Optimized Secure Data Delivery based on Randomized Routing in Wireless Sensor Networks

J.Preetheswari
M.E Student, Dr.Sivanthi Aditanar College of Engineering,
Tiruchendur

J. Mark Jain M.E
Lecturer, Dr.Sivanthi Aditanar College of Engineering,
Tiruchendur

ABSTRACT

Security and Energy restriction are of most concern in pushing the success of Wireless Sensor Networks (WSNs) for their wide deployment. Despite years of much intensive research, deploying secure communication between wireless nodes remains the cumbersome setup process. Due to the deprived physical layout of sensor nodes, it is generally assumed that an adversary can capture and compromise a small number of sensors in the network. The key attack identified in such a network is Compromised Node (CN) attack which has the ability to create black hole, thereby intercepting the active information delivery. In this paper, we develop an effective routing mechanism that can with high probability, circumvent the black hole formed by this attack. The Purely Random Propagation (PRP) algorithm developed generates randomized dispersive routes so that the routes taken by the shares of different packets changes over time. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of bypassing black hole. Also, the energy constraint is highly optimized in the entire routing mechanism leading to minimal energy consumption. Extensive simulations are conducted to investigate the security and energy performance of our mechanism.

General Terms

Network Security, Randomized Routing

Keywords – CN, PRP

1. INTRODUCTION

Our focus is on routing security in wireless sensor networks. Current proposals for routing mechanisms in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. Sensor networks are highly susceptible to denial of service attacks due to their inherent characteristics i.e., low computational power, limited memory and communication bandwidth coupled with use of insecure wireless channel. A black hole attack can be easily launched by an adversary node in the sensor network. The malicious node starts advertising very attractive routes to data sink. The neighbor nodes select the malicious node as the next hop for message forwarding considering it a high quality route and propagate this route to other nodes. Almost all traffic is thus attracted to the malicious node that can either drop it, selectively forward it based on some malicious filtering mechanism or change the content of the messages before relaying it. This malicious node has thus formed a sink hole with itself at the center.

Of the various possible security threats encountered in a wireless sensor network (WSN), in this paper, we are specifically interested in combating the attack, compromised node (CN). In the CN attack, an adversary physically compromises a subset of nodes to eavesdrop information. This attack generates black hole: area 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 [5]. Severe CN attack can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology.

One remedial solution to this attack 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 this paper, we propose 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 secret shares[3] 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 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. In addition, for efficiency purposes, we also require that the randomized routing algorithm only incurs a small amount of communication overhead.

2. RELATED WORK

The concept of multipath routing[9][24] dates back to 1970s, when it was initially proposed to spread the traffic for the purpose of load balancing and throughput enhancement [14]. Also, Split Multipath routing[4] and DSR[6] modifies AODV functionality. Later on, one of its subclasses, path-disjoint multipath routing, has attracted a lot of attention in wireless networks due to its robustness in combating security issues. WSNs composed of large number of sensors operate in real time mode wherein, soon after acquiring data, they communicate it to a trusted online entity called sink [2]. This paper focuses on unattended WSNs characterized by intermittent sink presence and operation in hostile settings. It deals with the security problems and also explores some techniques such as Do-Nothing (DO), Move-Once (MO) and Keep-Moving (KM) without cryptography to address the anticipated attacks. Intrusion detection detects the existence of inappropriate, incorrect or anomalous moving attackers. The WSN parameters such as node density and sensing range in terms of a desirable detection probability [10]. We derive the detection probability by considering two sensing models: single sensing detection and multiple sensing detection. Optimized Multipath Network Coding (OMNC)[12] is a rate control protocol that improves the throughput and also controls the end-to-end transmission of

coded packets in lossy wireless networks. OMNC is always able to keep the highest aggregate network throughput when compared with existing unicast network coding protocols.

