International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-5 E-ISSN: 2347-2693

# Efficient Data Collection Using Randomized Multipath Routes in WSN

*M. Trinath Basu[1*], G.Venkatesh[2], Immidisrikanth[3]*

*[1*,2,3]Vardhaman College Of Engineering, Hyderabad, Andhrapradesh, India*

www.ijcaonline.org

Received: 04/04/2014 Revised: 22 /04/2014 Accepted: 17/05/ 2014 Published: 31 /05/2014

**Abstract-** Wireless Sensor Networks (WSNs) are vulnerable to attacks such as Denial of Service (DoS) and compromised-node. This is due to the nature of the existing multi-path routing mechanisms which are deterministic in nature. Adversaries can steal information by compromising routing algorithm in WSN. In this paper we propose routing mechanisms where randomized multi-path routes are dynamically computed. Such routes can bypass the black holes made though DoS and compromised node attacks .The generated routes are energy efficient besides dispersive in nature. Simulation results reveal that the proposed mechanisms are energy efficient in bypassing black holes.

***Keywords*:** Wireless Sensor Network (WSN), Denial Of Service (DOS) Attack, Multi-Path Routing

## I. Introduction

WSNs are vulnerable to various security threats. This is due to constrained resources and their mobility in nature. This paper throws light into two such attacks namely Denial of Service (DOS) and Compromised Node (CN) . The CN attack compromises a node physically and the adversary is able to eavesdrop through the CN. DOS attack on the other hand disrupts the normal functionality of a node or set of nodes as adversary continuously sends unintended signals to block services in the network. These two attacks can generate block holes in WSN. The block holes are the areas through which hackers can eavesdrop actively or passively. Due to these attacks, the normal data delivery in WSN is disrupted. Security methods which are based on cryptography can't solve these problems. The reason behind this is that, the cryptographic keys can be taken by adversary once the node is compromised. One solution to the problem of these attacks is by exploiting routing mechanisms of WSN. If the black holes are known to routing mechanisms, it is possible to bypass the traffic. This idea is practically not easy as it is not possible to know the location information. However, a probabilistic approach can be followed using a two step process. The first step is known as secret sharing and the second step is known as multi-path routing. To achieve this, first of all a packet is converted into many shares. The original data can be established by using few shares. Based on certain constraints routes are either maximal node disjoint or node disjoint. Once routes are found, the shares are sent from source node to destination node. Thus the adversary can't attack as the original packet is now known. Moreover the packets are capable of bypassing the compromised nodes. However, in this approach there are three problems. They are: if the adversary makes attacks that selectively jam or compromise nodes, this approach is not valid. This is because the computation of multipath is deterministic. When shares are travelled through different paths, adversary can find original packet though selective attacks. Second, when distance between source and destination is more in terms of number of hops, only few node-disjoint routes can be found. Last, when routes are computed with constraints, the routes may not be dispersive enough to bypass black holes. In this paper, we propose and implement a randomized multi-path routing to overcome the above problems. This algorithm, instead of using paths from pre-computed collection of routes, computes paths in randomized fashion. Thus it can generate large number of routes between given source and destination.

.

## II. PRIOR WORK

Many prior works focused on the security of networks where multipath routing takes place. However, they are deterministic in constructing the multipath route construction. Most secure and disjoint paths are computed by SPREAD algorithm [2]. The likelihood of node compromise is considered as security in the given path. Such features are measured as weight which is used while making path selection. However, this algorithm does not simultaneously focus on the reliability attributes. An improvement over SPREAD algorithm is H-SPREAD which makes use of security and reliability simultaneously. In order to reduce performance degradation when network is under attacks, distributed Bound-Control and Lex-Control algorithms were proposed in [4] that can compute multiple paths simultaneously. There are other algorithms found in the literature for secure multipath-routing. They include AODV-MAP [6], Burmester's approach [7], SecMR [8] and SRP [9]. All existing multipath-routing algorithms in WSNs were not developed keeping security in mind because of they are resource constrained. This gap is filled by this paper by designing a secure multipath routing in the form of flooding. However, in flooding there is redundancy involved in communication mechanisms. To overcome this problem also in [10] an algorithm by name "Gossiping" was proposed which effectively controls flooding. There is percolation behavior associated with Gossiping algorithm. According to this behavior either few nodes receive packets or all nodes receive packets. In order to overcome the problem of percolation, the Parametric Gossiping [11] was proposed which relates the probability transmission of the node to its hop count from the source or destination. Another form of Gossiping algorithm know as "Wanderer algorithm" where packet to a neighbor node which has been picked randomly. This algorithm when used to counter Gossiping, Flooding, Parametric Gossiping an

