Improving Security and Enhancing Energy Efficiency in Routing for Wireless Sensor Networks

[1]Sangeeta Malik, [2]Sitender Malik
[1]Vaish College of Engineering, M.D.U, Rohtak, India
[2]N.C .College College of Engineering, K.U., Kurukshtra, India

Abstract
Wireless sensor networks are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. Wireless Sensor Networks (WSNs) have been increasingly available for large-scale applications in which energy efficiency & security is an important performance measure. Driven by the energy & security limitation nature of WSNs lots of research works have been done in aspects such as nodes replication,data aggregation routing, clustering for better coverage of network security moniroting etc.In this paper we implement a grid network.Then we propose a Horizontal –Vertical method for load balancing of the grid network.

Keywords
Wireless, Sensors, Replication, Aggregation, Clustering

I. Introduction

Wireless Sensor Networks have emerged as an important new area in wireless technology. In the near future, the wireless sensor networks are expected to consists of thousands of inexpensive nodes, each having sensing capability with limited computational and communication power [1-3] which enable us to deploy a large-scale sensor network.

A wireless network consisting of tiny devices which monitor physical or environmental conditions such as temperature, pressure, motion or pollutants etc. at different areas. Such sensor networks are expected to be widely deployed in a vast variety of environments for commercial, civil, and military applications such as surveillance, vehicle tracking, climate and habitat monitoring, intelligence, medical, and acoustic data gathering. The key limitations of wireless sensor networks are the storage, power and processing. These limitations and the specific architecture of sensor nodes call for energy efficient and secure communication protocols.

The key challenge in sensor networks is to maximize the lifetime of sensor nodes due to the fact that it is not feasible to replace the batteries of thousands of sensor nodes. Therefore, computational operations of nodes and communication protocols must be made as energy efficient as possible. Among these protocols data transmission protocols have much more importance in terms of energy, Since the energy required for data transmission takes 70 % of the total energy consumption of a wireless sensor network [2]. Area coverage and data aggregation [4], techniques can greatly help conserve the scarce energy resources by eliminating data redundancy and minimizing the number of data transmissions. Therefore, data aggregation methods in sensor networks are extensively investigated in the literature [4-7].

Security in data communication is another important issue to be considered while designing wireless sensor networks, as wireless sensor networks may be deployed in hostile areas such as battlefields [2, 8-9]. Therefore, data aggregation protocols should work with the data communication security protocols.

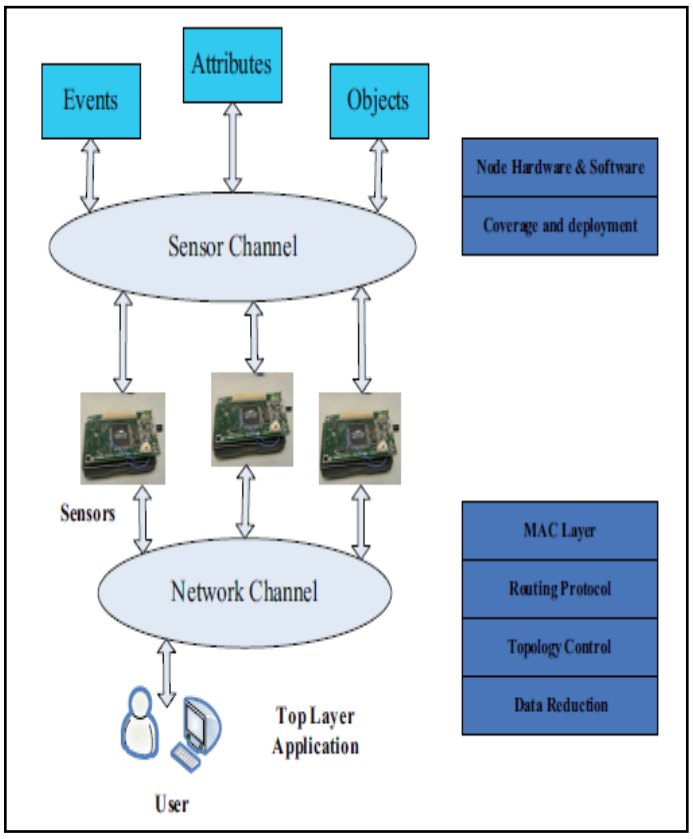

Fig. 1: Wireless Sensor Network Architecture

II. Literature Review

Eschenauer and Gligor [10] propose centralized node revocation in sensor networks. When the base station detects a misbehaving node, it broadcasts a message to revoke that node. Chan, Perrig, and Song [11] propose a localized mechanism for sensor network node revocation; in their approach, nodes can revoke their neighbors. F. Bouhafs [12] and his colleges present a clustering scheme for wireless sensor networks based on semantic properties. It implements Semantization in Wireless Sensor Networks from another angle. They try to minimize the amount and range of communication as much as possible by developing a clustering scheme that involves only nodes that are relevant to a given query or task, and groups them in a cluster.

