR protocol is only efficient in MANETs with less than 200 nodes. Problems appear by fast moving of more hosts, so that the nodes can only move around in this case with a moderate speed. Flooding the network can cause collusions between the packets. Also there is always a small time delay at the begin of a new connection because the initiator must first find the route to the target.

3.3 ATTACKS ON AODV PROTOCOL

CLASSIFICATION OF ATTACKS

Attacks against AODV can be classified into routing disruption attacks and resource consumption attacks.

1) Routing Disruption Attacks:

These attacks interrupt the establishment of a route or destroy an existing route. The most common attacks of this type are the modification of RREP (same as the Black hole Attack) and the modification Of RREQ.

2) Resource Consumption Attack:

This attack wastes resources of a specific node and the network as a whole. The most common attack of this type is malicious flooding.

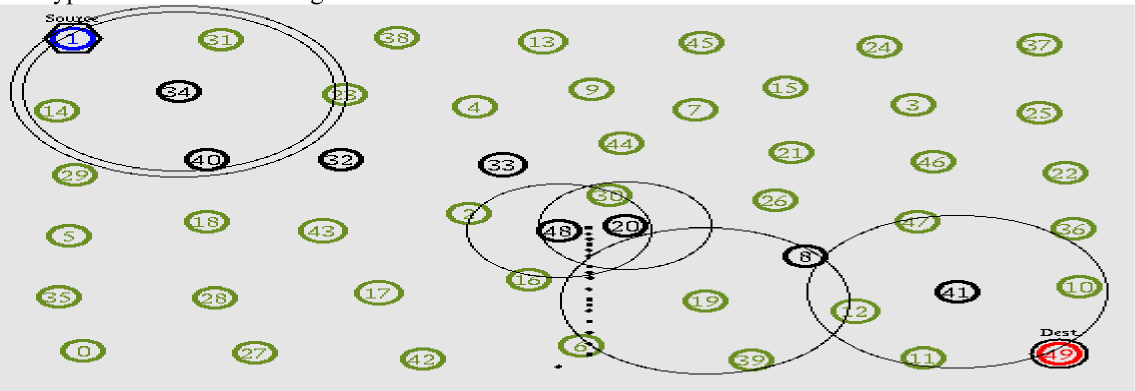


Figure 2 Packet Drop Due To Black Holes

i. Modification of RREP:

The Dst_Seq represents the freshness of routing information in the network. When a source node receives multiple RREP messages, it selects the node that has the largest Dst_Seq value and accordingly constructs a route. Therefore, a malicious node may intentionally attempt to modify the RREP packet and increase the Dst_Seq value of the RREP message. As a result, a false route will be established, and the legitimate data traffic will be interrupted. In addition, the victim nodes will further spread the false routing information to others, and thus, the damage will propagate throughout the network. In this case, consider that two types of forged packets. In the first type, the source and destination IP addresses are spoofed or forged to the destination node. In the second type, the destination IP address is forged to the destination node, and the source IP address is spoofed to a randomly selected node.

ii. Modification of RREQ:

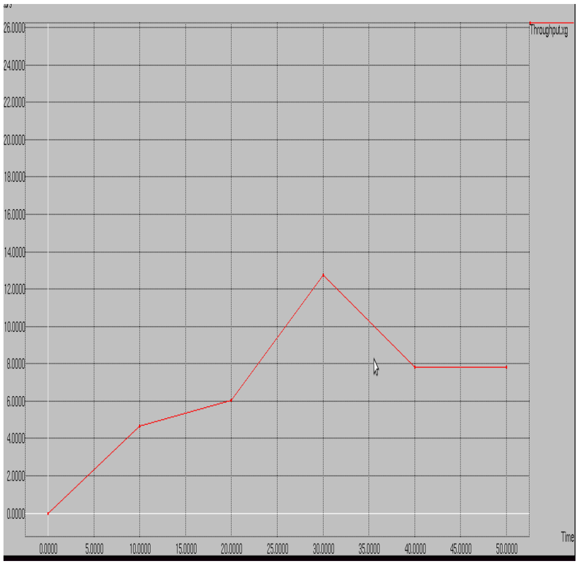
The RREQ ID represents the freshness of an RREQ message in the network. Based on the RREQ ID, each node decides whether to forward an RREQ message. Therefore, a malicious node attempts to intentionally increase the RREQ ID when an RREQ packet is received. Additionally, when a forged packet with a false source address in the IP header is sent, the route will never be established.

