

Secured And Performance Driven Mechanism For Mobile Data Gathering In Wireless Sensor Networks

Maibam Debina Devi¹, Dr. Kalaikumaran.T², Dr. Karthik .S³

PG Scholar, Department of CSE, SNS College of Technology, Coimbatore-351.

Professor and Head, Department of CSE, SNS College of Technology, Coimbatore-352.

Professor and Dean, Department of CSE, SNS College of Technology, Coimbatore-353.

email id: api.maibam@gmail.com

ABSTRACT

Wireless sensor network consist of data acquisition network and data distribution network, monitored and controlled by a management center known as base station. The objective of energy efficient routing protocol in wireless sensor network is to increase the operational lifetime of the networks. Routing protocols enhance the lifetime of the wireless sensor networks by distributing traffic among optimal path. Transmission of secured data is also an important research concern in the wireless sensor networks. A new data-gathering mechanism for large-scale wireless sensor networks by introducing mobility into the network. A mobile data collector, for convenience called an M-collector in this work, could be a mobile robot or a vehicle equipped with a powerful transceiver and battery, working like a mobile base station and gathering data while moving through the field. We propose a secure routing protocol for wireless sensor networks. Here, the data packets are transmitted in a secure manner by using the digital signature crypto system. It is compared with existing tour planning protocol. We also extend our work to cover the uncovered node using relay node. It shows better results in terms of packet delivery fraction, energy consumption, and end-to-end delay compared to the existing protocol.

Index Terms- Data-gathering mechanism, M-Collector, Routing protocol, Security, Wireless sensor networks.

1 INTRODUCTION

Wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Wireless Sensor Networks (WSN) provides different methods for sensing and disseminating information from various environments which provide the potential to serve many different applications. Each sensor has a wireless communication capability and some level of intelligence for signal processing and networking of the data. It provides a capable network infrastructure for many applications like environmental monitoring, medical care, military surveillance etc. WSN deployed the sensor node in

designated area. One of the major problem in wireless networks is the security. Often attacks happen in sensor network while communicating. Hence securing each node in the network becomes a major issue. Many types of attacks are present which makes short term unavailability of the networks, but a great deal of research has been done and under process to enhance the survivability. But these schemes cannot address the attacks that affect long term availability of the networks.

Wireless sensor networks have emerged with wide range of applications for new information-gathering paradigm, such as medical treatment, outer-space exploration, battlefield surveillance, emergency response, etc. Sensor nodes must be able to discover nearby nodes and organize themselves into a network before monitoring the environment. Most of the energy of a sensor is consumed on two major tasks: sensing the field and uploading data to the data sink. Energy consumption on sensing is relatively stable because it does not depend on the network topology or the location of sensors and it only depends on the sampling rate. On the other hand, the lifetime of the network is determined by data-gathering scheme.

As a result, after these if the sensors fail, other sensor nodes cannot reach the data collector and the network will be disconnected, although most of the nodes can still survive for a long period. Single data-centric is inefficient to use for a large-scale sensor network, and it result to inefficiency to use a single static data sink to gather data from all sensors. In some applications, sensors are deployed to monitor separate areas. In each area, sensors are densely deployed and connected, whereas sensors that belong to different areas may be disconnected. Unlike fully connected networks, some sensors cannot forward data to the data sink via wireless links. A mobile data collector is perfectly suitable for such applications. Sensing data are uploaded once in a while and it is collected at a low rate and are not so delay sensitive that it can be accumulated into fixed-length data packets. In order to provide a scalable data-gathering scheme for large-scale static sensor networks, to gather data from sensors we utilize

not on the tour is within some predetermined distance $dist$ of a city that is on the tour. If the transmission range of each sensor could be modelled as a disk-shaped area, the SHDGP can be simplified to the CSP by setting $dist$ in the CSP equal to the transmission range of sensors. We have managed to run the optimal algorithm for a few small networks to compare with our greedy algorithm. our greedy algorithm performs much better than the covering line algorithm in various scenarios and is close to the optimal algorithm in small networks.

The basic idea behind the greedy algorithm is to choose a subset of points from the candidate polling point set, each of which corresponds to a neighbour set of sensors. At each stage of the algorithm, a neighbour set of sensors can be covered when its corresponding candidate polling point is chosen as a polling point in the data-gathering tour. The algorithm will terminate after all sensors are covered. The algorithm tries to cover each uncovered neighbour set of sensors with the minimum average cost at each stage, where the "cost" will be formally defined later.