Corresponding Author: *M. Trinath Basu*

adversary can intercept packets as multiple copies exist. With respect to energy performance the Wanderer algorithm exhibits poor performance as it produces long paths. However, the other schemes like MTRP, DRP and NRRP explored in this paper provide security in an energy efficient fashion. Very highly diversified multipath routes are provided by them.

## III. PROPOSED MULTIPATH ROUTING

The overview of the proposed multipath routing mechanism is influenced by the architecture given by Shu et al. A three phase approach is followed for secure multipath routing in WSN. The architecture which influenced the work of this paper is as shown below.

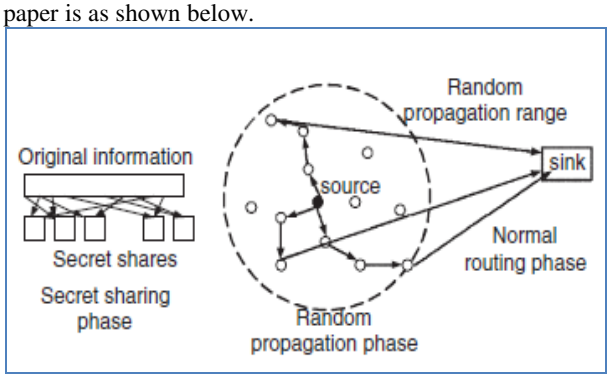



Fig. 1 –Architecture of Multipath Routing

As can be seen in fig. 1, the three phases involved in the architecture of secure multipath routing include normal routing phase, random propagation phase and secret sharing phase. The concept is that in the WSN, the nodes sense data and sends the data to sink. When a node sends data to sink, the data is considered to be a secret message. This message is split into many random shares. These shares are sent to randomly picked neighbors. Such neighbors will ping some nodes randomly and forward the data. This process continues until TTL is set to zero. Once the TTL reaches zero, that node will send the data directly to sink in single path routing concept. Once the sink node obtains some of the shares, it is possible to the sink to establish the whole data packet sent by the sensor node. In this model of data delivery an adversary could not prevent the shares to reach the sink in WSN. We built four random propagation mechanisms. They are known as Purely Random Propagation (PRP), Non-Repetitive Random Propagation (NRRP), Directed Random Propagation (DRP) and Multicast Tree-assisted Random Propagation (MTRP). Based on one-hop neighbor information the PRP works. NRRP is an improved form of PRP in which the nodes which have been traversed are remembered and not used for message propagation. In DRP two-hop neighborhood information is used. To the header of each share, last-hop neighbor list is added to achieve DRP. The lost hop neighbor list content is changed before a node propagates message to next node. This process continues until TTL reaches zero. Once it is set to zero, the node sends data directly to sink. Out of all these techniques, the MTRP scheme improves energy efficiency while propagating data towards sink. It chooses shortest end to end path in order to make the scheme energy efficient.

## IV. Equations

The worst-case scenario for packet interception happens when the points s, e, and o, in Fig. 3, 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 de. Given ds and de, 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 Si. The interception probability for an arbitrary share of information is given by

$$P_I = \sum_{i=1}^{N} \Pr\{\xi = i\} \frac{S_i}{\text{Area of ring } i} = \sum_{i=1}^{N} \Pr\{\xi = i\} \frac{S_i}{\pi i^2 R_h^2 - \pi(i-1)^2 R_h^2}. \quad (1)$$