An autonomous host-based intrusion detection system (IDS) has been approved for detecting malicious sinking behavior[11]. There are many attack threats to the network, so two machine learning techniques, Support Vector Machines (SVM) and Fischer Discriminant Analysis(FDA) have been utilized for learning and adaptation to new attack scenarios. To secure data aggregation using multipath routing[8], sensors split their readings into several shares and distribute them among several disjoint paths. Upon receipt of a minimum number of shares, the sink can reconstruct the aggregated value. Depending on the scheme and its parameters, these techniques provide varying levels of resistance against DoS at tacks, eavesdropping, and data tampering. By using secret multipath aggregation, one can guarantee that a subset of compromised paths cannot reveal/leak any information about the readings. This is at the cost of some overhead. By using dispersed multipath aggregation, one has an optimal overhead but achieves lower levels of confidentiality. Depending on the application or scenario, one approach offers more advantages than another.

3. INTELLIGENT BLACK HOLE DETECTION (IBHD) ALGORITHM:

It is a decentralized and an active detection system that uses Ants to reduce computation per node and to make it more reliable and robust. On the basis of functionality performed, all ants are identified into two types: Forward Ant (FA) and Backward Ant (BA). A FA is generated at source node and proceeds towards a destination node gathering information about the state of the network on its way. A BA makes use of the collected information to update the routing tables of nodes on their path and analyzes the collected information to detect attack.

The algorithm primarily employs two data structures:

- **Routing Table:** Routing table at each node stores the list of reachable nodes and their pheromone value. This value is used by the node to calculate the probability of each adjacent node to be the next hop in order to reach the Destination.

- **Neighbor list:** Neighbor list is used to store the IDs and distance of all the neighboring nodes.

3.1 Activation algorithm

This algorithm generates forward ants at source node. Forward ants choose their next node on the basis of transition probability (Tp) [7] given by

$$T_p = \frac{w_{\tau ij}(t) + (1-w)\psi_{ij}}{(1-w)(|N_i|-1)} \quad \text{- (1)}$$

On reaching the base station, it launches backward ant. Backward ant choose next node and calls Analysis Algorithm to detect faults within the network and update the pheromone according to updation rule [7] by

$$\tau_{ij}(t) = \rho(\tau_{ij}(t-1)) + \Delta p_{ij}(t) \quad \text{- (2)}$$

$$\Delta p_{ij}(t) = \frac{E_i * RF_i}{Age_{ant\_i}} \quad \text{- (3)}$$

where

$$E_i = E_{ini\_i} - E_{T\_i} \quad \text{- (4)}$$

$$E_{T-i} = K*(\alpha*age)^2 \quad \text{- (5)}$$

$$Age_{ant\_i} = CT + AT \quad \text{- (6)}$$

$$RF_i = \frac{Packet\_Sent_i}{Packet\_Recv_i} \quad \text{- (7)}$$

Where w is some constant parameter, τ_{ij} is the pheromone value corresponding to neighbor j at node i , ψ_{ij} is the local heuristic value of edge(i,j) for node, N_i is the Normalization Parameter, E_i is the remaining Energy of sensor node i., RF_i is the Reliability factor of node i., Age_{ant_i} is the Age of ant at node i., ρ is the Evaporation Coefficient of Local Search, E_{ini_i} is the Initial energy of node *i*, E_{T_i} is the Energy consumed in transmitting a packet.

3.2 Analysis Algorithm

Every node maintains its log table that contains the information about their remaining energy, age of ant, reliability (ratio of packet sent and packet delivered).If packet sent and packet received ratio is ∞ then it again evaporates pheromone and declares Black Hole attack. If both packets sent and packet received is equal then BA ant declares that node is stable and it not under any attack and increases the Δp accordingly to eq. (2) and eq. (3). The algorithm of analysis algorithm is depicted as:

While ($node_i$!= source node)
{ Read_logtable of $i \in NBR_{ds}$
If $RF_i = \infty$ then
Evaporate pheromone - Return Black Hole attack
If RF_i = Stable then
Update Δp - Return Stable node }

4. RANDOMIZED MULTIPATH DELIVERY

4.1 Overview

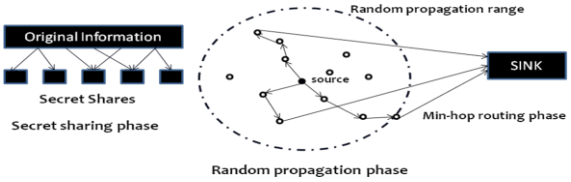

Fig 1: Randomized dispersive routing in a WSN.

We consider a three-phase approach for secure information delivery in a WSN(see Figure 1): 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 (T,M)-threshold secret sharing algorithm, e.g., Shamir's algorithm [3]. 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. Clearly, the random propagation phase is the key component that dictates the security and energy performance of the entire mechanism.

4.2 Random Propagation of Information Shares

4.2.1 Purely Random Propagation

In PRP[1], 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.

5. ASYMPTOTIC ANALYSIS OF THE PRP SCHEME

5.1 Network and Attack Models

We consider an area S that is uniformly covered by sensors with density ρ. We assume a unit-disk model for the sensor communication, i.e., the transmitted signal from a sensor can be successfully received by any sensor that is at most R_h meters away. Multihop relay is used if the intended destination is more than R_h away from the source. We assume that the black hole formed by the compromised nodes can be approximated by its circumcircle, i.e., the smallest circle that encompasses the shape of the black hole. Note that the schemes operation does not depend on the shape of the black hole. The analysis of the security performance is conservative (i.e., the system is more secure than what it shows by analysis) under this assumption. We denote the circle, its center, and its radius by E, e, and R_e, respectively.

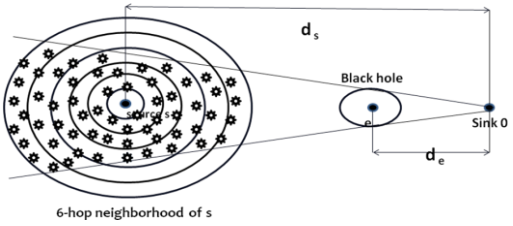

Fig 2: A six-hop random propagation example.

For a given source sensor node, the security provided by the protocol is defined as the worst-case (maximum) probability that for the M shares of an information packet sent from the source, at least T of them are intercepted by the black hole. Mathematically, this is defined as follows: Let the distance between the source s and the sink o be d_s. We define a series of N + 1 circles co-centered at s(see Figure 2). For the i^{th} circle, $1 \le i \le N$, the radius is iR_h. For circle 0, its radius is 0. These N + 1 circles will be referred to as the N-hop neighborhood of s. More specifically, we say that a node is i hops away from s if it is located within the intersection between circles i - 1 and i. We refer to this intersection as ring i. For an arbitrary share, after the random propagation phase, the id of the ring in which the last receiving node, say w, is located is a discrete random variable ξ with state space {1,…,N}. The actual path from w to the sink is decided by the specific routing protocol employed by the network. However, the route given by min-hop routing, which under high node density can be approximated by the line between w and the sink, gives an upper bound on the packet interception rates under all other routing protocols.

The worst-case scenario for packet interception happens when the points s, e, and o, (see Figure 2), are collinear (the shaded region denotes the locations of w for which the transmission from w to o using min-hop routing will be intercepted by E). Denote the distance between e and o by d_e. Given d_s and d_e, when s, e, and o are collinear, the shaded region attains its maximum area, and thus gives the maximum packet interception probability. For ring i, denote the area of its shaded portion by S_i. The interception probability for an arbitrary share of information is given by

$$P_I = \sum_{i=1}^{N} P_r\{\xi = i\} \frac{S_i}{Area\_of\_ring\_i}$$

$$= \sum_{i=1}^{N} P_r\{\xi = i\} \frac{S_i}{\pi i^2 R_h{}^2 - \pi(i-1)^2 R_h{}^2} \quad \text{- (8)}$$

Accordingly, the worst-case probability that at least T out of M shares are intercepted by E is given by

$$P_S^{(\max)} = \sum_{k=T}^{M} MC_K P_I{}^k (1 - P_t)^{M-k} \quad \text{- (9)}$$

5.2 Analysis of Black Hole Interception Area

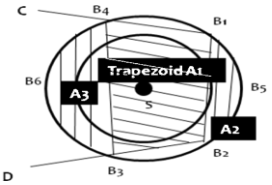

Fig 3: Packet interception area: Case 2.

The derivation of Si falls into one of the following three cases:

Case 1: When $iR_h \le \frac{R_e d_s}{d_e}$ (e.g., rings 1 to 3 see Figure 2), ring i is completely covered by the shaded region. Therefore,

$$S_i^{(case1)} = \pi\left[i^2 - (i-1)^2\right] R_h{}^2, 1 \le i \le \left\lfloor \frac{R_e d_s}{R_h d_e} \right\rfloor \quad \text{- (10)}$$

Case 2: When $(i-1)R_h < \frac{R_e d_s}{d_e} < iR_h$ (see Figure 3), ring i is partially shaded. The shaded area of ring i is the intersection of circle i and the cone CoD minus the area of circle i-1. The area of this intersection is composed of three components: the trapezoid A1 (B1B2B3B4), two circle segments A2 (surrounded by arch B1B5B2 and chord B1B2), and A3 (surrounded by arch B3B6B4 and chord B3B4). It can be shown that A1 has a height $h_{A1} = x_1 - x_2$ where

$$x_1 \xrightarrow{def} \frac{R_e{}^2 d_s + \sqrt{R_e{}^4 d_s{}^2 - d_e{}^2 R_2{}^2 d_s{}^2 + d_e{}^4 i^2 R_h{}^2 - i^2 d_e{}^2 R_h{}^2 R_e{}^2}}{d_e{}^2} \quad \text{- (11)}$$

$$x_2 \xrightarrow{def} \frac{R_e{}^2 d_s - \sqrt{R_e{}^4 d_s{}^2 - d_e{}^2 R_2{}^2 d_s{}^2 + d_e{}^4 i^2 R_h{}^2 - i^2 d_e{}^2 R_h{}^2 R_e{}^2}}{d_e{}^2} \quad \text{- (12)}$$

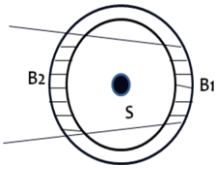

Fig 4: Packet interception area: Case 3.

The lengths of the two parallel edges of A1 are given by

$$l_1 = 2\left(\frac{-R_e}{\sqrt{d_e^2 - R_e^2}} x_1 + \frac{R_e d_s}{\sqrt{d_e^2 - R_e^2}} \right) \quad - (13)$$

$$l_2 = 2\left(\frac{-R_e}{\sqrt{d_e^2 - R_e^2}} x_2 + \frac{R_e d_s}{\sqrt{d_e^2 - R_e^2}} \right) \quad - (14)$$

Therefore, the area of A1 is given by

$$S_i^{(A1)} = \frac{(l_1 + l_2)h_{A1}}{2} \quad - (15)$$

The area of A2 and A3 are given by

$$S_i^{(A2)} = (iR_h)^2 \arctan(\frac{0.5l_1}{x_1}) - 0.5x_1 l_1 \quad - (16)$$

$$S_i^{(A3)} = (iR_h)^2 \arctan(-\frac{0.5l_2}{x_2}) + 0.5x_2 l_2 \quad - (17)$$

So the total shaded area in ring i, $\left\lceil \frac{R_e d_s}{R_h d_e} \right\rceil \le i \le \left\lceil \frac{R_e d_s}{R_h d_e} + 1 \right\rceil$,is given by

$$S_i^{(case2)} = S_i^{(A1)} + S_i^{(A2)} + S_i^{(A3)} - \pi(i-1)^2 R_h^2 \quad - (18)$$

Case 3: When $(i-1)R_h \ge \frac{R_e d_s}{d_e}$ (see Figure 4), the shaded area in ring i is the sum of the areas of two ring segments B1 and B2. Following a similar approach to Case 2, the areas of B1 and B2 are approximated by

$$S_i^{(B1)} \approx \left[i^2 - (i-1)^2 \right] R_h^2 \arctan\left(\frac{0.5l_1}{x_1} \right) \quad - (19)$$

$$S_i^{(B2)} \approx \left[i^2 - (i-1)^2 \right] R_h^2 \arctan\left(-\frac{0.5l_2}{x_2} \right) \quad - (20)$$

where x_1, x_2, l_1, and l_2 are given by (11) through (14), with i referring to the ring being calculated. So the total shaded area in ring i is

$$S_i^{(case3)} = S_i^{(B1)} + S_i^{(B2)}, i \ge \left\lceil \frac{R_e d_s}{R_h d_e} + 1 \right\rceil \quad - (21)$$

5.3 Determine Probability of Packet Interception

We derive the distribution of ξ in this section. For a given share of information, its random propagation process can be modeled as a random walk. Suppose that after the current hop, the share of information reaches at ring i, where $2 \le i \le N-1$. Let the location of the node that receives this share of information be w, and denote the one-hop neighborhood of w as circle O_w (this is the circle centered at w and with a radius of R_h). The next hop from w has three possibilities(see Figure 5):

Case 1: Node w picks a node in region R1 as the next hop to relay the share. Region R1 is defined as R1 = O_w \ Circle i,

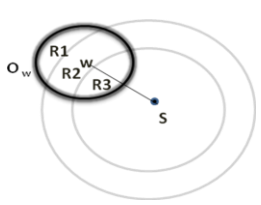

Fig 5: Possibilities of the next hop.

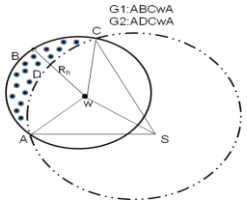

Fig 6: Calculation of $P_{i,i+1}$

where the operation A \ B denotes A - A ∩ B. This case corresponds to the transition from state i to i + 1 in the random walk. Given the distance from w to o be d, where $(i-1)R_h < d < iR_h$,the area of R1 is the difference between the pies G1 (the area surrounded by the arch ABC and the edges wA and wC) and G2 (surrounded by arch ADC and the edges wA and wC). The area of G1 is given by

$$S_{G1} = R_h^2 \arcsin\left(\frac{\sqrt{i^2 R_h^2 - y^2}}{R_h} \right) \quad - (22)$$

where

$$y = \frac{d^2 + (i^2 - 1)R_h^2}{2d} \quad - (23)$$

The area of G2 is given by

$$S_{G2} = i^2 R_h^2 \arcsin\left(\frac{\sqrt{i^2 R_h^2 - y^2}}{iR_h} \right) - 2S_{\Delta AWS} \quad - (24)$$

where $S\Delta_{AWS}$ is the area of the triangle AWS and can be calculated according to Heron's Formula:

$$S_{\Delta aws} = \sqrt{p(p - iR_h)(p - d)(p - R_h)} \quad - (25)$$

where $p = \frac{(i+1)R_h + d}{2}$ is half of the perimeter of the triangle. Given that $(i-1)R_h \le d \le iR_h$, the conditional probability density function (pdf) of d is given by

$$f_d\left(d \mid (i-1)R_h \le d \le iR_h\right)$$

$$\begin{cases} \frac{2d}{(2i-1)R_h^2}, & for\ (i-1)R_h \le d \le iR_h \\ 0, & \text{otherwise} \end{cases} \quad - (26)$$

Therefore, the transition probability $P_{i,i+1}$ can be calculated according to the probability theorem:

$$P_{i,i+1} = \frac{1}{\pi R_h^2} \int_{(i-1)R_h}^{iR_h} (S_{G1}(d) - S_{G2}(d)) \frac{2d}{(2i-1)R_h^2} dd \quad - (27)$$

where S_{G1} and S_{G2} are written as functions of d.

Case 2: Node w picks a node in region R3 as the next hop to relay the share. The region R3 is defined as R3 = O_w ∩ Circle i -1.

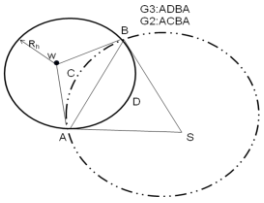

Fig 7: Calculation of $P_{i,i-1}$.

This case corresponds to the transition from state i to i - 1 in the random-walk process. Given the distance from w to o is $(i-1)R_h < d < iR_h$ (see Figure 7) , the area of R3 is the sum of the areas G3 (surrounded by the arch ADB and the

chord AB) and G4 (surrounded by the arch ACB and the chord AB). The area of G3 is given by

$$S_{G3} = R_h^2 \arcsin\left(\frac{\sqrt{(i-1)^2 R_h^2 - y'^2}}{R_h}\right) - (d - y')\sqrt{(i-1)^2 R_h^2 - y'^2} \quad \text{- (28)}$$

where $y' = \frac{(i^2 - 2i)R_h^2 + d^2}{2d}$. The area of G4 is given by

$$S_{G4} = (i-1)^2 R_h^2 \arcsin\left(\frac{\sqrt{(i-1)^2 R_h^2 - y'^2}}{(i-1)R_h}\right) - y'\sqrt{(i-1)^2 R_h^2 - y'^2} \quad \text{- (29)}$$

Following a similar argument in Case 1, the transition probability $P_{i,i-1}$ is calculated as

$$P_{i,i-1} = \frac{1}{\pi R_h^2} \int_{(i-1)R_h}^{iR_h} (S_{G3}(d) + S_{G4}(d)) \frac{2d}{(2i-1)R_h^2} dd \quad \text{- (30)}$$

Case 3: Node w picks a node in region R2 as the next hop to relay the share, where R2 = $O_w \setminus$ (R1 ∪ R3). This corresponds to the situation that the information share will stay in ring i after the next hop relay. Obviously, the transition probability $P_{i,i} = 1 - P_{i,i+1} - P_{i,i-1}$. When i = 1, the calculation of $P_{1,2}$ follows exactly the same analysis as in Case 1, i.e., using (20). There will not be Case 3 when i = 1 ($P_{1,0} = 0$). Therefore, the transition probability $P_{1,1} = 1 - P_{1,2}$. Denote the transition probability matrix of the Markov chain by P. The element of P can be numerically calculated, according to above analysis. To calculate the distribution of ξ, we compute the N-step transition probability matrix by conducting the matrix power operation P^N. The first row of the matrix P^N gives the probability mass vector of ξ. Substituting (10), (18), (21), and the distribution of ξ into (8), the worst-case packet interception probability is obtained.

5.4 Energy Efficiency of the Random Propagation

We assume that the energy consumption for delivering one bit over one hop is a constant q. Then, the average energy consumption for delivering one packet from source s to sink o depends on the average length (in hops) of the route. Note that each random route consists of two components. The first is a fixed N-hop component attributed to the random propagation operation. The second component involves sending the share from the last random relay node, i.e., w, to the sink o using a normal single path routing. Under the asymptotic assumption, when min-hop routing is used, the ratio between the number of hops from w → o and from s → o can be approximated by the ratio of the lengths of these two paths. This ratio can be calculated as follows. Suppose w is located in the ith ring. Let the distance between w and s be $(i-1)R_h \le d \le iR_h$. Given that the angle between sw and so be θ, the distance between w and o is given by

$$d_{wo}^{(i)}(d, \theta) = \sqrt{d^2 + d_s^2 - 2dd_s \cos\theta} \quad \text{- (31)}$$

Due to the symmetry of the random propagation on all direction, θ uniformly distributed between 0 and 2π. Therefore, the average distance while taking all directions into consideration is given by

$$d_{wo}^{(i)} = \int_0^{2\pi} \frac{1}{2\pi} \sqrt{d^2 + d_s^2 - 2dd_s \cos\theta} d\theta \quad \text{- (32)}$$

The average distance between w and o given that $(i-1)R_h \le d \le iR_h$ is given by,

$$d_{wo}^{(i)} = \int_{(i-1)R_h}^{iR_h} \int_0^{2\pi} \frac{d}{(2i-1)\pi R_h^2} \sqrt{d^2 + d_s^2 - 2dd_s \cos\theta} d\theta dd \quad \text{- (33)}$$

Therefore, the unconditionally average distance between w and o is given by the weighted sum of $d_{wo}^{(i)}s$ with weights $P_r\{\xi = i\}$,i.e.,

$$\overline{d_{wo}} = \sum_{i=1}^{N} d_{wo}^{(i)} P_r\{\xi = i\} \quad \text{- (34)}$$

where the distribution of ξ has been obtained in Section 3.4. When min-hop routing is used in the third phase, the number of hops from s to o can be approximated by d_s / R_h. Let the lengths of an information packet and a share generated by the secret sharing algorithm be L_p and L_s, respectively. Note that, in general, $L_s \ge \frac{L_p}{M}$, because a share contains a header and other redundant information of its original packet. To account for this segmentation overhead, let the extra bits of a share be a fraction, say α, of the length of the original packet, i.e., $L_s = \frac{L_p}{M} + \alpha L_p$.Under this notation, the average energy consumptions for delivering one information packet using PRP can be calculated as follows:

$$Q^{(PRP)} = ML_s\left(N + \frac{\overline{d_{wo}}}{R_h}\right)q = (1 + M\alpha)L_p\left(N + \frac{\overline{d_{wo}}}{R_h}\right)q \quad \text{- (35)}$$

5.5 Optimal Secret Sharing and Random Propagation

In this section, we consider the problem of deciding the parameters for secret sharing (M) and random propagation (N) to achieve a desired security performance. To obtain the maximum protection of the information, the threshold parameter should be set as T = M. Then, increasing the number of propagation steps (N) and increasing the number of shares a packet is broken into (M) has a similar effect on reducing the message interception probability. Specifically, to achieve a given $P_s^{(max)}$ for a packet, we could either break the packet into more shares but restrict the random propagation of these shares within a smaller range, or break the packet into fewer shares but randomly propagate these shares into a larger range. Therefore, when the security performance is concerned, a trade-off relationship exists between the parameters M and N. On the other hand, although different combinations of M and N may contribute to the same $P_s^{(max)}$, their energy cost may be different, depending on the parameters L_s, L_p, and q. This motivates us to include their energy consumption into consideration when deciding the secret sharing and random propagation parameters: We can formulate an optimization problem to solve for the most energy-efficient combination of M and N subject to a given security constraint. Formally, this is given as follows:

$$\begin{aligned} &minimize\, Q^{(PRP)}(M, N) \\ &s.t\, P_S^{\max}(M, N) \le P_S^{(req)}, \\ &1 \le M \le M_{\max} \\ &1 \le N \le N_{\max} \end{aligned} \quad \text{- (36)}$$

where M and N are variables and $P_s^{(req)}$ is the given security requirement. The upper bounds, M_{max} and N_{max}, are dictated by practical considerations such as the hardware or energy constraints.

6. SIMULATION ANALYSIS

In this section, we simulate the PRP scheme using NS2 to randomly route the packets to the sink node. First, many nodes are created in various positions. Then the source node and sink node are chosen randomly for the packet transit. At a particular instant of time, a node is implemented to behave as a black hole by dropping packets continuously and thereby blocking the routing process. Also, our implementation analyses the interception area of the black hole for the neighborhood of source node. Next step is to split the message

to be sent into secret shares based on the number of neighbors of the source node. Then we have started the Purely Random Propagation (PRP) Algorithm by finding the one hop neighbors list of each node by calculating the distance between the source node with the respective nodes(see Figure 8). Then the entire randomized routing has been developed(see Figure 9) and the packet interception probability has been analyzed for the possible values of secret shares(M) and random propagation steps(N)(see Figure 10).

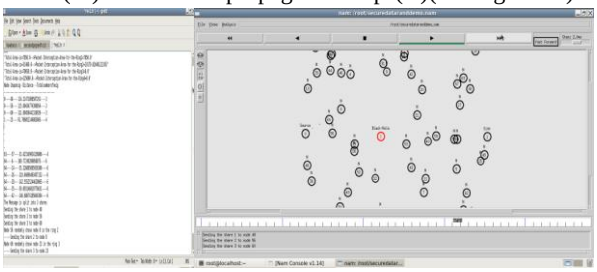

Fig 8: PRP Output Fig 9: Nodes Forwarding Secret Shares

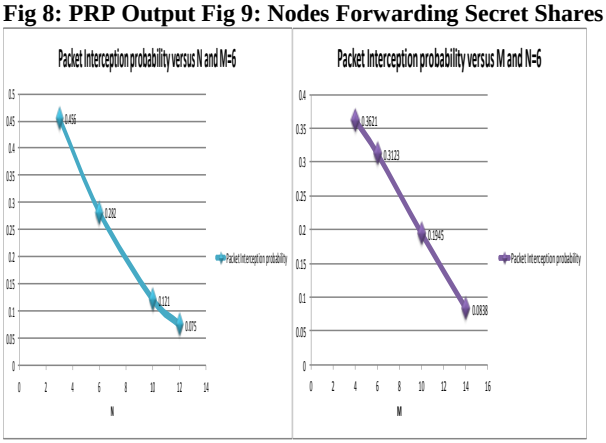

Fig 10: Packet Interception Probability Analysis

7. CONCLUSION

Our analysis and simulation results shows the network layout, black hole implementation, its influence in the source neighborhood and PRP output. By appropriately setting the secret sharing and propagation parameters, the packet interception probability is expected to reduce much smaller than approaches that use deterministic node-disjoint multipath routing. At the same time, security performance must be arrived at a reasonable cost of energy. The proposed algorithm 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 algorithm at different energy costs.

8. ACKNOWLEDGEMENTS

A preliminary version of this paper was presented at the IEEE TMC 2010 Conference. We would like to express our thanks to our management and institution for their material and spiritual support at critical and opportune times. We are particularly grateful to our guide for his thoughtful and creative comments, and more generally for exploring with us the boundaries of professional relationship. Any opinions, findings, conclusions, or recommendations expressed in this paper are entirely the views of the authors.

9. REFERENCES

[1] Tao Shu, Student Member, IEEE, Marwan Krunz, Fellow, IEEE, and Sisi Liu, Student Member, IEEE," Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes", IEEE Transactions On Mobile Computing, Vol. 9, No. 7, July 2010

[2] Roberto Di Pietro, Luigi V. Mancini, Claudio Soriente, Angelo Spognardi, and Gene Tsudik," Data Security in Unattended Wireless Sensor Networks", IEEE Transactions On Computers, Vol. 58, , Nov 2009

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

[4] 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.

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

[7] Dimple Juneja, Neha Arora, Sandhya Bansal "An Agent based Routing Algorithm for Detecting Attacks in Wireless Sensor Networks". IJCIR, 2010.

[8] 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

[9] 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.

[10] Yun Wang, Student Member, IEEE, Xiaodong Wang, Student Member, IEEE, Bin Xie, Senior Member, IEEE, Demin Wang, Student Member, IEEE, and Dharma P. Agrawal, Fellow, IEEE,"Intrusion Detection In Homogeneous And Heterogeneous Wireless Sensor Networks", IEEE Transactions On Mobile Computing, Vol. 7, No. 6, June 2008

[11] John Felix Charles Joseph, Member, IEEE, Bu-Sung Lee, Amitabha Das, Senior Member, IEEE, and Boon-Chong Seet, Member, IEEE "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA",IEEE Transactions On Dependable And Secure Computing, Vol. 8, No. 2, March-April 2011 233

[12] Xinyu Zhang, Baochun Li," Optimized Multipath Coding In Lossy Wireless Networks", IEEE Journal On Selected Areas In Communications, Vol. 27, No. 5, June 2009

[13] Z. Ye, V. Krishnamurthy, and S.K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, vol. 1, pp. 270-280, Mar. 2003.

[14] N.F. Maxemchuk, "Dispersity Routing," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 41.10-41.13, 1975.