ISSN:0975-9646

Achieving Energy Conservation in Wireless Sensor Networks by using WB (Witness-Based) Approach

S.Anandamurugan*, C.Venkatesh**

* CSE, Kongu Engineering College, Erode, Tamil Nadu, India
** Faculty of Engineering, EBET Group of Institutions, Erode, Tamil Nadu, India

Abstract—In this paper, Wireless sensor networks place sensors into an area to get data and send them back to a base station. Data fusion, in which collected data are fused before they are sent to the base station, is usually implemented over the network. Since a sensor is typically placed in locations that are accessible to malicious attackers, information assurance of the data fusion process is very important. A WB (Witness-Based) approach [9] has been proposed to verify the fusion data. In this approach, the base station receives the fusion data and "votes" on the data from a randomly chosen sensor node. The vote comes from other sensor nodes, called "witnesses," to confirm the correctness of the fusion data. Since the base station receives the vote through the chosen node, this node could forge the vote if it is compromised. Accordingly, the witness node must apply cryptographic operations to the vote to prevent this forgery. The cryptographic operation requires more bits than the vote, increasing the transmission burden from the chosen node to the base station. The chosen node consumes large power. This work improves the WB approach using a direct voting mechanism such that the proposed scheme performs better in terms of assurance, overhead, and delay. The witness node transmits the vote directly to the base station. Forgery does not pose a problem in this scheme. Moreover, fewer bits are necessary to represent the vote, significantly reducing the power consumption.

Key Words— Wireless sensor networks, data fusion, Energy conservation, voting mechanism, witness.

1 INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control.

The applications for WSNs are many and varied, but typically involve some kind of monitoring, tracking, and controlling. Specific applications for WSNs include habitat monitoring, object tracking, nuclear reactor control, fire detection, and traffic monitoring. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. A number of WSN deployments have been done in the past in the context of environmental monitoring. A sensor node, also known as a 'mote', is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network.

The main components of a sensor node are microcontroller, transceiver, external memory, power source and one or more sensors. Microcontroller performs tasks, processes data and controls the functionality of other components in the sensor node. Other alternatives that can be used as a controller are: General purpose desktop, Microprocessor, Digital signal processors, Field Programmable Gate Array and Application-specific integrated circuit. Microcontrollers are most suitable choice for sensor node. Each of the four choices has their own advantages and disadvantages. Microcontrollers are the best choices for embedded systems.

In general purpose microprocessor the power consumption is more than the microcontroller, therefore it is not a suitable choice for sensor node From an energy perspective, the most relevant kinds of memory are on-chip memory of a microcontroller and FLASH memory off-chip RAM is rarely if ever used. Flash memories are used due to its cost and storage capacity. Memory requirements are very much application dependent. Two categories of memory based on the purpose of storage a) User memory used for storing application related or personal data. b) Program memory used for programming the device. This memory also contains identification data of the device if any. Power consumption in the sensor node is for the Sensing, Communication and Data Processing. More energy is required for data communication in sensors.

Energy expenditure is less for sensing and data processing. The energy cost of transmitting 1 Kb a distance of 100 m is approximately the same as that for the executing 3 million instructions by 100 million instructions per second/W processor. Power is stored either in Batteries or Capacitors. Batteries are the main source of power supply for sensor nodes. Namely two types of batteries used are chargeable and non-rechargeable. They are also classified according to electrochemical is thematerial used for electrode such as NiCd (nickel-cadmium), NiZn (nickel-zinc), Nimh (nickel metal hydride), and Lithium-Ion. Current sensors are developed which are able to renew their energy from solar, thermo generator, or vibration energy.