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

$$P_S^{(\max)} = \sum_{k=T}^{M} \binom{M}{k} P_I^k (1-P_I)^{M-k}. \quad (2)$$

**Derivation of the Packet Interception Area**

$$S_i^{(case\,1)} = \pi[i^2 - (i-1)^2] R_h^2, 1 \le i \le \left\lfloor \frac{R_c d_s}{R_h d_c} \right\rfloor. \quad (3)$$

**Case 2:** When $(i-1)R_h < \frac{R_h d_s}{d_c} < iR_h$,

$$x_1 \overset{def}{=} \frac{R_c^2 d_s + \sqrt{R_c^4 d_s^2 - d_c^2 R_c^2 d_s^2 + d_c^4 i^2 R_h^2 - i^2 d_c^2 R_h^2 R_c^2}}{d_c^2}, \quad (4)$$

$$x_2 \overset{def}{=} \frac{R_c^2 d_s - \sqrt{R_c^4 d_s^2 - d_c^2 R_c^2 d_s^2 + d_c^4 i^2 R_h^2 - i^2 d_c^2 R_h^2 R_c^2}}{d_c^2}. \quad (5)$$

The lengths of the two parallel edges of $A_1$ are given by

$$l_1 = 2\left( -\frac{R_c}{\sqrt{d_c^2 - R_c^2}} x_1 + \frac{R_c d_s}{\sqrt{d_c^2 - R_c^2}} \right), \quad (6)$$

$$l_2 = 2\left( -\frac{R_c}{\sqrt{d_c^2 - R_c^2}} x_2 + \frac{R_c d_s}{\sqrt{d_c^2 - R_c^2}} \right). \quad (7)$$

Therefore, the area of $A_1$ is given by

$$S_i^{(A_1)} = \frac{(l_1 + l_2) h_{A_1}}{2}. \quad (8)$$

The area of $A_2$ and $A_3$ are given by

$$S_i^{(A_2)} = (iR_h)^2 \arctan\left(\frac{0.5 l_1}{x_1}\right) - 0.5 x_1 l_1, \quad (9)$$

$$S_i^{(A_3)} = (iR_h)^2 \arctan\left(-\frac{0.5 l_2}{x_2}\right) + 0.5 x_2 l_2. \quad (10)$$

So the total shaded area in ring $i$, $\lceil \frac{R_c d_s}{R_h d_c} \rceil \le i \le \lfloor \frac{R_c d_s}{R_h d_c} + 1 \rfloor$, is given by

$$S_i^{(case\,2)} = S_i^{(A_1)} + S_i^{(A_2)} + S_i^{(A_3)} - \pi(i-1)^2 R_h^2. \quad (11)$$

$$S_i^{(B_1)} \approx [i^2 - (i-1)^2] R_h^2 \arctan\left(\frac{0.5l_1}{x_1}\right), \quad (12)$$

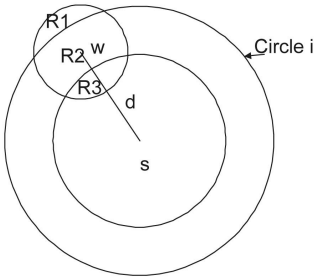
$$S_i^{(B_2)} \approx [i^2 - (i-1)^2] R_h^2 \arctan\left(-\frac{0.5l_2}{x_2}\right), \quad (13)$$

where $x_1$, $x_2$, $l_1$, and $l_2$ are given by (4) through (7), with $i$ referring to the ring being calculated. So the total shaded area in ring $i$ is

$$S_i^{(case\ 3)} = S_i^{(B_1)} + S_i^{(B_2)}, \quad i \geq \left\lceil \frac{R_e d_s}{R_h d_e} + 1 \right\rceil. \quad (14)$$

**Derivation of Packet Interception Probability**

Suppose that after the current hop, the share of informa- tion reaches at ring i, where 2 ≤i ≤ 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 Ow.