Ref. [13] addresses the issues related to data integration in wireless sensor networks with respect to heterogeneity, dynamicity, and distribution at both the technology and application levels. The authors present and discuss a query processing algorithm which make use of the semantic knowledge about sensor networks expressed in the form of integrity constraints to reduce network traffic overheads, improve scalability and extensibility of wireless networks and increase the stability and reliability of networks against hardware and software failures.

[14], presents a detailed review of in-network aggregation techniques for wireless sensor networks. Aggregation techniques are an essential building block to keep the WSN operational as long as possible, as they aim to reduce the number of transmissions

required for data collection, which, in turn, reduces energy consumption.

Existing researches have been conducted to address pure data aggregation routing problem in WSN. In [15], they devise three interesting suboptimal aggregation heuristics, Shortest Paths Tree (SPT), Center at Nearest Source (CNS), and Greedy Incremental Tree (GIT) for data centric routing problems. In [16], mathematical formulations for data aggregation problem in WSN are well formulated, and an optimization-based heuristic algorithm is then proposed to tackle the problem.

In EEUC(An Energy-Efficient Unequal Clustering), to address the hot spot problem, author proposed an unequal clustering mechanism to balance the energy consumption among cluster heads [17]. Clusters closer to the base station have smaller sizes than those farther away from the base station, thus cluster heads closer to the base station can preserve some energy for the purpose of inter-cluster data forwarding. And an energy-aware multi-hop routing protocol is proposed for the inter-cluster communication in EEUC mechanism.

Marti et al. [18] and Buchegger and Boudec [19] consider the problem of minimizing the effect of misbehaving or selfish nodes on routing through punishment, reporting, and holding grudges. These application of these techniques to sensor networks is promising, but these protocols are vulnerable to blackmailers.

Perrig et al. [20] present two building block security protocols optimized for use in sensor networks, SNEP and TESLA. SNEP provides confidentiality, authentication, and freshness between nodes and the sink, and u-TESLA provides authenticated broadcast.

III. Proposed Work

We are representing energy efficient secure routing in case of a Wireless Sensor Network. In it we use Grid network to represent the proposed work.

In Grid network, each node is connected with two neighbors along one or more dimensions. If the network is one-dimensional, and the chain of nodes is connected to form a circular loop, the resulting topology is known as a ring.

In general, when an n-dimensional grid network is connected circularly in more than one dimension, the resulting network topology is a torus, and the network is called "toroidal". When the number of nodes along each dimension of a toroidal network is 2, the resulting network is called a hypercube.

In our work there are number of possible approaches of routing. One of such approach is Horizontal-Vertical Mapping. In this, first move one step horizontally and the one step node vertically. Because of this approach the load on the centralized node increased.

To resolve this problem there are some existing methods:-

- Shifting the load on neighbor node based on minimum load
- Removing the center node.

The proposed algorithm we will use for energy efficient & secure routing in wireless sensor network.In this algorithm we follow the following step:-

Algorithm(Network,Source,Destination,N)

/* Network define a Grid Network of N*N Grids from Source to Destination*/

A. c(0) to c(N) :- Refers to the Compromising Nodes i.e. Neighbor Nodes

1. For node(i)=source to destination
2. If node(i)=center node
   Then identify the load on center node
3. Find list of neighbours node from c(0) to c(N).
4. If load(center node)<c(i)
   Then load(center node)++;
   else
   load(c(i))++;
5. Exit.

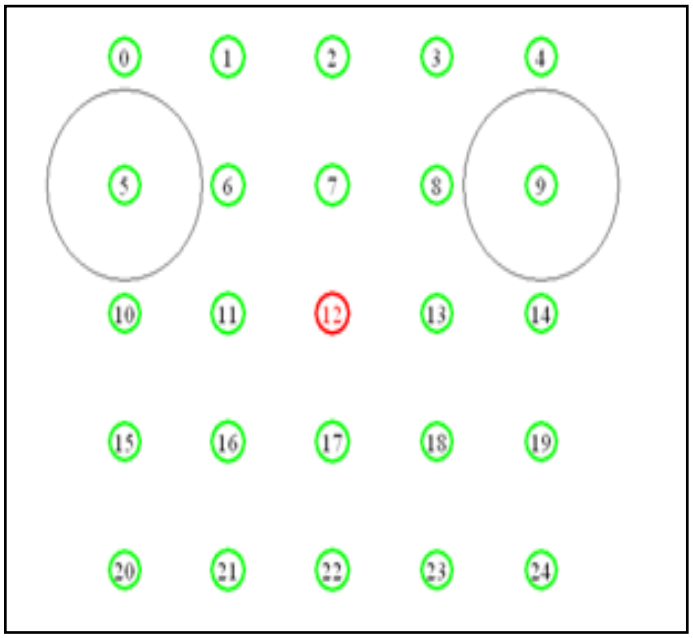

Fig. 2: Implementation of Energy Efficient & Secure Wireless Sensor Networks

IV. Conclusion

We analyzed Horizontal–Vertical method that performs better load balancing of the grid network, all communication mode in a grid network. We will first identify the center node for the exceeding load limit and then release this node from the communication path. Now its load gets distributed on the surrounding other nodes. This distribution will be taken on basis of average distance from the center. After this central node is now not overloaded. Holes would also minimize in this approach. Energy consumption on central node will be minimum so that the network can be used more efficiently.For security if any node is overloaded then its packets will distributed on neighbouring nodes for avoiding packet loss by overloaded node.

V. Future Work

In this proposed work we defined the whole concept respective to a specific topological representation i.e. Grid network. We can enhance our work by using different topological areas. We can also extend it to different kind of network like manet, wimax etc.

References

[1] W. Su Y. Sankarasubramaniam E. Cayirci Akyildiz, I.F. "A survey on sensor- networks", IEEE Communications Magazine, pp. 102-114, 2002.

[2] Kumar.S.P. Chee-Yee Chong,"Sensor networks: Evolution, opportunities, and challenges", Proc IEEE, August 2003.

[3] Ismail H. Kasimoglui Ian .F. Akyildiz,"Wireless sensor and actor: research challenges", (Elsevier) Journal, 2(38), pp. 351-367, 2004.
[4] Sundeep Karthikeyan Vaidynathan, Sayantan sur, Sinha, Data aggregation techniques in sensor networks", Technical Report, OSU-CISRC-11/04-TR60, 2004.
[5] D. Agrawal N. Shrivastava, C. Buragohain, S. Suri. Medians and beyond: new aggregation techniques for sensor networks", Proceedings of the 2nd inter-national conference on Embedded networked sensor systems, pp. 239-249, 2004. ACM Press.
[6] Xiuli Ren, Haibin Yu.,"Security mechanisms for wireless sensor networks", IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No. 3, pp. 100-107, March 2006.
[7] S. Setia S. Zhu, S. Jajodia,"Leap: e±cient security mechanisms for large scale distributed sensor networks", Proceedings of the 10th ACM conference on Computer and communications security, pp. 62-72, 2003. ACM Press.
[8] J. Stankovic A. Perrig, D. Wagner,"Security in wireless sensor networks".
[9] P.Nair H.Cam, S.Ozdemir, D. Muthuavinashiappan, "Espda: Energy- efficient and secure pattern based data aggregation for wireless sensor networks", Computer Communications IEEE Sensors, 29, 446-455, 2006.
[10] L. Eschenauera, V. Gligor,"A key-managemensct hemef or distributed sensor networks", In Proceedings of the ACM Conference on Computer and Communication Security (CCS), Nov. 2002.
[11] H. Chan, A. Perrig, D. Song,"Randomk ey predistribution schemes for sensor networks", In Proceedings of IEEE Symposium on Security and Privacy, May 2003.
[12] F. Bouhafs, M. Merabti, H. Mokhtar,"A Semantic Clustering Routing Protocol for Wireless Sensor Networks", Proceedings of the 3rd IEEE Consumer Communications and Networking Conference, 2006, pp. 351-355.
[13] I.K. Ibrahim, R. Kronsteiner, G. Kotsis,"A Semantic Solution for Data Integration in Mixed Sensor Networks", Computer Communications, 28(13), Elsevier, 2005, pp. 1564-1574.
[14] E. Fasolo,"In-network Aggregation Techniques for Wireless Sensor Networks: A survey", IEEE Wireless Communications, 14(2), 2007, pp. 70-87.
[15] Krishnamachari, B.; Estrin, D.; Wicker, S. Modeling, "Data-Centric Routing in Wireless Sensor Networks", USC Computer Engineering Technical Report CENG 02-14, 2002.
[16] Yen, H.H.; Lin, F.Y.S.; Lin, S.P.,"Energy-Efficient Data-Centric Routing in Wireless Sensor Networks", IEICE Trans. Commun. 2005, E88-B, 4470-4480.
[17] C. F. Li, M. Ye, G. Chen, J. Wu,"An Energy-Efficient Unequal Clustering Mechanism for Wireless Sensor Networks", IEEE International Conf. Mobile Adhoc and Sensor Systems, pp. 8, Nov. 2005.
[18] S. Marti, T. J. Giuli, K. Lai, M. Baker,"Mitigating routing misbehavior in mobile Ad-Hoc networks", in Sixth annual ACM/IEEE Internation Conference on Mobile Computing and Networking, 2000, pp. 255–265.
[19] S. Buchegger, J.-Y. L. Boudec,"Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks", in Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing. Canary Islands, Spain: IEEE Computer Society, January 2002, pp. 403–410.
[20] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, "SPINS: Security protocols for sensor networks", in Proceedings of Mobile Networking and Computing 2001.