The witness-based approach that was presented by Du et al. [9] does not have this difficulty. Several fusion nodes are used to fuse the collected data and they can communicate with the base station. Only one node is chosen to transmit the fusion result to the base station. The other fusion nodes, serving as witnesses, hash the fusion results to message authentication codes (MACs). The MACs are then sent to the base station through the chosen fusion node. Finally, the base station utilizes the received MACs to verify the received fusion data. The verification may be wrong since the chosen node may be compromised and forge MACs. The correctness of the verification depends not only on the number of malicious fusion nodes but also on the length of the MAC. A long MAC increases the reliability of the verification. However, the transmission of a long MAC imposes a large communication burden. If the received fusion result at the base station cannot pass the verification, then a polling scheme is started to determine whether any valid fusion result is available at the other fusion nodes. In addition to the fusion result that had been sent by the malicious fusion node, several copies of the correct fusion result may also have to be transmitted to the base station. The transmission of the correct fusion result consumes the power of the uncompromised fusion node.

Even though the witness-based approach developed in [9] is more attractive than previous approaches, it suffers from several drawbacks. First, several copies of the fusion result may be sent to the base station by uncompromised nodes, increasing the power consumed at these nodes. Second, a MAC mechanism must be implemented in each sensor node that occupies limited memory resources at each sensor. The MAC mechanism is designed solely for fusion data assurance; cryptographic operations are not otherwise needed for applications in which the fusion result need not be kept secret. Third, the voting information in the current polling round is not used in the next polling round if the verification has not been passed in the current polling round. All votes are collected in each polling round. If the voting can be used in any way, then the polling process should be shortened to save power and reduce the time delay. Finally, since all votes are collected by one node and sent to the base station, this node can forge the fusion result and the votes. Such forgery must be prevented to increase security in the data fusion system.

This work develops a novel data fusion assurance mechanism to eliminate all of the aforementioned shortcomings in the witness-based method by Du et al. [9]. The correctness of the verification in the proposed scheme depends only on the number of compromised fusion nodes. As in the witness-based approach, a fusion node is selected to transmit the fusion result, while other fusion nodes serve as witnesses. Nevertheless, the base station obtains votes that contribute to the transmitted fusion result directly from the witness nodes. No valid fusion data are available if the transmitted fusion data are not approved by a preset number of witness nodes. Based on this voting mechanism, two schemes are described: One needs variant rounds of voting and the other requires only one round of voting. The key advantages of the variant-round (VR) scheme over that presented in [9] are summarized as follows:

Only one copy of the correct (valid) fusion result, provided by one of uncompromised fusion nodes, is transmitted to the base station, regardless of whether the system is comprised of sufficient uncompromised nodes to support the fusion result. This single transmission saves the power of the uncompromised node. However, in the scheme in [9], when too few witness nodes are available to verify the correct fusion result, the polling continues until not enough votes to pass the verification can be collected to verify the fusion result. During the polling process, more than one uncompromised node may send the correct fusion result to the base station.

- The direct voting scheme is adopted and no MAC mechanism needs to be implemented at each node; therefore, no extra memory is needed to implement such a mechanism. Moreover, no communication is necessary between the sensors in this voting scheme. In contrast, the MAC message of each witness node must be collected at the fusion node in the scheme that is presented in [9].
- Early termination is achievable when the base station receives enough "agree" or "disagree" votes. In contrast, the scheme in [9] always collects all votes.
- A witness node may remain silent (without transmis sion) when it agrees with the transmitted fusion result. Only "disagree" votes need to be sent. This "silent assent" feature drastically reduces the transmission power consumption in the system. However, in [9], MACs are always sent and they cannot be too short to jeopardize verification of the fusion result.
- A compromised fusion node can be identified if it has been excluded by the base station during the polling process. This "traitor exclusion" is useful for further verification of the fusion result. Even though the scheme in [9] also offers this "traitor exclusion" feature, it fails to exploit it when the fusion node can successfully forge the fusion result.
- No forged result can be accepted by the base station unless the number of compromised nodes reaches the number of support votes that is required to verify the fusion result and these nodes collude to forge the fusion result. In contrast, for the scheme in [9], the node that sends the fusion result and all votes may still successfully forge the fusion result, even when it is the only node to be compromised.
- Analytical and simulation results reveal that the proposed scheme has an up-to-40 times lower overhead than the scheme by Du et al. [9].

