International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 7 –OCTOBER 2016.

Secured and Efficient Routing Strategy for Wireless Sensor Networks Using CASER

MUDIGONDA NAGAPURNA CHANDRA RAO[#1] and SAYEED YASIN[*2]

[#] *Student, M.Tech (C.S.E), Nimra College of Engineering & Technology, A.P., India.*

[*] *Associate professor & Head, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

***Abstract*— Wireless Sensor Networks have the solutions which maintains extensive range of applications. Based on the application, their WSN environment is the risky, challenging and fewer problematic. Even the Encoded Security Systems in WSNs not to notice the node physical internment, the malicious or selfish nodes. A novel secure and efficient Cost-Aware secure Routing (CASER) protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic based random walking. We then discover that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. For this propose an efficient no uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. Here also provide a quantitative security analysis on the proposed routing protocol. The theoretical analysis and OPNET simulation results demonstrate that the proposed CASER protocol can provide an excellent tradeoff between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks in all scenarios. For the non-uniform energy deployment, the analysis shows that we can increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption. Thisdemonstrate that the proposed CASER protocol can achieve a high message delivery ratio while preventing routing trace back attacks.**

***Index Terms*— Security ,WSN, CASER,OPNET.**

I. INTRODUCTION

Wireless sensor networks (WSNs) are an important for monitoring distributed remote environments. As one of the key technologies involved in WSNs, nodes fault detection is indispensable in most WSN applications. It is well known that the distributed fault detection scheme checks out the failed nodes by exchanging data and mutually testing among neighbor nodes in this network, but the fault detection accuracy of a scheme would decrease rapidly when the number of neighbor nodes to be diagnosed is small and the node's failure ratio is high. an improved scheme is proposed by defining new detection criteria. Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties Routing is another very challenging design issue for WSNs. A properly designed routing protocol should notonly ensure a high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime. Motivated by the fact that WSNs routing is often geography-based secure and efficient Cost-Aware secure routing (CASER) protocol for WSNs without relying on flooding. CASER allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same framework. The distribution of these two strategies is determined by the specific security requirements. This scenario is analogous to delivering US Mail through USPS: express mails cost more than regular mails; however, mails can be delivered faster. The protocol also provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks. CASER protocol has two major advantages: (i) It ensures balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized. (ii) CASER protocol supports multiple routing strategies based on the routing requirements, including fast/slow message delivery and secure message delivery to prevent routing trace back attacks and malicious traffic jamming attacks in WSNs

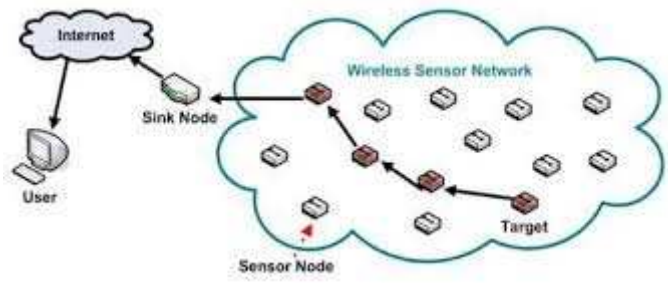

Figure 1: Wireless Sensor Networks

II. PROPOSED SYSTEM

Cost-Aware SEcure Routing (CASER) protocol that can address energy balance and routing security concurrently in WSNs. In CASER protocol, each sensor node needs to maintain the energy levels of its immediate adjacent neighbouring grids in addition to their relative locations. Using this information, each sensor node can create varying filters based on the expected design trade-off between security and efficiency. The quantitative security analysis demonstrates the proposed algorithm can protect the source location information from the adversaries -justified.

1. Network formation In this module the network is formed for secure routing. The networks are composed of a large number of sensor nodes and a sink node. Each sensor node has a very limited and non-replenish able energy resource. The sink node is the only destination for all sensor nodes to send messages to through a multi-hop routing strategy. The network is evenly divided into small grids. Each grid has a relative location based on the grid information. The node in each grid with the highest energy level is selected as the head node for message forwarding. Each node in the grid will maintain its own attributes, including location information, remaining energy level of its grid, as well as the attributes of its adjacent neighbouring grids. The information maintained by each sensor node will be updated periodically.

2. Energy Balance Routing [0, 1]. Nodeα αThis module send message from sensor to sink using EBC (Energy Balance Control) parameter maintains its relative location and the remaining energy levels of its immediate adjacent neighboring grids. For node A, NA. Withαdenote the set of its immediate adjacent neighboring grids as NA and the remaining energy of grid i as Eri , i NA Eri..αiαthis information, the node A can compute the average remaining energy of the grids in NA as Ea(A) = 1/NA To achieve energy balance among all the grids in the sensor network, we carefully monitor and control the energy consumption for the nodes with relatively low energy levels by configuring A to only select the grids with relatively higher remaining energy levels for message forwarding. . Increasing ofα Ea(A)} based on the EBC α α NA | Eri αA={i αThe candidate set for the next hop node as N a may also increase the routing length. However, it can effectively control energy consumption from the nodes with Ea(A).αenergy levels lower than Ea(A).

