INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

# SECURE DATA COLLECTION IN WIRELESS NETWORKS

**SARASWATI S. BHAKARE, PROF. LAULKAR C.A, YADAV N.G**

1. M.E. Student, Sinhgad College of Engineering, Pune, India.
2. Asst. Prof., Sinhgad College of Engineering, Pune, India.
3. M.E. Student SVERI, COE Pandhrpur, India.

**Accepted Date:**

27/02/2013

**Publish Date:**

01/04/2013

**Keywords**

Message Transmission,

Distributed Wireless Sensor Network,

Black Holes,

MTRP,

DRP,

CN,

DOS.

**Corresponding Author**

**Ms. Saraswati S. Bhakare**

## Abstract

Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs). In this paper, we study data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. We argue 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 paper, we develop mechanisms that generate randomized multi-path routes. Under our designs, 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 generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. We analytically investigate the security and energy performance of the proposed schemes. We also formulate an optimization problem to minimize the end-to-end energy consumption under given security constraints. Extensive simulations are conducted to verify the validity of our mechanisms.

## I.INTRODUCTION

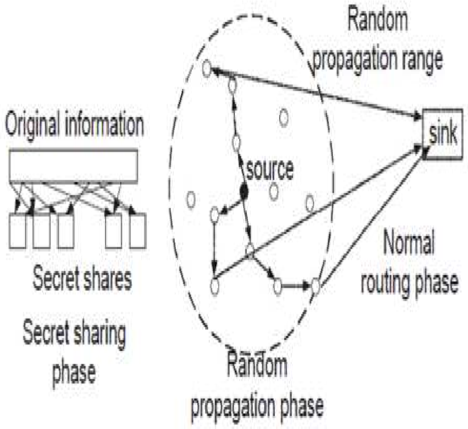
Of the various possible security threats encountered in a wireless sensor network (WSN), in this paper we are especially interested in combating two types of attacks: compromised-node (CN) and denial-of-service (DOS) [1]. In the CN attack, an adversary physically compromises a subset of nodes to eavesdrop 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 [4]. 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 dentition, 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 crypto-system. 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. 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. First, the 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 [2]. 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. Second, multiple routes from the source to the destination are computed according to some multi-path routing algorithm (e.g., [5], [7], [6], [3]).

These routes are node-disjoint or maximally node-disjoint subject to certain constraints (e.g., min-hop routes). The M shares are then distributed over these routes and delivered to the destination. As long as at least M¡T +1 (or T) shares bypass the compromised (or jammed) nodes, the adversary cannot acquire (or deny the delivery of) the original packet. We argue that three security problems exist in the above counter-attack approach. First, this approach is no longer valid if the adversary can selectively compromise or jam nodes. This is because the route computation in the above multi-path 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 (this can be done, e.g., through memory interrogation of the compromised node), 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 shares of the information, rendering the above counter-attack approaches ineffective. Second, as pointed out in [8], actually very few node-disjoint routes can be found when the node density is moderate and the source and destination nodes are several hops apart. For example, for a node degree of 8, on average only two node-disjoint routes can be found between a source and a destination that are at least 7 hops apart. There is also 30% probability that no node disjoint paths can be found between the source and the destination [8]. The lack of enough routes significantly undermines the security performance of this multi-path approach. Last, because the set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to circumvent a moderate-size black hole.

## II.OBJECTIVE

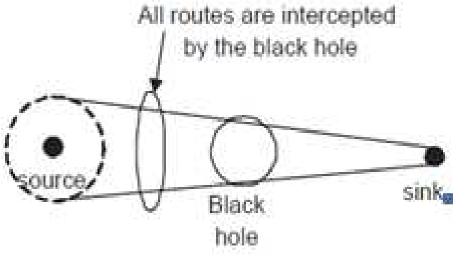
Secure Message Transmission (SMT) mechanism proposed in continuously updates the rating of the routes: For each successful (failed) share, the rating of the corresponding route is increased (decreased). The delivery of subsequent shares will be in favor of those routes.

Energy consumption of the proposed randomized multi-path 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. Considering that the percentage of packets in a WSN that require a high security level is small, we believe that the selective use of the proposed algorithms does not significantly impact the energy efficiency of the entire system.

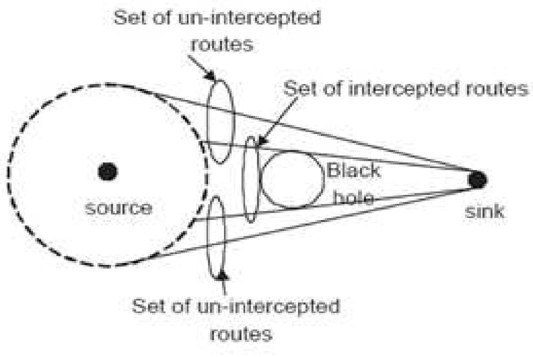


Proposed system is sensor technology allow better, cheaper, and smaller sensors to be used in both military and civilian applications, especially when the environment is harsh, unreliable, or even adversarial. A large number of sensors are usually deployed in order to achieve quality through quantity. On the other hand, sensors typically communicate through wireless networks where the network bandwidth is much lower than for wired communication. These issues bring new challenges to the design of DWSN (Distributed Wireless Sensor Networks).