The rest of the paper is organized as follows. Section 2 summarizes related work. Section 3 investigates the performance Section 4 gives the simulation results on finite random networks. Finally, Section 5 concludes the paper.

2. RELATED WORK

The related works are as follows. In a WSN, the sensors collect the data. The fusion nodes fuse these data and one of the fusion nodes send this fused data to the base station. This fusion node may be attacked by malicious attackers. If a fusion node is compromised, then the base station cannot ensure the correctness of the fusion data that have been sent to it. The witness based approach does not have this difficulty as it uses MAC mechanism to verify the result.

Drawbacks of Existing Systems are several copies of the fusion result may be sent to the base station by uncompromised nodes. It increases the power consumed at these nodes. A MAC mechanism must be implemented in each sensor node. In [5], the voting information in the current polling round is not used in the next polling round. Even though the witness-based approach developed is more attractive than previous approaches, it suffers from several drawbacks. In [2], several copies of the fusion result may be sent to the base station by uncompromised nodes, increasing the power consumed at these nodes. In [1], a MAC mechanism must be implemented in each sensor node that occupies limited memory resources at each sensor. The MAC mechanism is designed solely for fusion data assurance. Cryptographic operations are not otherwise needed for applications in which the fusion result need not be kept secret.

In [3], the voting information in the current polling round is not used in the next polling round if the verification has not been passed in the current polling round. All votes are collected in each polling round. If the voting can be used in any way, then the polling process should be shortened to save power and reduce the time delay. In [4], since all votes are collected by one node and sent to the base station, this node can forge the fusion result and the votes. Such forgery must be prevented to increase security in the data fusion system.
One round voting mechanism is proposed to overcome the disadvantages of the existing system. Advantages of Proposed Systems are i) Only one copy of the correct fusion result is sent to the base station ii) MAC mechanism need not be implemented at each node iii) Silent Assent Mechanism. iv) The power and delay associated with the transmission of the fusion result are significantly reduced.

3. VOTING MECHANISM

The various modules in the proposed schemes are as follows: Data Fusion, Witness Based Data Fusion Verifier, One Round Voting – Base Station Transmission, Voting acknowledgement of Random Selected Node, and Performance Metrics

Data Fusion

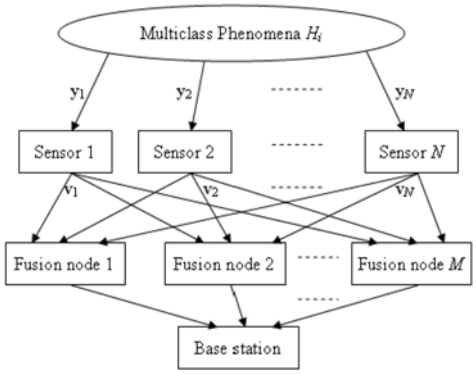

Fig1: Structure of WSN

Fig. 1 depicts a WSN for distributed detection with N sensors for collecting environment variation data and a fusion center to make a final decision concerning detections. This network architecture is similar to the architecture of the so-called SENsor with Mobile Access (SENMA). Since the distance between the fusion node and the base station is usually long, the power consumed by the fusion node upon receiving data is much lower than the power associated with transmission.

If the detection (raw) data are transmitted to the fusion nodes without any processing, then the transmission imposes a very high communication burden. Hence, each sensor must make a local decision based on the raw data before transmission. The sensor then transmits the local decision to M fusion nodes by broadcasting. The fusion node combines all the local decisions to yield a final result and it communicates directly with the base station. Finally, one of the fusion nodes is specified to send the final result to the base station. Unless all of the fusion nodes or all of the sensors fail, this detection and fusion scheme guarantees that the base station will receive the detection result. However, the accuracy of the result is uncertain.

Two problems must be solved to ensure that the base station obtains the correct fusion result. i)Every fusion node must correctly fuse all the local decisions such that all of the fusion results must be identical. ii)The second problem concerns the assurance of the fusion result.