3. Caser Routing This module provides routing path unpredictability and security. The routing protocol contains two options for message forwarding: one is a deterministic shortest path routing grid selection algorithm, and the other is a secure routing grid selection algorithm through random walking. A based on the relative locations of theαIn the deterministic routing approach, the next hop grid is selected from N grids. The grid that is closest to the sink node is selected for message forwarding. In the secure routing case, the next hop A for message forwarding. The distribution of these two algorithms is controlled by aαgrid is randomly selected from N [0, 1] carried in each message.ααsecurity level called then the nodeα α α[0,1], If ααWhen a node needs to forward a message, the node first selects a random number selects the next hop grid based on the shortest routing algorithm; otherwise, the next hop grid is selected using random is small the results in a shorter routing pathα is an adjustable parameter. The Value of αwalking. The security level provides more routing diversity andαand is more energy efficient in message forwarding. On the other hand, a larger security.

III. LITERATURE SURVEY

G.Wang[1]Sensor deployment is an important issue in designing sensor networks. This evaluates a distributed sensor Protocols for mobile sensors. After discovering coverage holes the protocols calculate the position of sensors where they should move. The protocols that provide high coverage within a limited deployment time and limited movement. We use Voronoi diagrams to discover the coverage holes and design three movement-assisted sensor deployment protocols, VEC (VECtorbased),VOR and Minimax based on the principles of moving sensors from densely deployed areas to sparsely deployed areas.

X. Li[2] achieving focused coverage around a Point of Interest, and introduce an evaluation metric, coverage radius. The self deployment sensors is an important research that deals with self directed coverage formation in mobile sensor network. The two purely localized solution protocols Greedy Advance (GA) and Greedy-Rotation-Greedy(GRG), which are rigid to node failures and work regardless of network partition. The algorithms drive sensors to move along a locallycomputed triangle tessellation(TT) to surround the Point of Interest. In Greedy Advance, nodes greedily keep as close to the Point of Interest as they can; in GRG, when their greedy advance is blocked, nodes rotate around the POI to a TT vertex.

Y. Zou and K. Chakrabarty[3] cluster based distributed sensor deployment. A virtual force algorithm(VFA)as a sensor Deployment strategy to enhance the coverage after the placement of sensors, VFA attempts to maximize the sensor field coverage. Once the effective sensor positions are identified. The one time movement with energy consideration incorporated is carried out i.e., the sensor are redeployed to these positions. The positioning of sensors affects coverage, communication cost and resource management. The positioning of sensors affects given number of sensors within a cluster in cluster based DSNs. For a given number of sensors, the VFA algorithm attempts to maximize the sensor countryside coverage. We also propose a novel probabilistic target localization algorithm that is executed by the cluster head to query only a few sensors (out of those that report the presence of a target) for more detailed information.

IV. RELATED WORK

The base station plays an important role in finding multiple

paths between the source and the sink node. The control overhead is very high in the SEEM model as it uses Neighbour Discovery (ND) packet, Neighbour Collection (NC) packet and Neighbour Collection Reply (NCR) packet in the routing protocol. The ND packet is broadcast in network to know the neighbouring nodes of every node. Once all the nodes identify their neighbouring nodes, the base station node broadcasts NC packets in order to collect the neighbour's information of each node gathered during the previous broadcasting. The sensor nodes acknowledge to the NC packet by sending the neighbour collection reply packet to the base station. They SEEM model justifies the security without using the crypto system mechanism in the routing protocol.

A .Maximum Lifetime Routing In Wireless Sensor Networks The problem of routing messages in a wireless sensor network so as to maximize network lifetime is NP-hard. In our model, the online model, each message has to be routed without knowledge of future route requests. Here develop also an online heuristic tomaximize network lifetime. Our heuristic, which performs two shortest path computations to route each message, is superior to previously published heuristics for lifetime maximization– our heuristic results in greater lifetime and its performance is less sensitive to the selection of heuristic parameters. Additionally, our heuristic is superior on the capacity metric.A new online heuristic– OML–for lifetime maximization. Extensive simulations show that new heuristic is superior to previously published heuristics for lifetime maximization both in terms of providing larger lifetime and in terms of sensitivity to algorithm parameters. Additionally, proposed heuristic provides larger network capacity than provided by competing heuristics.

B. Routing with Guaranteed Delivery in ad hoc Wireless Networks Mobile ad hoc networks (Manets) consist of wireless hosts that communicate with each other in theabsence of infrastructure. Two nodes in a manet can communicate if the distance between them is less than the minimum of their two broadcast ranges. Because stations whose broadcast areas overlap can interfere with each other and also because of health problems that can occur because of long-term exposure to powerful radio signals , it is generally not possible (or desirable) for all hosts in a manet to be able to communicate with each other directly. Thus, sending messages between two hosts in a Manet may require routing the message through intermediate hosts. In many cases, Manets are pieced together in an uncontrolled manner, changes in topology are frequent and unstructured, and hosts may not know the topology of the entire network. Consider routing in manets for which hosts know nothing about the network except their location and the locations of the hosts to which they can communicate directly. In particular, we consider the case in which all hosts have the same broadcast rangeAlgorithms for routing, broadcasting and geocasting in unit graphs. The algorithms do not require duplication of packets, or memory at the nodes of the graph, and yet guarantee that a packet is always delivered to (all of) its destination(s).

C. Energy Aware Routing for Low Energy Ad Hoc Sensor Networks These schemes typically try to find the minimum energy path to optimize energy usage at a node. In this we take the view that always using lowest energy paths may not be optimal from the point of view of network lifetime and long-term connectivity. To optimize these measures, a new scheme called energy aware routing that uses suboptimal paths occasionally to provide substantial gainsa new routing protocol that is suitable for low energy and low bit rate networks. The idea behind the protocol is very simple – using the lowest energy path always is not necessarily best for the long-term health of the network.

D. Source-Location Privacy in Energy-Constrained Sensor Network Routing Source-location privacy is critical to the successful deployment of wireless sensor networks. In this paper we first propose and analyze a routing-based scheme through single-intermediate node. Then two multi intermediate node schemes are introduced. For each of these schemes, we carried out simulations to evaluate the performances. Simulation results demonstrate that the proposed schemes can achieve very good performance in energyonsumption, message delivery latency and message delivery ratio.

V. CONCLUSION

In this paper, we presented a secure and efficient Cost-Aware SEcure Routing (CASER) protocol for WSNs to balance the energy consumption and increase network lifetime. CASER has the flexibility to support multiple routing strategies in message forwarding to extend the lifetime while increasing routing security. Both theoretical analysis and simulation results show that CASER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. We also proposed a non-uniform energy deployment scheme to maximize the sensor network lifetime. Our analysis and simulation results show that we can increase the lifetime and the number of messages that can be delivered under the non-uniform energy deployment by more than four times..

REFERENCES

[1] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, accepted, to appear.

[2] Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in IEEE INFOCOM 2012 Mini-Conference, Orlando, Florida, USA., March 25-30, 2012 2012.

[3] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in MobiCom'2000, New York, NY, USA, 2000, pp. 243 – 254.

[4] J. Li, J. Jannotti, D. S. J. D. C. David, R. Karger, and R. Morris, "A scalable location service fo geographic ad hoc routing," in MobiCom'2000. ACM, 2000, pp. 120 – 130.

[5] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing," in the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2001, pp. 70–84.

[6] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks," UCLA Computer Science Department Technical Report, UCLACSD, May 2001.

[7] S. Yang, M. Li, and J.Wu, "Scan-based movement-assisted sensor deployment methods in wireless sensor networks," IEEE Trans. Parallel Distrib.Syst.,vol.18,no.8,pp.1108– 1121,Aug.2007
[8] Y. Zou and K. Chakrabarty, "Sensor deployment and target localization based on virtual forces," in Proc. 22nd Annu.Joint Conf. INFOCOM, San Francisco, CA, Apr. 2003, pp. 1293–1303.
[9] X. Li, H. Frey, N. Santoro, and I. Stojmenovic, "Localized sensor selfdeployment with coverage guarantee," ACM Sigmobile Mobile Comput.Commun. Revi., vol. 12, no. 2, pp. 50–52, Apr. 2008.
[10] K. Akkaya and M. Younis, "COLA: A coverage and latency aware actor placement for wireless sensor and actor networks," in Proc. IEEE VTC, Montreal, QC, Canada, Sep. 2006, pp. 1–5.
[11] R.-S. Chang and S.-H. Wang, "Self-deployment by density control in sensor networks," IEEE Trans. Veh. Technol., vol. 57, no. 3, pp. 1745–1755, May 2008
[12] Z. Shen, Y. Chang, H. Jiang, Y. Wang, and Z. Yan, "A generic framework for optimal mobile sensor redeployment," IEEE Trans. Veh. Technol.,vol. 59, no. 8, pp. 4043–4057, Oct. 2010.

MUDIGONDA NAGAPURNA CHANDRA RAO, is a student of NIMRA COLLEGE OF ENGINEERING AND TECHNOLOGY, JUPUDI,IBRAHIMPATNAM. He is presently pursuing his M.Tech degree from JNTU, Kakinada. He has obtained B.Tech, degree from JNTU, Kakinada.

SAYEED YASIN received his M.TECH in Computer Science & Engg from JNTU Hyderabad. He is pursuing Ph.D., in Rayalaseema University, Kurnool. He is currently working as an Associate Professor & Head in Nimra College of Science & Technology the Department of Computers Science and Engineering & Technology, Jupudi, Ibrahimpatnam,Vijayawada-521456. He has more than Eight years of experience in teaching field. His area of interests are wireless networks & programming, & Mobile Computing.