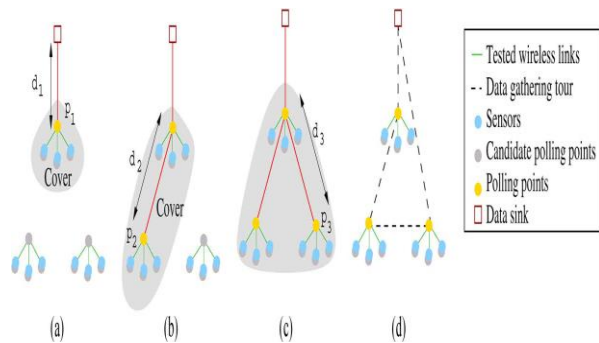


Fig 2: Spanning tree covering algorithm. (a) Neighbour set of p_1 is covered with the average cost $d_1/3$. (b) Neighbour set of p_1 is covered with the average cost $d_2/3$. (c) neighbour set of p_1 is covered with the average cost $d_3/3$. (d) Data-gathering tour obtained by the spanning tree covering algorithm.

3.4 Data Gathering with Multiple M-Collectors

In this data-gathering scheme with multiple M-collectors, only one M-collector needs to visit the transmission range of the data sink. As shown in Fig 3 (b)-(d), the entire network can be divided into sub networks. In each sub network, an M-collector is responsible for gathering data from local sensors in the subarea. Once in a while, the M-collector forwards the sensing data to one of the other nearby M-collectors, when two M-collectors move close enough. Finally, data can be forwarded to the M-collector that will visit the data sink via relays of other M-collectors.

In Fig 3 (d), all data are forwarded to M-collector 1 from other M-collectors, and then, M-collector 1 carries and uploads data to the data sink. There are some interesting issues here, such as how to relay the packets to the data sink energy efficiently, how to schedule the movement of M-collectors to reduce the packet delay, and so on. Here, we will focus on how to plan the subtours of multiple M-collectors to minimize the number of M-collectors.

3.5 Discovering the Uncovered Node-Making Link With Covered Node

The positions of sensors are either the polling points in the data-gathering tour or within the one hop range of the polling points. For the sake of simplicity, we assume that M-collectors move at a fixed speed and ignore the time for making turns and data transmission, such that we can roughly estimate the time of a data-gathering tour by the tour length

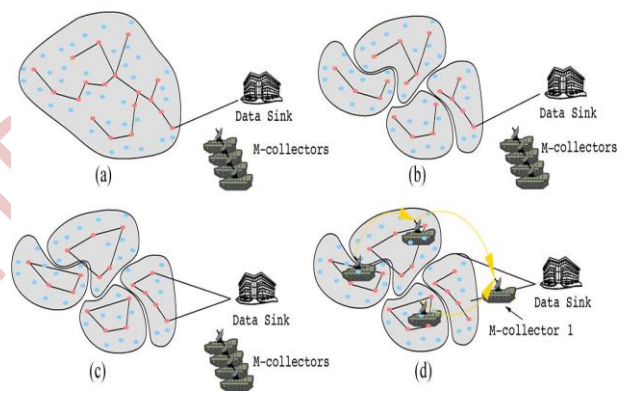


Fig 3: Data gathering with multiple M-collectors.

But the major disadvantages of the existing polling point position based system for gathering the data based M-collector it misses some nodes information in the sensor network, to find the missing node/uncovered node information we use the relay node it contains information about the covered node in the polling point based on this we collect uncovered node information with covered node information in the relay node.

3.6 Security to Mobile Collector Node

Public key cryptography provides authentication and confidentiality. The high processing overhead and energy cost make the implementation of public key cryptography in WSNs impractical. Few researchers proposed mechanisms to reduce processing and energy cost in Elliptic curve cryptography ECC. Each sensor node has a fixed transmission range R . Multiple paths are available between the sensors and sink node in the network. The M-

collector selects the polling points between the sensors to route the sensed data to the sink node. Every node has a unique private key and a public key. Common hash function is used by all nodes in the network. To generate the digital signature, MD5 hash function is used. The private and public keys are generated using the RSA algorithm. It is a widely used public key crypto system. It may be used to provide both secrecy and digital signatures.

A polling points on reception of (dsign, M) and the path in the data packet, verifies the digital signature by comparing decrypted value of de sign mod n with message digest H(M). The de sign mod n is key (e, n) using the formula, decrypted using sender's public

$$\begin{aligned} \text{De signmod } n &= ((H(M))d \text{ mod } n) \text{ e mod } n \\ &= (H(M))e \text{ mod } n \quad (1) \end{aligned}$$

By applying Little Fermat's and Chinese Remainder Theorem to Equation (1), it can be shown that designmod n = H(M)

If the generated H(M) by the receiver and the decrypted H(M) of digital signature dsign is equal, then the receiver accepts the data; otherwise rejects the data and informs the sender that the data is altered through by generating route error packet. This process is repeated in every hop of the node between sensors. The proposed public key crypto system provides authentication, integrity and non-repudiation in the wireless sensor network.

3.7 Performance Evaluation

In the simulations, we assume that a bunch of sensor nodes is uniformly deployed in the sensing field. For covering the uncovered node using relay node for M-collector in both small and large networks, compare the relative network lifetime and security of the proposed with the data-gathering schemes, and illustrate the data-gathering algorithm with multiple M-collectors in a randomly generated network.

4 CONCLUSION

A mobile data-gathering scheme for large-scale sensor networks is generated. The mobile data collector, called an M-collector, which works like a mobile base station in the network. An M-collector starts the data gathering tour periodically from the static data sink, traverses the entire sensor network, polls sensors and gathers the data from sensors one by one, and finally returns and uploads data to the data sink. Our mobile data-gathering scheme improves the scalability and solves intrinsic problems of large-scale homogeneous networks. By introducing the M-collector, data gathering becomes more flexible and adaptable to the unexpected changes of the network topology. In addition to the uncovered sensor form the polling points are identified by relay node and covered and link the uncovered node to the M-collector. We extend our proposed to provide the security to the mobile collector

using digital signature, which is generated by using the MD5 hash function and RSA algorithm. The security ensures the correctness of data, nonrepudiation and authentication.

5 REFERENCES

- [1] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proc. ACM Int. Workshop Wireless Sens. Netw. Appl.*, Atlanta, GA, Sep. 2002, pp. 88–97.
- [2] S. Chessa and P. Santi, "Crash faults identification in wireless sensor networks," *Comput. Commun.*, vol. 25, no. 14, pp. 1273–1282, Sep. 2002.
- [3] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet," in *Proc. ASPLOS*, 2002, pp. 96–107.
- [4] T. Small and Z. Haas, "The shared wireless infostation model—A new adhoc networking paradigm (or where there is a whale, there is a way)," in *Proc. ACM MobiHoc*, 2003, pp. 233–244.
- [5] I. Vasilescu, K. Kotay, D. Rus, M. Dunbabin, and P. Corke, "Data collection, storage and retrieval with an underwater sensor network," in *Proc. ACM SenSys*, 2005, pp. 154–165.
- [6] A. Chakrabarty, A. Sabharwal, and B. Aazhang, "Using predictable observer mobility for power efficient design of a sensor network," in *Proc. 2nd Int. Workshop IPSN*, Apr. 2003, pp. 129–145.
- [7] B. Hull, V. Bychkovskiy, K. Chen, M. Goraczko, E. Shih, Y. Zhang, H. Balakrishnan, and S. Madden, "CarTel: A distributed mobile sensor computing system," in *Proc. ACM SenSys*, 2006, pp. 125–138.
- [8] A. Pentland, R. Fletcher, and A. Hasson, "Daknet: Rethinking connectivity in developing nations," *Computer*, vol. 37, no. 1, pp. 78–83, Jan. 2004.
- [9] D. Jea, A. A. Somasundara, and M. B. Srivastava, "Multiple controlled mobile elements (data mules) for data collection in sensor networks," in *Proc. IEEE/ACM Int. Conf. DCOSS*, Jun. 2005, pp. 244–257.
- [10] R. C. Shah, S. Roy, S. Jain, and W. Brunette, "Data MULEs: Modeling a three-tier architecture for sparse sensor networks," in *Proc. IEEE Workshop Sens. Netw. Protocols Appl.*, 2003, pp. 30–41.
- [11] S. Jain, R. C. Shah, W. Brunette, G. Borriello, and S. Roy, *Exploiting mobility for energy efficient data collection in wireless sensor networks*. Norwell, MA: Kluwer, 2005.
- [12] W. Zhao, M. Ammar, and E. Zegura, "A message ferrying approach for data delivery in sparse mobile

- ad hoc networks," in Proc. ACM MobiHoc, 2004, pp. 187-198.
- [13] J. Luo and J.-P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks," in Proc. IEEE INFOCOM, 2005, pp. 1735-1746.
- [14] A. A. Somasundara, A. Ramamoorthy, and M. B. Srivastava, "Mobile element scheduling for efficient data collection in wireless sensor networks with dynamic deadlines," in Proc. IEEE RTSS, Dec. 2004, pp. 296-305. MA et al.: TOUR PLANNING FOR MOBILE DATA-GATHERING MECHANISMS IN WSNs 1483.
- [15] G. Xing, T. Wang, W. Jia, and M. Li, "Rendezvous design algorithm for wireless sensor networks with a mobile base station," in Proc. ACM Mobihoc, May 2008, pp. 231-240.
- [16] C. Konstantopoulos, G. Pantziou, D. Gavalas, A. Mpitziopoulos, and B. Mamalis, "A rendezvous-based approach enabling energy-efficient sensory data collection with mobile sinks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 5, pp. 809-817, May 2012.
- [17] M. Zhao and Y. Yang, "Bounded relay hop mobile data gathering in wireless sensor networks," IEEE Trans. Comput., vol. 61, no. 2, pp. 265-277, Feb. 2012.
- [18] W. Liang, P. Schweitzer, and Z. Xu, "Approximation algorithms for capacitated minimum forest problems in wireless sensor networks with a mobile sink," IEEE Trans. Comput., to be published.
- [19] P. Skraba, H. Aghajan, and A. Bahai, "RFID wakeup in event driven sensor networks," in SigComm Poster Session, Portland, OR, Aug. 2004. [Online]. Available: <http://conferences.sigcomm.org/sigcomm/2004/posters/skraba.pdf>.
- [20] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy efficient communication protocols for wireless microsensor networks," in Proc. HICSS, Maui, HI, Jan. 2000, pp. 1-10.
- [21] O. Younis and S. Fahmy, "Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach," in Proc. IEEE INFOCOM, Hong Kong, China, 2004, pp. 629-640.
- [22] A. D. Amis, R. Prakash, T. H. P. Vuong, and D. T. Huynh, "Max-min Dcluster formation in wireless ad hoc networks," in Proc. IEEE INFOCOM, Tel-Aviv, Israel, 2000, pp. 32-41.
- [23] X. Liu, J. Cao, S. Lai, C. Yang, H. Wu, and Y. Xu, "Energy efficient clustering for WSN-based structural health monitoring," in Proc. IEEE INFOCOM, Apr. 2011, pp. 2768-2776.
- [24] M. Ma and Y. Yang, "Data gathering in wireless sensor networks with mobile collectors," in Proc. 22nd IEEE Intern. Parallel Distrib. Symp., Miami, FL, Apr. 2008, pp. 1-9.
- [25] Z. Zhang, M. Ma, and Y. Yang, "Energy efficient multi-hop polling in clusters of two-layered heterogeneous sensor networks," IEEE Trans. Comput., vol. 57, no. 2, pp. 231-245, Feb. 2008.
- [26] A. Arora, R. Ramnath, E. Ertin, P. Sinha, S. Bapat, V. Naik, V. Kulathumani, H. Zhang, H. Cao, M. Sridharan, S. Kumar, N. Seddon, C. Anderson, T. Herman, N.

Trivedi, M. Nesterenko, R. Shah, S. Kulkarni, M. Aramugam, L. Wang, M. Gouda, Y. Choi, D. Culler, P. Dutta, C. Sharp, G. Tolle, M. Grimmer, B. Ferriera, and K. Parker, "ExScal: Elements of an extreme scale wireless sensor network," in Proc. 11th IEEE Int. Conf. RTCSA, 2005, pp. 102-108.



Maibam Debina Devi received Bachelor degree in Computer Science and Engineering from KK Wagh College of Engineering, Nashik, India. Currently, pursuing M.E degree in Computer Science and Engineering from SNS College of Technology, Anna University, Chennai. Her area of interest are wireless sensor networks, grid

computing.



Professor Dr. T. Kalaikumar, is presently Professor & Head in the Department of Computer Science & Engineering, SNS college of Technology (An Autonomous Institution), Coimbatore. He received M.E degree from the Anna University, Chennai and Ph.D degree from Anna University, Chennai. His area of interest

includes data mining and specifically, he is into detecting hotspots in crime.



Professor Dr. S. Karthik is presently Professor & Dean in the Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University Coimbatore, Tamilnadu, India. He received the M.E degree from the Anna University Chennai and Ph.D degree from Anna University of

Technology, Coimbatore. His research interests include network security, web services and wireless systems. In particular, he is currently working in a research group developing new Internet security architectures and active defense systems against DDoS attacks. Dr. S. Karthik published more than 35 papers in refereed international journals and 25 papers in conferences and has been involved many international conferences as Technical Chair and tutorial presenter. He is an active member of IEEE, ISTE, IAENG, IACSIT and Indian Computer Society.