Data Fusion Assurance

Although fusion markedly lowers the traffic between the fusion node and the base station, the fusion node is more critical and vulnerable to malicious attacks than the non fusion sensors. If a fusion node is compromised, then the base station cannot ensure the correctness of the fusion data that have been sent to it. This problem of fusion data assurance arises because the detection results are not sent directly to the base station.

WB(Witness Based) Approach

In this witness based approach several fusion nodes are used to fuse the collected data and they can communicate with the base station. Only one node is chosen to transmit the fusion result to the base station. The other fusion nodes, serving as witnesses, hash the fusion results to message authentication codes (MACs). The MACs are then sent to the base station through the chosen fusion node. Finally, the base station utilizes the received MACs to verify the received fusion data. The verification may be wrong since the chosen node may be compromised and forge MACs. The correctness of the verification depends not only on the number of malicious fusion nodes but also on the length of the MAC. A long MAC increases the reliability of the verification. However, the transmission of a long MAC imposes a large communication burden. If the received fusion result at the base station cannot pass the verification, then a polling scheme is started to determine whether any valid fusion result is available at the other fusion nodes. In addition to the fusion result that had been sent by the malicious fusion node, several copies of the correct fusion result may also have to be transmitted to the base station. The transmission of the correct fusion result consumes the power of the uncompromised fusion node.

The base station determines from the received data that the fusion result from the chosen node is accurate. In the T + 1 out of M voting scheme, the fusion result of the chosen node needs support from at least T witness nodes, where M is the number of fusion nodes and T is a threshold. That is, the base station accepts the fusion result if the fusion result is supported by atleast T MACs. Normally, T > M/2. However, even when the number of compromised nodes C is less than T, the fusion result accepted by the base station is not always correct. If the chosen node is compromised, then it may forge the fusion result and the MACs. Although only one copy of the fusion result is sent to the base station by each chosen node in this witness-based approach, the witness nodes still require significant communication bandwidth because the MACs of the fusion results are transmitted. If the received fusion result at the base station cannot pass the verification, then a polling scheme is started to determine whether any valid fusion result is available at the other fusion nodes. In addition to the fusion result sent by the malicious fusion node, several copies of the correct fusion result may also have to be transmitted to the base station.

Improved Voting Mechanism

The voting mechanism in the witness-based approach is designed according to the MAC of the fusion result at each witness node. This design is reasonable when the witness node does not know the fusion result at the chosen node. However, in practice, the base station can transmit the fusion result of the chosen node to the witness node. Therefore, the witness node can obtain the transmitted fusion result from the chosen node through the base station. The witness node can then compare the transmitted fusion result with its own fusion result. Finally, the witness node can send its vote (agreement or disagreement) on the transmitted result directly to the base station, rather than through the chosen node. When a fusion node sends its fusion result to the base station, other fusion nodes serve as witness nodes. The witness node then starts to vote on the transmitted result. One Round scheme is proposed.

One Round Scheme

In this scheme, the base station may receive different fusion results from the witness nodes. It requires that all received fusion results be stored. This scheme has a fixed delay and is summarized as follows:

Step 1. The base station randomly chooses a fusion node. Other fusion nodes serve as witness nodes. A set of witness nodes that includes all of the witness nodes is defined and the nodes in the set are randomly ordered.

Step 2. The chosen node transmits its fusion result to the base station. The base station sets the fusion result as the best temporary voting result and the number of votes for agreement with the fusion result is set to zero.

Step 3. The base station polls the nodes with the best temporary voting result, which currently has the maximum number of votes, following the order of the witness nodes.

The witness node compares its fusion result with the best temporary voting result. If the witness node agrees with the best temporary voting result, it sends an agreeing vote to the base station. The base station increases the number of agreeing votes for the best temporary voting result by one. If the witness node does not agree with the best temporary voting result, it transmits its fusion result to the base station. If the fusion result has been stored in the base station, then the base station increases the number of agreeing votes for the fusion result by one. If the fusion result has not been stored in the base station, then the base station stores the fusion result and the number of agreeing votes for the fusion result is set to zero.

