Random routing scheme with misleading dead ends

Chitra Rajarama[1], Jagadeesha Narasimhamurthy Sugatoor[2], Yerri Swamy T[3]
[1]Department of Information Science & Engineering, NIE Institute of Technology, India
[2]Department of E & C, PES Institute of Technology Management, India
[3]Department of CSE, KLE Institute of Technology, India

Article Info

Article history:

Received Jan 25, 2019
Revised Mar 30, 2019
Accepted Apr 15, 2019

Keywords:

Misleading dead ends
Random routing
Sink location security
Traffic analysis attacks

ABSTRACT

A new method of sink location security in a Wireless Sensor Network is proposed. In the proposed scheme, all the node addresses are encrypted and an attacker cannot determine the real sink address by capturing the packets and analyzing its contents for the final destination. The main contribution of our proposed method is to use random routing scheme with misleading dead ends. This provides security against traffic analysis attack.

Corresponding Author:

Chitra Rajarama,
Department of Information Science & Engineering,
NIE Institute of Technology,
Mysuru 570018, Karnataka, India.
Email: chitramanuel@yahoo.co.in

1. INTRODUCTION

A sink is a critical node in a Wireless Sensor Network, as it collects all the data from the sensors and acts as a gate way to the Internet and other networks. Thus we should provide the highest degree of anonymity and security to the sink [1] from the adversaries. Several works have been done to provide sink location security using random routing and other method [2-5].

In our proposed scheme, packet data security is achieved by encrypting the entire content of the data packet using pairwise secret keys. Traffic analysis attacks are basically passive attacks by adversaries where they listen to the traffic flow and then deduce the direction towards the sink. Here the adversary uses packet tracing technique to reach the sink. To counter this attack we propose the Random Routing Scheme with Misleading Dead Ends (RRSMDE).

2. BASIC SCHEME AND WORKING

RRSMDE is basically a randomized multicast routing. Fake copies of the original data packet are transmitted to reach different random dummy destinations while one true copy reaches the actual final destination which is normally the sink. To make matter clear, an instance of the multi-paths of RRSMDE is shown in Figure 1. The shortest path from the source to the sink is called the main path. In Figure 1, the path list [V1, V2, V3, V4, V5] gives the main path which is shown in the black bold font.

Here V_1 is the source and V_5 is the sink node. In this paper, symbol V_j represents both the node name (identity) and the encrypted node address of node j where j $\in$ {1 to N}.

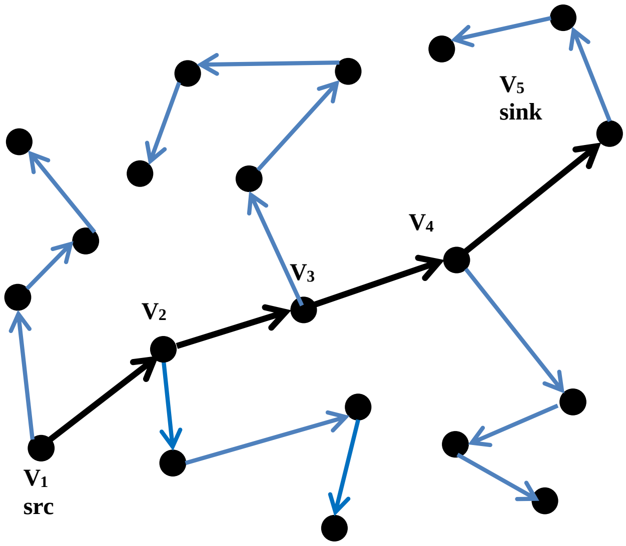

Figure 1. RRMSDE multicast paths

The nodes along the main path are called the *main path nodes*. In our scheme, branching towards the random fake destinations takes place at successive main path nodes including the final destination node. In Figure 1, multicast branching occurs along the main path at nodes V_1, V_2, V_3, V_4, and V_5. Sub branches are shown in blue. In our scheme, at present, only one sub branch originates at each branch point. The number of branch points is equal to the number of nodes along the main path. The number of sub branches in Figure 1 is 5. In Figure 1, the lengths of the sub branches are all chosen randomly. The original packet is sent along the main path and this packet is called the main packet. The main packet header information is updated at each main path node as it travels along the main path and ultimately reaches the final destination. At each branch point, an altered copy of the main packet, called the fake packet, is created and it is sent along the sub branch for its travel further. The update operation of the main packet and the creation of fake packets are described later. In RRSMDE, the sink (the final real destination) is not one of the dead ends. A branch path starts from the sink and continues further. This is to confuse the attacker further.