Given the distance from w to o be d, where (i-1)Rh<d<iRh 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

$$S_{G_1} = R_h^2 \arcsin\left(\frac{\sqrt{i^2 R_h^2 - y^2}}{R_h}\right), \quad (15)$$

where

$$y = \frac{d^2 + (i^2 - 1)R_h^2}{2d}. \quad (16)$$

The area of $G_2$ is given by

$$S_{G_2} = i^2 R_h^2 \arcsin\left(\frac{\sqrt{i^2 R_h^2 - y^2}}{iR_h}\right) - 2S_{\triangle Aws}, \quad (17)$$

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

$$S_{\triangle Aws} = \sqrt{p(p - iR_h)(p - d)(p - R_h)}, \quad (18)$$

where $p = \frac{(i+1)R_h + d}{2}$ is half of the perimeter of the triangle.

Given that $(i-1)R_h \leq d \leq iR_h$, the conditional probability density function (pdf) of $d$ is given by

$$f_d(d|(i-1)R_h \leq d \leq iR_h) = \begin{cases} \frac{2d}{(2i-1)R_h^2}, & \text{for}(i-1)R_h \leq d \leq iR_h, \\ 0, & \text{otherwise.} \end{cases} \quad (19)$$

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

$$P_{i,i+1} = \frac{1}{\pi R_h^2} \int_{(i-1)R_h}^{iR_h} (S_{G_1}(d) - S_{G_2}(d)) \frac{2d}{(2i-1)R_h^2} dd, \quad (20)$$

where $S_{G_1}$ and $S_{G_2}$ are written as functions of $d$.

$$S_{G_3} = R_h^2 \arcsin\left(\frac{\sqrt{(i-1)^2 R_h^2 - y'^2}}{R_h}\right) - (d - y')\sqrt{(i-1)^2 R_h^2 - y'^2}, \quad (21)$$

where $y' = \frac{(i^2 - 2i)R_h^2 + d^2}{2d}$. The area of $G_4$ is given by

$$S_{G_4} = (i-1)^2 R_h^2 \arcsin\left(\frac{\sqrt{(i-1)^2 R_h^2 - y'^2}}{(i-1)R_h}\right) - y'\sqrt{(i-1)^2 R_h^2 - y'^2}. \quad (22)$$

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

$$P_{i,i-1} = \frac{1}{\pi R_h^2} \int_{(i-1)R_h}^{iR_h} (S_{G_3}(d) + S_{G_4}(d)) \frac{2d}{(2i-1)R_h^2} dd. \quad (23)$$

$$d_{wo}^{(i)}(d, \theta) = \sqrt{d^2 + d_s^2 - 2dd_s \cos\theta}. \quad (24)$$

$$d_{wo}^{(i)}(d) = \int_0^{2\pi} \frac{1}{2\pi} \sqrt{d^2 + d_s^2 - 2dd_s \cos\theta} d\theta. \quad (25)$$

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

$$d_{wo}^{(i)} = \int_{(i-1)R_h}^{iR_h} \int_0^{2\pi} \frac{d}{(2i-1)\pi R_h^2} \sqrt{d^2 + d_s^2 - 2dd_s \cos\theta} d\theta dd. \quad (26)$$

## V Experimental Results

We have made experiments with a customer simulator where we simulated wireless sensor nodes and sink. We made experiments with all the four randomized routing models namely PRP, NRRP, DRP, and MTRP and compared the results with their predecessor named "H-SPREAD".

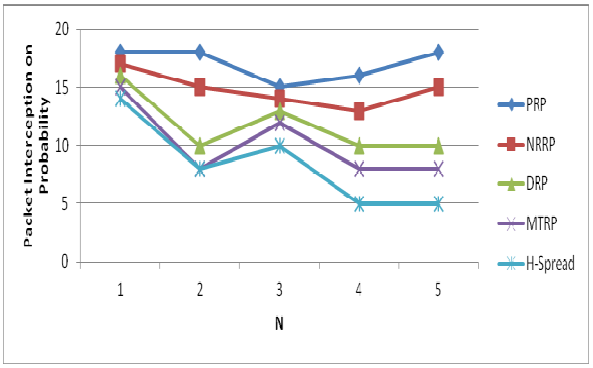



Fig.. Packet interception prob. vs. N

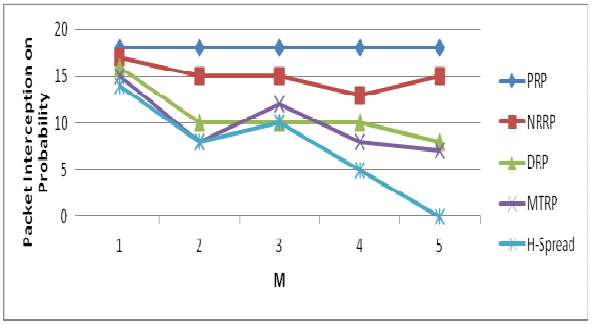



Fig.. Packet interception prob. vs. *M*.

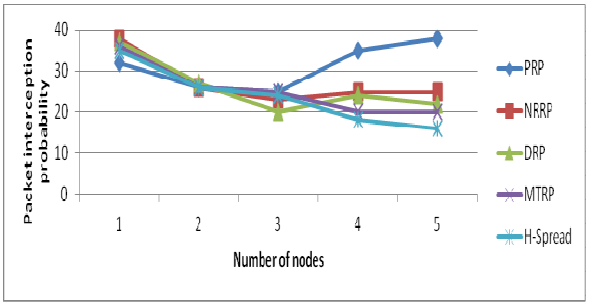



Fig. 5. Packet interception prob. vs. number of nodes.

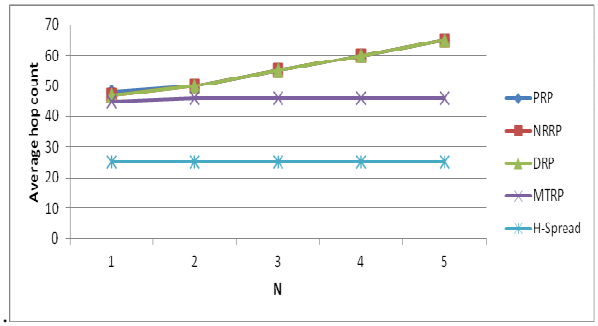



Fig. 7. Hop count vs. *N*.

## VI. CONCLUSION

We proposed and implemented a routing mechanism that can effectively bypass the attacks such as Denial of Service and compromised node. This is achieved by generating randomized and diversified multipath routes which are not vulnerable to attacks. The reason behind this is that the packets are built in such a way that some of the packets when reach the destination can make the whole content. Thus by computing multiple randomized paths it is possible to protect data from adversaries. Even when few packets are known, the adversary can't intercept the whole content. For this reason security probability is more in the proposed algorithm. We also built a custom simulator which demonstrates the proof of concept. The empirical results revealed that the proposed multipath routing mechanism provides improved security when compared with deterministic node-disjoint multi-path routing. Our approach also reduces energy consumption.

## REFERENCES

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

[2] W. Lou, W. Liu, and Y. Fang. Spread: enhancing data confidentiality in mobile ad hoc networks. In *Proceedings of the IEEE INFOCOM Conference*, volume 4, pages 2404–2413, Mar. 2004.

[3] W. Lou and Y. Kwon. H-spread: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 55(4):1320–1330, July 2006.

[4] P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing in attack-resistant networks. *IEEE/ACM Transactions on Networking*, 15(6):1490–1501, Dec. 2007.

[5] 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.

[6] B. Vaidya, J. Y. Pyun, J. A. Park, and S. J. Han. Secure multipath routing scheme for mobile ad hoc network. In *Proceedings of IEEE International*
*Symposium on Dependable, Autonomic and Secure Computing*, pages 163–171, 2007.

[7] M. Burmester and T. V. Le. Secure multipath communication in mobile ad hoc networks. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, pages 405–409, 2004.

[8] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris. Secmr- a secure multipath routing protocol for ad hoc networks. *Elsevier Journal of Ad Hoc Networks*, 5(1):87–99, Jan. 2007.

[9] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2002.

[10] X. Y. Li, K. Moaveninejad, and O. Frieder. Regional gossip routing wireless ad hoc networks. *ACM Journal of Mobile Networks and Applications*, 10(1-2):61–77, Feb. 2005.

[11] 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.

[12] Tao Shu, Sisi Liu, and Marwan Krunz. Secure Data Collection in Wireless Sensor NetworksUsing Randomized Dispersive Routes. IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2009 proceedings.