The base station sets the best temporary voting result to the received fusion result that had received the maximum number of agreeing votes to poll the next witness node. If two or more fusion results receive the maximum number of votes, then the temporarily best voting result is set to the result that had most recently been voted for. The polling stops when any received fusion result receives T votes or when the number of unpolled nodes plus the maximum number of votes for the results recorded at the base station is less than T.

From Step 3, we know that the base station keeps only one best temporary voting result when it is polling a witness node. Therefore, the witness node may be silent when it agrees with the best temporary voting result. This is known as the Silent Assent Mechanism.

The fusion node established a hash tree using collected detection results as leaves. The base station requests one of the results and checks if it is consistent with the tree during the assurance process. The probability of detecting a cheating fusion node can be increased by transmitting

fewer detection results to the base station. However, different assurance algorithms must be developed for various fusion operations. No general assurance approach is provided. Additionally, only one fusion node is assumed. When it is compromised, the base station can no longer receive correct fusion data.

All fusion nodes, other than the chosen node, act as witnesses to the transmitted fusion result. The witness nodes compute MACs on the fusion results with private keys that are shared with the base station and then send the MACs, as "votes," to the chosen node. The chosen node collects all of the MACs from the witness nodes and transmits them with its own fusion result to the base station.

The base station determines from the received data whether the fusion result from the chosen node is accurate. In the out of M voting scheme, the fusion result of the chosen node needs support from at least T witness nodes, where M is the number of fusion nodes and T is a threshold. That is, the base station accepts the fusion result if the fusion result is supported by at least T MACs. However, even when the number of compromised nodes C is less than T, the fusion result accepted by the base station is not always correct. If the chosen node is compromised, then it may forge the fusion result and the MACs. The probability that the base station accepts the forged fusion result where k_w is the size of each MAC. Since the number of the transmitted MACs is M-1, the number of the transmitted bits, excluding the fusion result, is
$(M-1)k_w$.

Although only one copy of the fusion result is sent to the base station by each chosen node in this witness-based approach, the witness nodes still require significant communication bandwidth because the MACs of the fusion results are transmitted. If the received fusion result at the base station cannot pass the verification, then a polling scheme is started to determine whether any valid fusion result is available at the other fusion nodes. In addition to the fusion result sent by the malicious fusion node, several copies of the correct fusion result may also have to be transmitted to the base station.

In a fair comparison between the proposed scheme with the witness-based approach, the overhead is defined as the total number of bits, excluding the bits associated with one copy of the correct fusion result, that are transmitted to the base station by uncompromised nodes during the data assurance process. The power consumed at all compromised nodes is not considered since they are not useful to the WSN. Therefore, the overhead can be regarded as the useful power that is consumed for the data assurance by the sensor. Since the base station is generally powerful and not battery powered, its power consumption is not critical in a WSN. The round delay is defined as the number of rounds that are required to collect all MACs (votes) from the witness nodes; the polling delay is defined as the number of votes (including all "agree" and "disagree" voting).

4. SIMULATION RESULTS

In this section, numerical and computer simulations are conducted to evaluate the performance of the proposed schemes.

We have simulated this experiment using NS-2 simulator. The figure 2 shows the creation of data fusion environment. The figure 3 shows the WB data fusion verification. One round base station transmission was simulated and method shown in figure 4. The voting acknowledgement of random selected node error detected is simulated in figure 5. The figure 6 shows the simulation of voting acknowledge of random selected node no error.. In figure 7, the performance measures between number of nodes and packet overhead was represented. Here we take 50,000 nodes. In this, the packet overhead of the existing is 180, 0000. But the packet overhead of proposed method is only 170, 0000. It shows that 10 % of overhead is eliminated. We have done a simulation between the numbers of nodes versus delay.
The result is presented in the figure 8. Here also improvement in reducing the delay. In this, we consider 50,000 nodes; the delay taken by the existing system was 1.2000. But in the present system the delay are only 0.9500. It represents 20% improvement in reducing the relay. In figure 9, the analysis between the numbers of nodes and the power consumption by the nodes. We take assume that 50,000 MR. Existing system consumes 1.1000 amount of energy. But in the present systems consumes only 0.7000. Here also 10 % improvement in power saving.

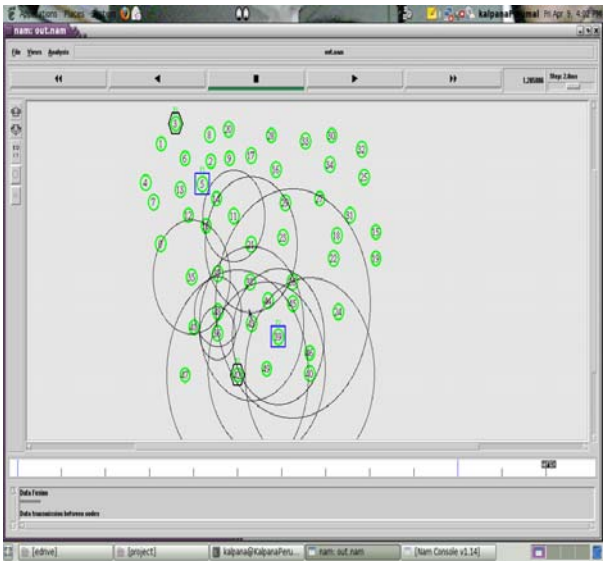

Fig 2: Data fusion

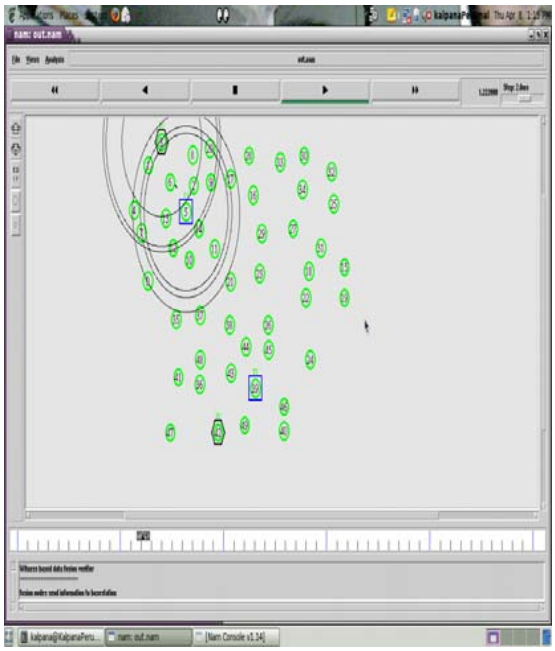

Fig3: WB data fusion verification

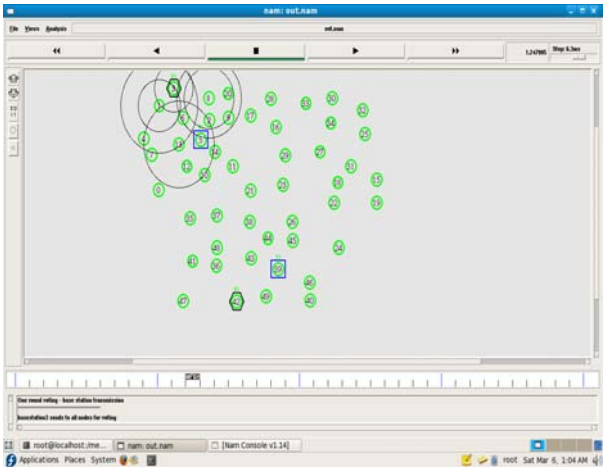

Fig 4 : One round-base station transmission

Fig 5: Voting Acknowledgement of Random Selected Node-error detected

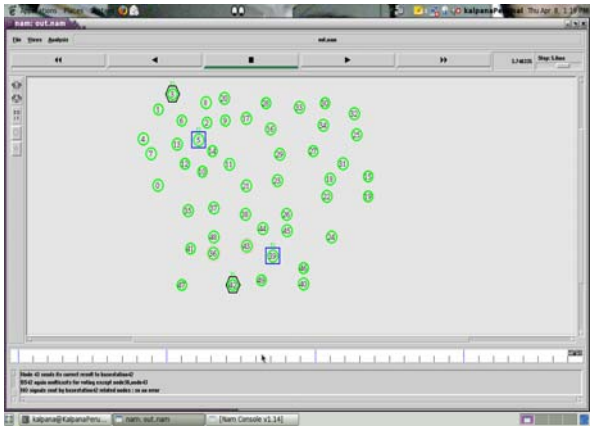