## III.SYSTEM ARCHITECTURE



(b) Routes of lower dispersiveness


Set of un-intercepted routes
Set of intercepted routes
Black hole
source
sink
Set of un-intercepted routes

(a) Routes of higher dispersiveness

## IV.ALGORITHMS

### A. Pure Random Propagation:-

Pure Random Propagation (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 data to destination, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicast the share to that neighbor. After receiving the share, the neighbor first decrements the TTL, if the new TTL is greater than , 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.

### B. Non-Repetitive Random Propagation (NRRP):-

Improves propagation efficiency by recording the nodes traversed so far:

– Adds node-in-route (NIR) field to the share header

– Initially NIR is empty at the source node

– When a share is propagated, the ID of the upstream node is added to the NIR field

– Nodes in NIR fields are excluded from random pick at the next hop

– Thus share is relayed to a different node in each step, leading to better propagation efficiency.

### C. Directed Random Propagation (DRP):-

Improves propagation efficiency with two hop neighborhood information:

– Adds last-hop-neighbor list (LHNL) field to the header of each share International Journal of Computer Science and Telecommunications

– Propagating node updates the LHNL field before sending the share

– Receiving node compares this LHNL against its own

LHNL & randomly picks a node that is not in LHNL of both nodes

– TTL value decremented, LHNL is updated, share relayed

– If the LHNL fully overlaps the relaying node LHNL, a random neighbor is selected, just like PRP.

• Benefits:-

– Reduces the chance of propagating a share back and forth

– Better propagation efficiency as the share is pushed outwards

**D. Multicast Tree Assisted Random Propagation (MTRP):-**

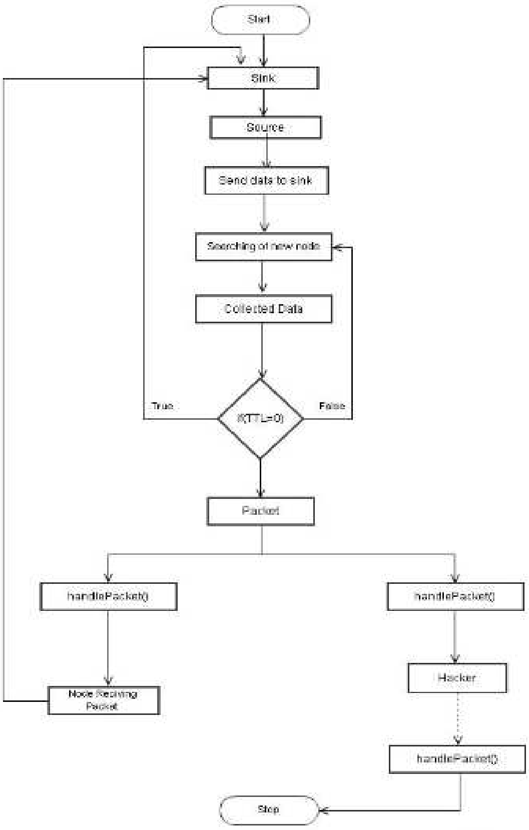
– Traditional location based routing algorithms

– Require location information at both the source and the destination and sometimes intermediate nodes (GPS at each node)

– Low accuracy of localization and high cost

– MTRP involves directionality in its propagation without needing location information

Flow of data:-



## V.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 educed 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 multi-path 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 multi-path 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. Considering that the percentage of packets in a WSN that require a high security level is small, we believe that the selective use of the proposed algorithms does not significantly impact the energy efficiency of the entire system.

Our current work is based on the assumption that there is 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 secret share from the source can escape from being intercepted by the adversary. Our current 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 our future work.

## VI. REFERANCE

1. A.D. Wood and J. A. Stankovic. Denial of service in sensor networks. IEEE Computer Magazine, 35(10):54–62, Oct. 2002.

2. C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith. Parametric probabilistic sensor network routing. In Proceedings of the ACM International Conference on Wireless Sensor Networks and Applications (WSNA), pages 122–131, 2003.

3. D. R. Stinson. Cryptography, Theory and Practice. CRC Press, 2006.

4. I. F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci. A survey on

sensor networks. IEEE Communications Magazine, 40(8):102–114, Aug. 2002.

5. D. B. Johnson, D. A. Maltz, and J. Broch. DSR: the dynamic source routing protocol for multihop wireless ad hoc networks. In C. E. Perkins, editor, Ad Hoc Networking, pages 139–172. Addison- Wesley, 2001.

6. M. K. Marina and S. R. Das. On-demand multipath distance vector routing in ad hoc networks. In Proceedings of the IEEE International Conference for Network Protocols (ICNP), pages 14–23, 1Nov. 2001.

7. S. J. Lee and M. Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks. In Proceedings of the IEEE ICC Conference, pages 3201–3205, 2001.

8.Z. Ye, V. Krishnamurthy, and S. K. Tripathi. A framework for reliable routing in mobile ad hoc networks. In Proceedings of the IEEE INFOCOM Conference, volume 1, pages 270–280, Mar. 2003.