Malicious Flooding:

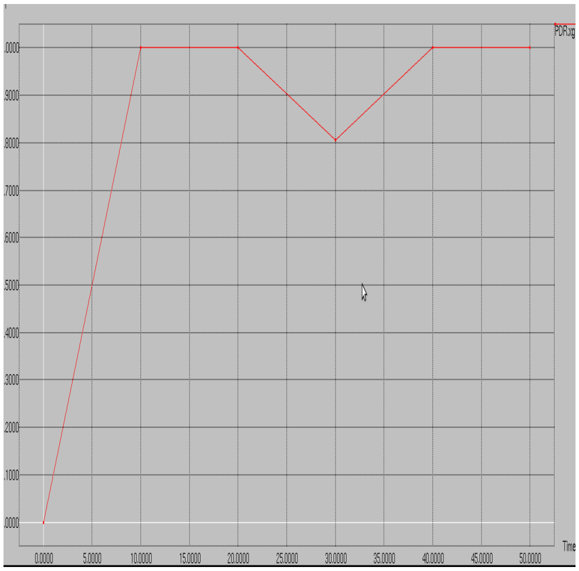
Generally, the RREQ messages are broadcasted to select new routes. If a malicious node sends an excess number of RREQ messages, then the network will become congested with a huge amount of RREQ traffic. The preliminary experimental results, when a malicious node sends more than 20 RREQ packets per second, the congestion occurs, this leads to significant unnecessary delays and packet drops. In this case, consider that two forged packet types. In the first type, the source IP address is forged to a randomly selected node. In the second type, the source IP address is forged to a destination node, and the RREQ ID is intentionally increased at the same time.

3.4 AD HOC ON-DEMAND MULTIPATH DISTANCE VECTOR ROUTING

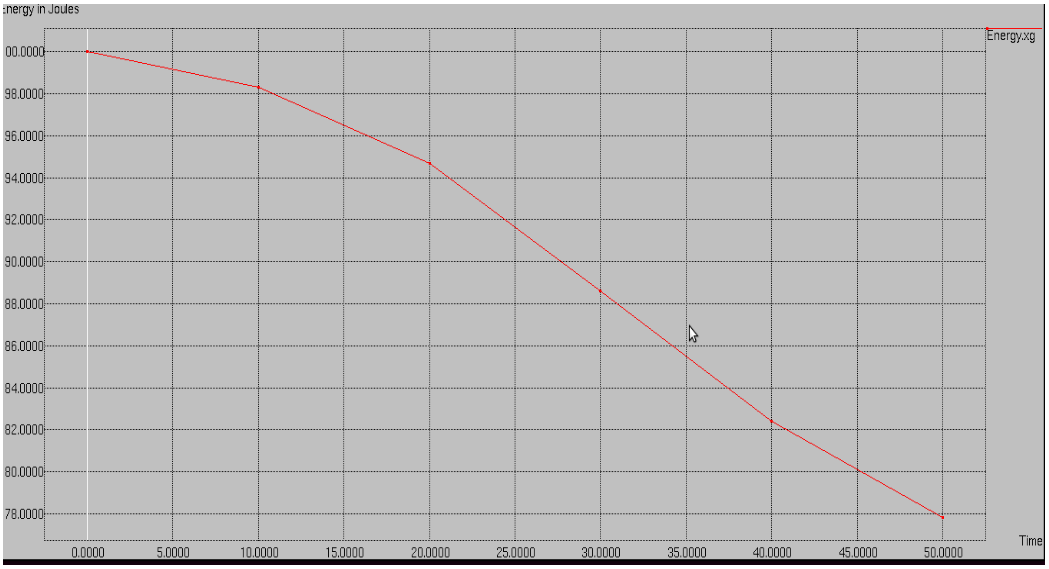
Every node maintains a monotonically increasing sequence number for itself. It also maintains the highest known sequence numbers for each destination in the routing table (called "destination sequence numbers").Destination sequence numbers are tagged on all routing messages, thus providing a mechanism to determine the relative freshness of two pieces of routing information generated by two different nodes for the same destination. The AODV protocol maintains an invariant that destination sequence numbers monotonically increase along a valid route, thus preventing routing loops.



a) Throughput



b) Packet Delivery Ratio



c) Energy Consumption

AOMDV has numerous features which are similar with AODV. It is dependent on the distance vector theory and utilizes hop-by-hop routing technique. Furthermore, AOMDV also discovers routes on demand using a route discovery method. The most important variation is the amount of routes found in each route discovery. In AOMDV, RREQ transmission from the source to the target establishes multiple reverse paths both at intermediary nodes in addition to the destination. Multiple RREPs navigates this reverse route back to form multiple onward routes to the target at the source and intermediary nodes. Moreover, AOMDV also makes intermediary nodes available with alternate routes since they are established to be helpful in dropping route discovery frequency.

The basis of the AOMDV protocol lies in guaranteeing that multiple routes revealed are loop-free and disjoint, and in competently discovering such paths by means of a flood-based route discovery. AOMDV path revise rules, exploited locally at every node, play a major role in preserving loop-freedom and disjointness characteristics. AOMDV depends more on the routing information previously available in the fundamental AODV protocol, thus preventing the overhead acquired in determining multiple paths. Specifically, it does not make use of any particular control packets. Additional RREPs and RERRs for multipath discovery and protection together with a small amount of extra fields in routing control packets (i.e., RREQs, RREPs, and RERRs) comprise the only extra overhead in AOMDV compared with AODV.

IV.CONCLUSION

The analysis and simulation results have shown the effectiveness of the randomized dispersive routing in combating CN and DOS attacks. By appropriately setting the random propagation the packet Interception probability can be easily reduced by the proposed systems. 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 higher than that of their deterministic counterparts.

The proposed work is based on the assumption that there are only a small number of black holes in the WSN. In reality, a stronger attack could be formed, whereby the adversary selectively compromises a large number of sensors that are several hops away from the sink to form clusters of black holes around the sink. Collaborating with each other, these black holes can form a cut around the sink and can block every path between the source and the sink. Under this cut around-sink attack, no packets from the source can escape from being intercepted by the adversary. The proposed work does not address this attack. Its resolution requires us to extend our mechanisms to handle multiple collaborating black holes, which will be studied in future work.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci(2002), "*A Survey on Sensor Networks,*" IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114.

[2] M.K. Marina and S.R. Das(2001), "*On-Demand Multipath Distance Vector Routing in Ad Hoc Networks,*" Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 14-23.

[3] P. Papadimitratos and Z.J. Haas(1994), "*Secure Data Communication in Mobile Ad Hoc Networks,*" IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 343-356.

[4] Tao Shu, Marwan Krunz, and Sisi Liu(2010), "*Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes*" IEEE Comm vol. 9, no.7.

[5] A.D. Wood and J.A. Stankovic(2002), "*Denial of Service in Sensor Networks,*" Computer, vol. 35, no. 10, pp. 54-62.

[6] The Network Simulator - NS-2, http://www.isi.edu/ nsnam/ns/tutorial.

[7] Wireless Sensor Networks, en.wikipedia.org/wsn/index.php.