2.1. Packet header information for the main path

The address information stored in the encrypted form in the main packet header is shown in Table 1. In general, the Main Packet at start is called MP_1 and that at k^{th} main node is called MP_k, for k = 1 to L where L is the total number of nodes in the Main Path. The k^{th} node transmits MP_k to the (k+1)th node.

Table 1. Header fields in the main packet MP_1 at source V_1

Present Source Address	Next Destination Address	Node count k	Main Path List	Others
Initially V_1	V_2	1	[V_1, V_2, …, V_L]	--------

The second row gives the corresponding terms from the Example of Figure 1. The header content of the main packet, travelling from the original source to the final destination, changes as the packet goes from the present node to the next node. In general, the Main Packet at start is called MP_1 and that at k^{th} main node is called MP_k, for k = 1 to L where L is the total number of nodes in the Main Path. The k^{th} node transmits MP_k to the $(k+1)^{th}$ node. When the main packet reaches V_2, The present address is updated to V_2 and the next destination address is updated from the Main Path List and k is incremented by 1. In general, when the main packet arrives at the k^{th} node of the main path the values of the address fields and k value before and after updating would be as shown in Table 2.

Table 2. Header fields of the packet at k^{th} main path node

Present Source Address	Next Destination Address	Node count k	Main Path List	Others
		Before update		
V_{k-1}	V_k	k−1	$[V_1,V_2, ,,\ldots, V_L]$	------
		After update		
V_k	V_{k+1}	k	$[V_1,V_2, ,,\ldots, V_L]$	------

The values of Table 2 hold true for $k = 2, 3,\ldots, L-1$. Note that the L^{th} node is the sink and no further update and forwarding at the sink, because the main path routing is over. When the main packet arrives at the sink, it checks that k = L and also the present source address field value $V_k = L$. In our scheme, the main packet contains the address of the next destination. Thus we use source routing to send the main data.

2.2. Sub branch paths and packets

A sub branch originates from every main path node. The sub branch path starting from V_k is called SB_k. In Figure 1, $SB_2 = [U_{21}, U_{22}, U_{23}, U_{24}]$. The nodes along the sub branch paths are random. The present source node, in a sub branch path, selects the next hop destination randomly among its neighbors excluding the main path nodes and the nodes which have been already traversed so far. When there are no neighbors for a sub branch node, the transmission automatically gets terminated even if TTL has not yet reached zero.

The sub branch packet which is a fake packet contains the Time To Live (TTL) which determines the length of the sub branch path. After each sub branch hop, TTL gets decremented by 1. When the TTL reaches zero, the propagation is terminated.

2.3. Algorithm for the main path propogation

The working of the main path propagation of RRSMDE is represented by the term RRSMDE-MPP and the algorithm RRSMDE-MPP is described as follows.

Algorithm RRSMDE- MPP. Inputs : The shortest path $[V_1, V_2,\ldots,V_k,\ldots, V_L]$.

1. Set k =1. //Start at V_1.
2. Create the main path packet MP_k,
3. Create the fake packet and choose its TTL
4. Start sub branch propagation starting from this main path node V_k.
5. Send the main packet to the next main path node V_{k+1}
6. Receive the packet at V_{k+1}. Update the Present Source Address and the Next Destination Address fields of the main packet
7. Increment k as, k = k+1. //Main packet is fully updated
8. If k = L go to 9. // Final destination is reached
   Else go to 3.
9. Start the sub branch propagation starting from this main path node V_L.
10. Over.

2.4. Sub branch propagation

Sub Branch Propagation (SBP) is a random path travel with fake data packets. The purpose is to confuse the attacker who may follow the packets to discover the destination (sink or BS). In our scheme, one sub branch propagation starts from each main path including the final destination. There are L separate sub branch paths where L is the number of nodes along the main path. The nodes along a sub branch random path are so selected that the nodes do not repeat (which means no loops) and the path excludes the nodes of the main path which provides better security by drawing the attention away from the main path. When the sub branch path ends, the fake packet is discarded.

2.5. RRSMDE Example

The WSN layout is shown in Figure 2. A grid based deployment is used with a few missing nodes at random grid points. Here 82 nodes are distributed in a 10x10 grid. Each grid cell is 100mx100m. The communication range of each node is set to 150 meters. A node can have a maximum of 8 neighbors along north, south, east, west, north-east, south-east, north-west, south-west. In this example, source node is 11 and the final main destination (sink) is node 56.

The shortest (main) path is: [11, 12, 21, 29, 37, 38, 39, 48, 56]. The length of the shortest path SPL = 8. The total number of nodes of the main path = L = 9. There are 9 sub branches. The sub branch paths for one trial are shown in Figure 2. The sub branch path SB3, starting from node 21 does not exist because it has no valid neighbors.

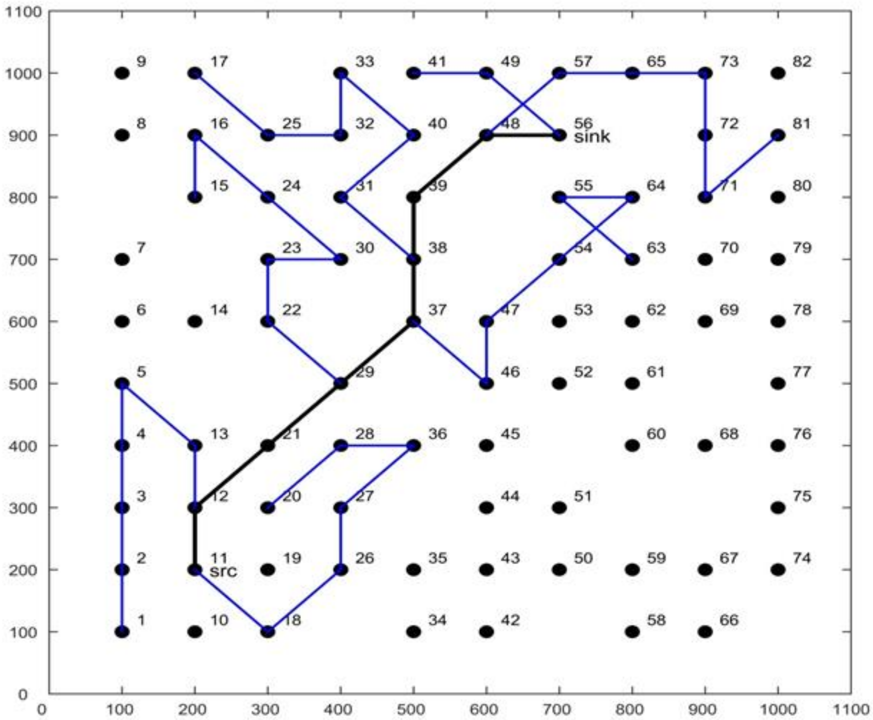

Figure 2. Main path and sub branch paths for example 1. src =11 and sink =56

For the same WSN layout of of Figure 2, the formation of paths when src = 9 and sink = 59 is shown in Figure 3. From Figure 2 and 3, we can see the possible patterns of RRSNDE.