Fig 6: Voting Acknowledgement of Random Selected Node-no error

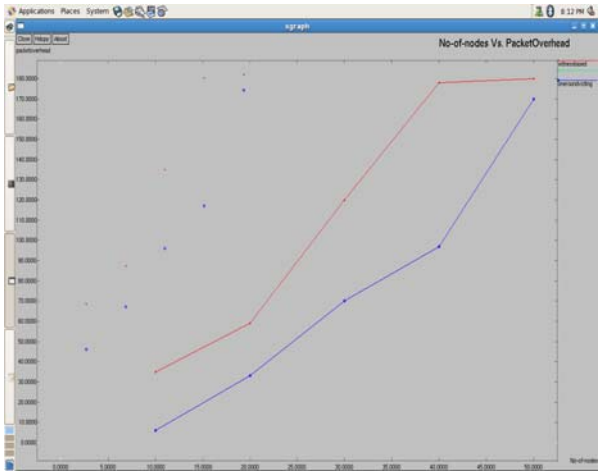

Fig 7: Performance Measure (Number. of Nodes vs Overhead)

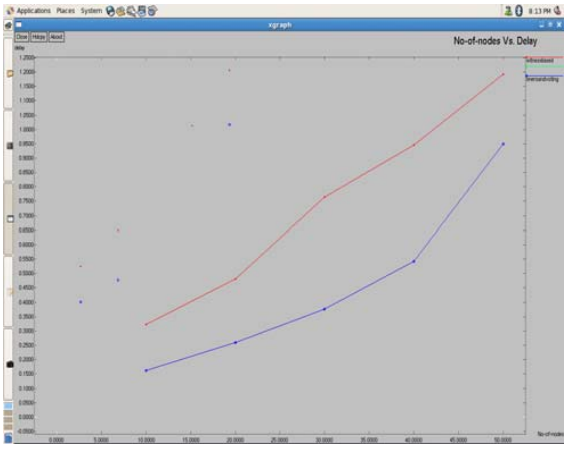

Fig 8: Performance Measure (Number of Nodes vs Delay)

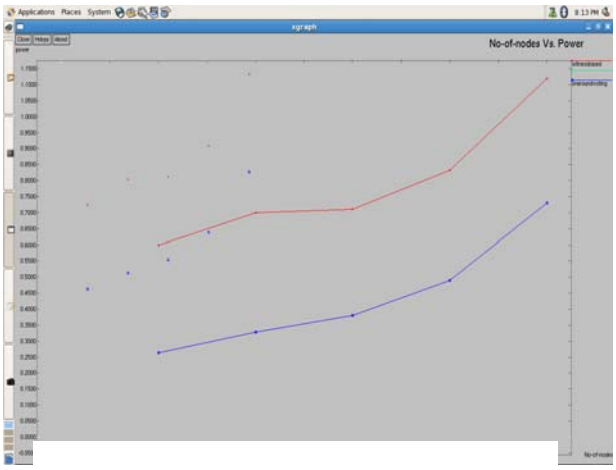

Fig 9: Performance Measure (Number of Nodes vs Power)

5. CONCLUSION

We have investigated the possibility of using a heterogeneous network composed of many simple undynamic nodes and a few mobile nodes. We show that node as a mobile relay, we can get a lifetime improvement of up to 40% over the undynamic network in the ideal case. Another interesting property of this mobile relay approach is that we only need to change the routing algorithm for a relatively small area to use the mobile relay. Furthermore, the mobile relay need not travel all around the network. It never needs to venture farther than two hops from the sink. We see that mobility is actually a great advantage since the mobile relay is more efficient than most static energy-provisioning methods. We also investigate other ways to use mobile nodes, such as mobile sink approach. Although it is clear from our analysis that using a mobile sink is always beneficial in terms of the lifetime of the network, there are certain tradeoffs to make the sink mobile.

In this paper, we make some simplifying assumptions, e.g., the network is running a data-logging application and sensors are incapable of power control. However, in a network which is event based, using mobile relay may be even more beneficial. Since the traffic is not uniformly distributed in such a network, we can move the mobile relay in the directions where traffic is high. In this case we may not need to redirect the traffic as in the data-logging application, so that the overhead caused by mobile relay will be reduced. Our scheme can also work together with power control or data aggregation/compression methods. Although the traffic can be reduced by data compression, the bottleneck described in this paper still exists in such network since the information generated per unit area is still fixed, and our model of uniform packet generation rate can be applied.

REFERENCES

[1] H. Liu, P. Wan, C. Yi, X. Jia, S. Makki, and P. Niki, " Maximal lifetime scheduling in sensor surveillance networks," in *Proc. IEEE INFOCOM*, Mar. 2005, pp. 2482-2491.

[2] R. Shah, S. Roy, S. Jain, and W. Brunette, "Data mules: Modeling a three-tier architecture for sparse sensor networks," in *Proc. IEEE SNPA*, May 2003, pp. 30-41.

3] R. Zheng, J. C. Hou, and L. Sha, "Asynchronous wakeup for ad hoc networks," in *Proc. ACMMobiHoc*, Jun. 2003, pp. 35-45.

[4] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC A protocol for wireless sensor networks," in *Proc. IEEE INFOCOM*, Jun.2002, pp. 1567-1576.

[5] J.H.Chang L.Tassiulas,"Energy conserving routing in wireless ad-hoc networks", in proce. IEEE INFOCOM, Mar 2000, PP 22-31.

[6] N. Sadagopan and B. Krishnamachari, "Maximizing data extraction in energy-limited sensor networks," in *Proc. IEEE INFOCOM*, Mar.2004, pp. 1717-1727.

[7] S. Gandham, M. Dawande, R. Prakash, and S. Venkatesan, "Energy-efficient schemes for wireless sensor networks with multiple mobile base stations," in *Proc. IEEE GLOBECOM*, Dec. 2003, pp. 377-381.

[8] Z. M. Wang, S. Basagni, E. Melachrinoudis, and C. Petrioli, "Exploiting sink mobility for maximizing sensor networks lifetime," in *Proc. HICSS*, Jan. 2005.

[9] J. Luo and J. P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks," in *Proc. IEEE INFOCOM*, Mar.2005,pp. 1735-1746.

[10] A. Chakrabarti, A. Sabharwal, and B. Aazhang, "Using predictable observer mobility for power efficient design of sensor networks," in *Proc. IPSN*, Apr. 2003, pp. 129-145.

[11] A. Kansal, A. Somasundara, D. Jea, M. Srivastava, and D. Estrin, "Intelligent fluid infrastructure for embedded networks," in *Proc. ACM MobiSys*, Jun. 2004, pp. 111-124.

[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*, May 2004, pp. 187-198.

[13] I. Papadimitriou and L. Georgiadis, "Maximum lifetime routing to mobile sink in wireless sensor networks," in *Proc. IEEE SoftCOM*, 2005.

[14] J. Luo, J. