PERFORMANCE ANALYSIS OF COST AWARE SECURE ROUTING PROTOCOL

Bharathi P[1] ' Nithyalakshmi R [2]

M.E Communication Systems[1] , Assistant Professor[1]

Department of Electronics and Communication Engineering

Bharathiyar Institute of Engineering for Women

(bhararul14@gmail.com)1 ' (nithyalaxshimibaskar@gmail.com)[2]

Abstract

Natural life optimization and security are two conflicting intend issue for multi-hop wireless sensor networks (WSNs) with non-replenishable power resources. In this paper, we first propose a original secure and resourceful Cost-Aware Secure Routing (CASER) protocol to talk to these two incompatible issues through two variable parameters: energy balance control (EBC) and probabilistic based unsystematic walking. We then find out that the energy consumption is severely disproportional to the even energy exploitation for the given network topology, which really reduces the lifetime of the sensor networks. To solve this problem, we propose an professional non-uniform energy deployment strategy to optimize the lifetime and communication delivery ratio under the same power foundation and security requirement.

KEYWORDS: CASER, lifetime, non replish

I Introduction

The recent technical advances make wireless sensor networks (WSNs) technically and economically feasible to be widely used in both armed and civilian applications, such as monitoring of ambient conditions related to the situation precious species and serious infrastructures. A key feature of such networks is that each network consists of a large number of untethered and unattended feeler nodes. These nodes often have very imperfect and non-replenishable energy possessions which makes energy an important design issue for these network Routing is another very testing design issue for WSNs. A correctly designed routing protocol should not only ensure a high declaration delivery ratio and low energy consumption for communication delivery, but also balance the entire sensor network energy consumption, and thereby enlarge the sensor network lifetime. In addition to the abovementioned issues, WSNs rely on wireless relations, which is by nature a transmit medium. It is more vulnerable to security attacks than its wired counterpart due to lack of a physical periphery In particular, in the wireless sensor domain, anybody with an fitting wireless receiver can monitor and intercept the sensor set of connections communications. The adversaries may use expensive radio transceivers, powerful workstations and act together with the network from a distance since they are not controlled to using sensor network hardware. It is possible for the adversary to perform jamming and routing traceback attacks.

Motivated by the fact that WSNs routing is often natural features- base we propose a natural features based secure and efficient Cost-Aware Secure routing (CASER) protocol for WSNs without relying on flood CASER allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same construction The allocation of these two strategies is determined by the specific security necessities This scenario is analogous to delivering USMail through USPS: express mails costmore than regular mails; still mails can be delivered faster. The protocol also provides a secure communication delivery option to maximize the message delivery ratio under adversarial attacks. In addition, we also give quantitative protected analysis on the expected routing protocol based on the criterion proposed in [1]. CASER protocol has two chief advantages: (i) It ensures balanced energy preservation of the entire sensor network so that the lifetime of the WSNs (ii) CASER protocol supports multiple routing strategy based on the routing supplies, including fast/slow message rescue and secure message delivery to prevent routing traceback attacks and nasty traffic congestion attacks inWSNs.

Our offerings of this paper can be summarized as follows:

1) We propose a protected and efficient Cost-Aware Secure Routing (CASER) protocol for WSNs. In this protocol, cost-aware based excursion strategy can be applied to address the message rescue requirements.

2) We devise a quantitative system to balance the energy consumption so that both the sensor network lifetime and the total number of communication that can be delivered are maximize under the same energy deployment (ED).

3) We develop hypothetical formulas to estimate the number of routing hops in CASER under unpredictable routing energy balance control (EBC) and safety requirements.

4) We quantitatively investigate security of the proposed routing algorithm.

5) We provide an most favorable non-uniform energy deployment (noED) strategy for the given sensor networks based on the energy consumption ratio. Our hypothetical and imitation results both show that under the same total energy deployment, we can increase the life span and the number of communication that can be delivered more than four times in the non-uniform energy operation scenario.

II RELATED WORK

Routing is a challenging task in WSNs due to the imperfect resources. Geographic routing has been broadly view as one of the most shows potential approaches for WSNs. Geographic routing protocols utilize the geographic spot information to route data packets hop-by-hop from the source to the destination [2]. The source chooses the instantaneous neighboring node to forward the message based on either the direction or the distance [3], [4], [5], [6]. The distance between the neighboring nodes can be estimated or acquire by signal strength or using GPS equipments [7], [8]. The relative location information of neighbor nodes can be exchanged between adjacent nodes. In [5], a geographic adaptive fidelity (GAF) routing scheme was proposed for sensor

networks operational with low power GPS receiver. In GAF, the network area is divided into fixed size virtual grids. In each grid, only one node is chosen as the active node, while the others will sleep for a stage to save energy. The sensor forwards the messages based on insatiable geographic routing strategy. A query based geographic and energy aware routing (GEAR) was proposed in [6]. In GEAR, the sink node disseminate requests with geographic attributes to the intention region instead of using flooding. Each node forwards messages to its adjoining nodes based on estimated cost and learning cost. The estimated cost considers both the distance to the target and the remaining energy of the sensor nodes. While the learning cost provides the updating in sequence to deal with the local minimum problem.

While geographic routing algorithms have the advantage that each node only needs to maintain its adjoining information, and provides a higher efficiency and a better scalability for sweeping WSNs, these algorithms may reach their local minimum, which can result in dead end or loops. To solve the local lowest amount problem, some variation of these basic routing algorithms were proposed in [9], including GEDIR, MFR and compass routing algorithm. The liberation ratio can be improved if each node is aware of its two-hop neighbors. There are a few identification [3], [10], [11], [12] discussed combining greedy and face routing to solve the local bare minimum problem. The basic idea is to set the local topology of the set of associations as a planar graph, and then the relay nodes try to forward communication along one or possibly a succession of contiguous faces toward the destination. Lifetime is another area that has been lengthily studied in WSNs. In [13], a routing scheme was projected to find the sub-optimal path that can make longer the lifetime of the WSNs instead of always selecting the lowest energy path. In the proposed scheme, numerous routing path is set ahead by a inconsiderate protocol such as AODV or directed diffusion. Then, the routing scheme choose a path based on a probabilistic method according to the enduring energy. In [14], Chang and Tassiulas unspecified that the spreader power level can be attuned according to the distance between the spreader and the recipient Routing was formulated as a linear programming problem of neighboring node mixture to maximize the network lifetime. Then Zhang and Shen [15] investigate the unbalanced energy consumption for uniformly deployed data get-together sensor networks. In this paper, the network is divided into multiple nimbus zones and each node can perform data aggregation.

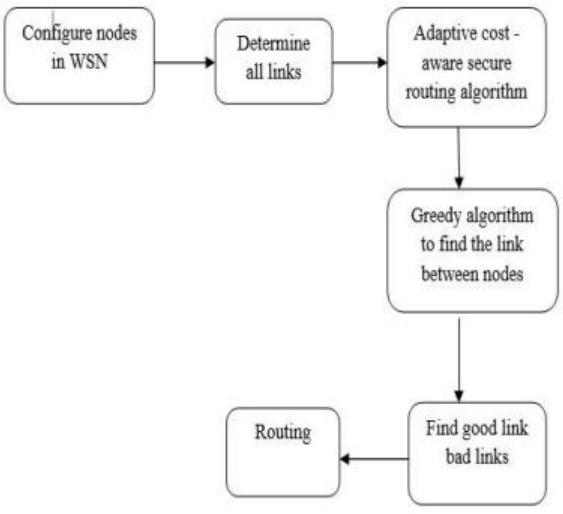


Fig 1: PROPOSED METHOD

A restricted zone-based routing scheme was proposed to balance energy consumption among nodes within each corona. [16] formulated the integrated design of route selection, traffic load allocation, and sleep development to make best use of the network lifetime. Based on the concept of opportunistic routing, [17] urbanized a routing metric to attend to both link reliability and node outstanding energy. The sensor node computes the optimal metric value in a limited to a small area area to achieve both dependability and lifetime maximization. In addition, exposure of routing information presents significant security threats to sensor networks. By achievement of the location and routing information, the adversary may be able to trace back to the source swelling easily. To solve this problem, several schemes have been proposed to provide source-location privacy through secure routing protocol design [18], [19], [20].

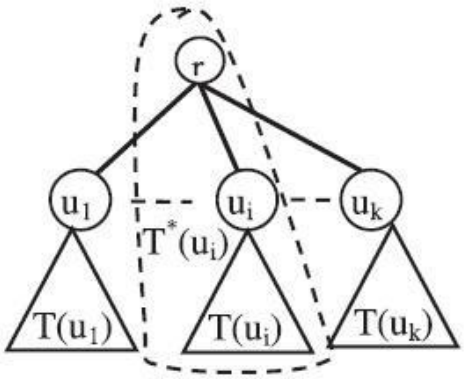
III Proposed Method

We develop two algorithms to solve the problems in secured routing. Both algorithms choose a sequence of links to test. After testing a link, based on whether the relation is good or bad, it obtains the resultant topology following Algorithm 1 or 2, and then chooses another link to test.

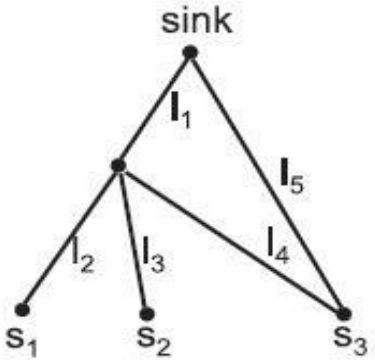
1. Ordering Algorithm.
2. Greedy Algorithm.

Ordering Algorithm

This algorithm picks the link with the highest nk, where 'nk' is the number of paths that use link 'lk'. It Checks links that are used by more paths. In Fig, after finding link 'ui' to be lossy, all the paths using 'ui' are removed, and hence none of the links in the sub tree deep-rooted at 'ui' needs to be tested.



Consider three sources(s1,s2 and s3) send data to a sink. It has five links, l1; . . . ; l5. The ground truth is that links l1 and l5 are bad. The cost for testing a link is 1 unit. The probability that a link is lossy is p =0:2. We denote the bad paths as p1={l2,l1},p2={l3,l1},p3={l4,l1},p4=l5;Without any testing, we identify l5 as a responsible link since it is only used by P4, and P4 is lossy. We, therefore, contract link l5 and remove P4.



Greedy Algorithm

This algorithm picks the link that provides the highest gain. 'Φk' denote the probable gain of link 'lk'.

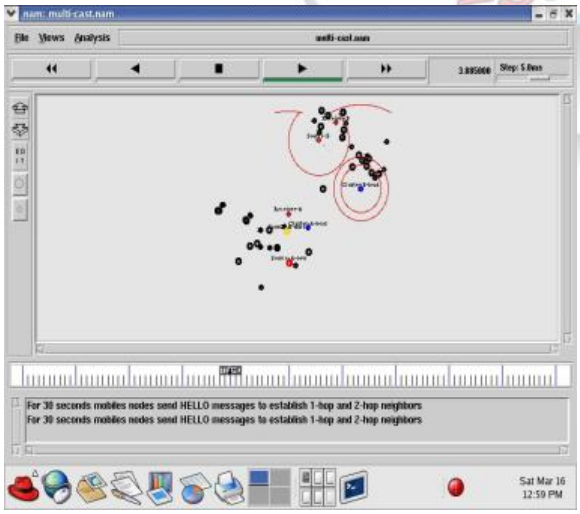
- $\Phi k = p_k \cdot \Phi_{kb} + (1-p_k) \cdot \Phi_{kg} - C_k$

- ‘p_k ‘ is the probability that ‘lk is bad, and ck is the cost of testing lk.
- let Φ_{kb} denote the cost savings when knowing ‘lk’ is bad, and let Φ_{kg} denote the cost savings when knowing ‘lk’ is good.
- Φ_{kg} is the sum of the testing costs of all the responsible and irrelevant links identified after knowing that ‘lk’ is good.
- C_k is the cost of testing ‘lk’.

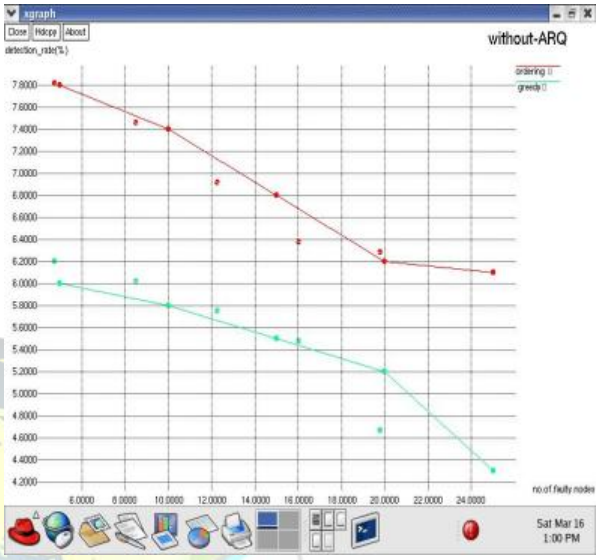
IV Simulation Results

Parameters	Type
channel type	Wireless Channel
radio-propagation model	Two Ray Ground
Antenna type	Omni Antenna
max packet	300
network interface type	Physical layer
Standard	IEEE 802.11b
number of mobile nodes	100
routing protocol	DSR
Initial energy in Joules	1000
Data Rate	1Mbps
Area	1000*1000
Distance between nodes	250

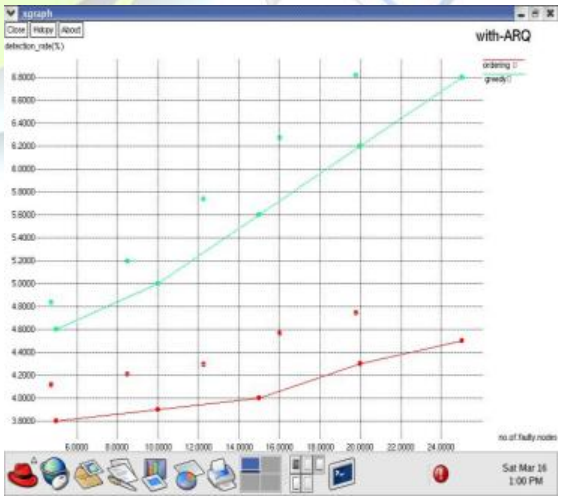
Table 1. Network initial setup



This figure shows that wireless communication between nodes and clusters and cluster head and destination node. The intermediate nodes are marked as black color, source and receiver are manifest as red color and Cluster head is marked as blue color. In this replication, we consider 50 nodes spreaded over the full area.

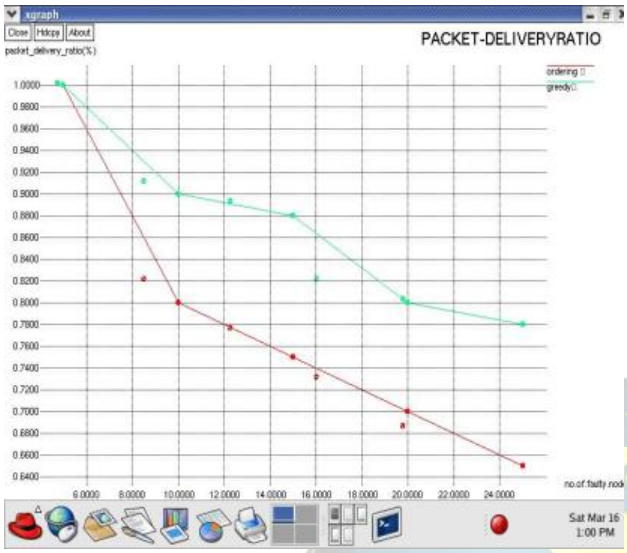


This figure shows that relation between number of faulty nodes and detection rate. If number of faulty nodes are increasing in order, then recognition rate will be decreased. In this method,the ordering algorithm works well than the greedy algorithm.



This figure shows that relation between number of faulty nodes and detection rate. If number of faulty nodes are increasing in order, then detection rate will

be decreased. In this method, the order algorithm works well than the greedy algorithm.



This figure shows that relation between number of faulty nodes and Packet delivery ratio. If number of faulty nodes is increasing in order, then delivery ratio will be decreased.

V Conclusion

In this paper, we existing a secure and professional Cost- Aware SEcure Routing (CASER) protocol for WSNs to sense of balance the energy consumption and increase network lifetime. CASER has the flexibility to support numerous routing strategy in message forward to extend the lifetime while increasing routing defense Both theoretical analysis and simulation results show that CASER has an excellent routing show in terms of energy balance and routing path allocation for routing path security.

VI REFERENCES

[1] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 7, pp. 1302–1311, Jul. 2012.

[2] Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in Proc. IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.

[3] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in Proc. 6th Annu. Int. Conf.

Mobile Comput. Netw., New York, NY, USA, 2000, pp. 243–254.

[4] J. Li, J. Jannotti, D. S. J. De Couto, D. R.

Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," in

Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 120–130.

[5] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing," in Proc. 7th Annu.

ACM/IEEE Int. Conf. Mobile Comput. Netw., 2001, pp. 70–84.

[6] Y. Yu, R. Govindan, and D. Estrin,

"Geographical and energyaware routing: A recursive data dissemination protocol for wireless sensor networks," Comput. Sci.

Dept., UCLA, TR-010023, Los Angeles, CA, USA, Tech. Rep., May 2001.

[7] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoor localization for very small devices," Comput. Sci. Dept.,

Univ. Southern California, Los Angeles, CA, USA, Tech. Rep. 00- 729, Apr. 2000.

[8] A. Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic finegrained localization in ad-hoc networks of sensors," in Proc. 7th ACM Annu. Int. Conf. Mobile Comput. Netw., Jul. 2001, pp. 166–179.

[9] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," in Proc. 3rd Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., 1999, pp. 48–55.

[10] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," in Proc. 3rd ACM Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., Seattle, WA, USA, Aug. 1999, pp. 48–55.

[11] T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowledge for energy efficient geographical routing in sensor networks," in Proc. IEEE Conf. Comput. Commun., Mar. 2004, vol. 3, pp. 1705–1716.

[12] Y. Li, Y. Yang, and X. Lu, "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," IEEE Trans. Mobile Comput., vol. 9, no. 4, pp. 582–595, Apr. 2010.

[13] R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in Proc. IEEE Wireless Commun. Netw. Conf., Mar. 17–21, 2002, vol. 1, pp. 350–355.

[14] J.-H. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 609–619, Aug. 2004.

[15] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 10, pp. 1526–1539, Oct. 2009.

[16] F. Liu, C.-Y. Tsui, and Y. J. Zhang, "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks," IEEE Trans. Wireless Commun., vol. 9, no. 7, pp. 2258–2267, Jul. 2010.

[17] C.-C. Hung, K.-J. Lin, C.-C. Hsu, C.-F. Chou, and C.-J. Tu, "On enhancing network-lifetime using opportunistic routing in wireless sensor networks," in Proc. 19th Int. Conf. Comput. Commun. Netw., Aug. 2010, pp. 1–6.

[18] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw., 2004, pp. 88–93.

[19] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in Proc. IEEE 6th Annu. Commun. Soc. Conf. Sens., Mesh Ad Hoc Commun. Netw., Rome, Italy, Jun. 2009, pp. 493–501.

[20] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in Proc. IEEE INFOCOM 2010, San Diego, CA, USA., Mar. 15–19, 2010. pp. 1–9.

[21] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in Proc. IEEE 27th Conf. Comput. Commun., Apr. 2008, pp. 51–55.

[22] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2005, pp. 599–608.