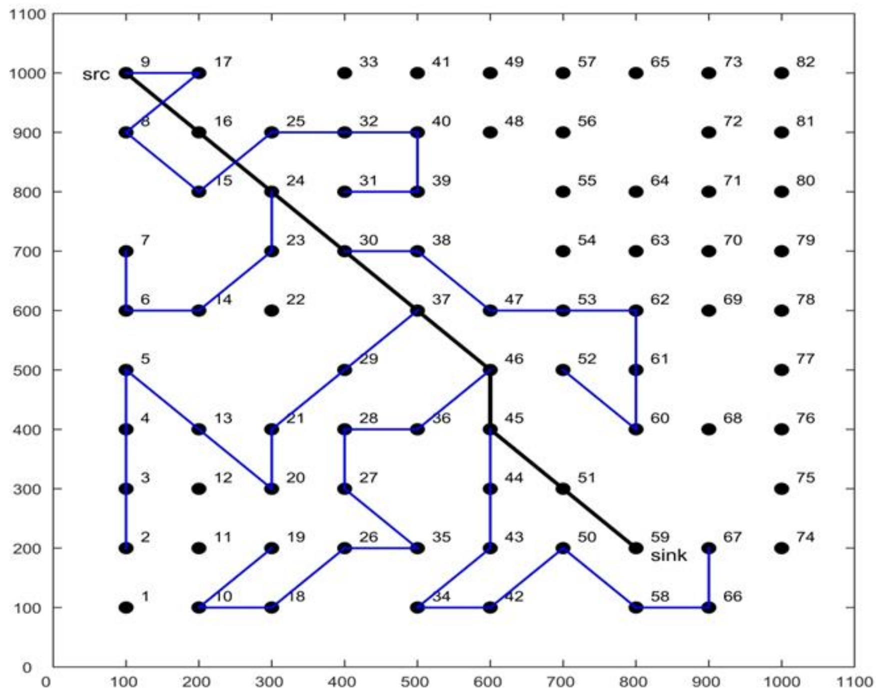

Figure 3. Main path and sub branch paths for example 1. src =9 and sink =59

3. SIMULATION, RESULTS AND RELATIVE PERFORMANCE

3.1. Average Path Length (APL)

APL is measured in terms of the average number of hops required to reach the destination from the source. The packet delivery time mainly depends on the APL. Smaller the APL, better is the performance. In RRSMDE, the true packets follow the shortest (main) path from the source to the destination. Therefore the APL is same as the Shortest Path Length (SPL). Both are expressed in terms of the number of hops. Therefore,

$$APL(RRSMDE) = SPL \quad (1)$$

In Purely Random Propagation (PRP) [6] and Location Privacy Routing (LPR) [7], the routes are randomized. In PRP, the APL is given by,

$$APL(PRP) = average(TTL)+SPL \quad (2)$$

Here, TTL is the length of the random part of the path in each trial. In LPR, the average length of the routing path is given by [7],

$$APL(LPR) = \{1/(1-2*Pf)\}*SPL \quad (3)$$

Here, Pf is the probability of selecting the next node further away from the destination.

Taking the WSN as given in the Example of Section 2.4, the APLs are calculated for different SPL values and for different methods. In calculating APL(PRP), average(TTL) is obtained by taking 100 trials with TTL(max) set to 8. In calculating APL(LPR), Pf is taken as 0.2. The variation of APL which represents the packet delivery time is shown in Figure 4.

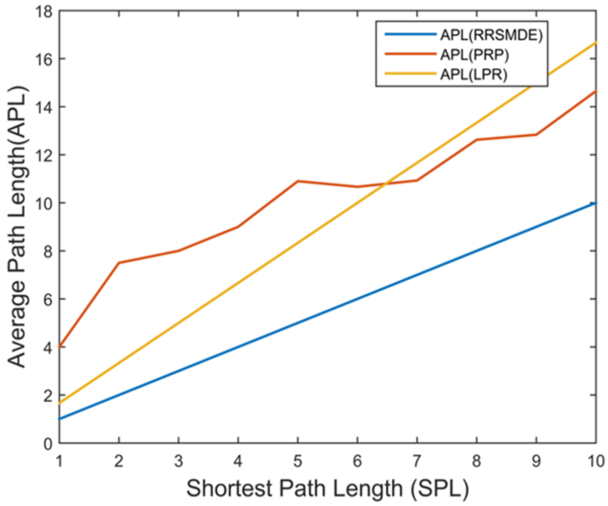

Figure 4. Average path length vs shortest path length

3.2. Overall Energy Consumption (OEC)

The Overall Energy Consumption (OEC) for a given trial (to send a data packet from src to dst) depends on the total length of the paths generated (both main and sub branch paths) or the Total Number of Hops (TNH). The TNH values for algorithms RRSMDE, PRP and LPR are given by,

$$TNH(RRSMDE) = SPL + \text{sum of the sub branch path lengths} \quad (4)$$

$$TNH(PRP) = SPL+ average(TTL) \quad (5)$$

$$TNH(LPR) = \{1/(1-2*Pf)\}*SPL \quad (6)$$

In PRP and LPR methods, in each, there is only one path per trial.

Variation of TNH with SPL is shown in Figure 5. In the case of RRSMDE, the TNH value is very large because of multiple fake paths. Therefore the energy consumption is more, compared to the other two methods.

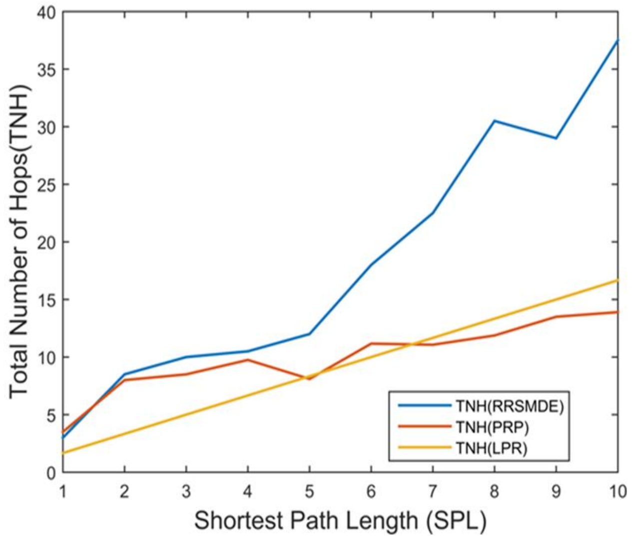

Figure 5. Total number of paths (TNH) vs shortest path length

3.3. Strength of receiver anonymity protection

In evaluating the strength of the receiver anonymity, we use the adversary model as in [7]. One of the measures to represent the strength of receiver anonymity is Adversary's Attack Time (AAT) which is "measured as the number of moving steps (from one sensor location to a neighbor) the adversary has to make before he reaches the receiver". In RRSMDE, the adversary has to traverse each sub branch twice, once to go forward (miss the real receiver) and then to retreat. Therefore the number of steps the adversary has to traverse before reaching the final destination is given by,

$$AAT(RRSMDE) = SPL + 2*\text{sum of the sub branch path lengths} \quad (7)$$

In PRP and LPR, AAT is same as the Average Path Length, APL, as given by (2) and (3). Variation of AAT with SPL is shown in Figure 6. The results are obtained by analytical calculations. In the case of RRSMDE, the AAT value is very large because of multiple fake paths. Therefore the strength of anonymity is very high, compared to the other two methods.

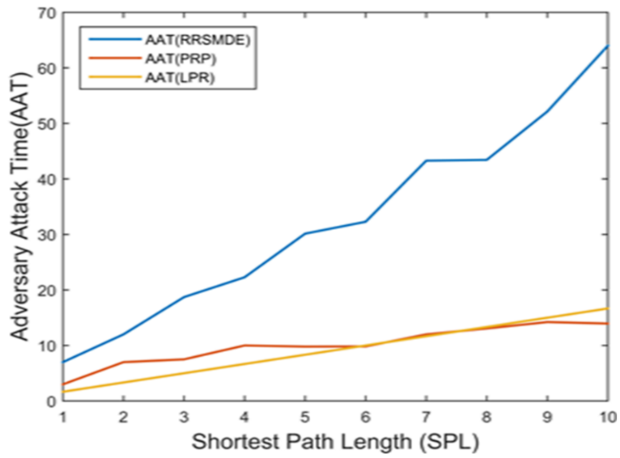

Figure 6. Adversary's attack time (AAT) vs shortest path length

4. CONCLUSION

A new method of random routing scheme with misleading dead ends is presented. The packet tracing attacker will be utterly confused because of multiple random paths which lead to wrong dead ends. From the relative performance plots, it can be seen that RRSMDE is much better than other methods.

REFERENCES

[1] Lin Yao, Lin Kang, Pengfei Shang, Guowei Wu, "Protecting the sinklocation privacy in wireless sensor networks," *Personal and Ubiquitous Computing*, vol. 17, no. 5, pp 883–893, June 2013.

[2] A. R. Malviya and B. N. Jagdale, "Location privacy of multiple sink using zone partitioning approach in WSN," 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, 2015, pp. 449-454.

[3] Pavitha N, S. N. Shelke. "Techniques for Protecting Location Privacy of Source and Sink Node Against Global Adversaries in Sensor Network," *International Journal of Research (IJR)*, vol. 1, no. 8, pp. 42-50, September 2014.

[4] Chinnu George, Dhinakaran Nathaniel, "Protecting Location Privacy in Wireless Sensor Networks against a Local Eavesdropper–A Survey," *International Journal of Computer Applications*, vol. 56, no. 5, pp. 25-29, October 2012.

[5] Ngai, Edith. "On providing sink anonymity for sensor networks." *Security and Communication Networks*, vol. 9, no. 2, pp. 269-273, January 2009.

[6] T. Shu, M. Krunz and S. Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes," in *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 941-954, July 2010.

[7] Y. Jian, S. Chen, Z. Zhang and L. Zhang, "Protecting Receiver-Location Privacy in Wireless Sensor Networks," *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, Barcelona, 2007, pp. 1955-1963.

BIOGRAPHIES OF AUTHORS

Chitra Rajarama. received her B.E., in Computer Science & Engineering., and M.Tech., in Computer Science & Engineering, from Visvesvaraya Technological University, Belgaum, Karnataka, India . She is currently pursuing PhD under Visvesvaraya Technological University, Belgaum, Karnataka, India. Her area of interest is in the field of wireless networks. She has guided many undergraduate projects. She has attended many national/international conferences and published several papers in international journals. At present she is Associate Professor in the department of Information Science & Engineering, NIE Institute of Technology, (affiliated to Visvesvaraya Technological University) Mysuru, Karnataka, India,

Dr. S.N. Jagadeesha received his B.E.,in Electronics and Communication Engineering, from University B. D. T. College of Engineering., Davangere affiliated to Mysore University, Karnataka, India in 1979, M.E. from Indian Institute of Science (IISC), Bangalore, India specializing in Electrical Communication Engineering., in 1987 and Ph.D. in Electronics and Computer Engineering., from University of Roorkee, Roorkee, India in 1996. He is an IEEE member. His research interest includes Array Signal Processing, Wireless Sensor Networks and Mobile Communications. He has published and presented many papers on Adaptive Array Signal Processing and Direction-of-Arrival estimation. Currently he is professor in the department of Electronics and Communications Engineering, PES Institute of Technology & Management, (Affiliated to Visvesvaraya Technological University), Shimoga, Karnataka, India.

Dr. Yerri Swamy T received his B.E.,in Electronics and Comm-unication Engineering, from Gulbarga Univerisity,Gulbarga, Karnataka , India in 2000. MTech in Network and Internet Engineering, from Visve-svaraya Technological University, Belgaum, Karnataka. at J. N. N. College of Engineering, Shimoga, Karnataka in 2005. and PhD in the Faculty of Computer and Information Sciences from Visvesvaraya Technological niversity, Belgaum, Karnataka in the year 2013. He is an ISTE member. His research interest includes Antenna Array Signal Processing, Statistical Signal Processing, Detection and Estimation, Cognitive radio comm-unications ,LTE/MIMO. He has published and presented number of papers in national/international conferences and journals. Currently he is Professor and Head, in the department of Computer Science & Engineering, KLE Institute of Technology, (Affiliated to Visvesvaraya Technological University), Hubli, Karnataka, India.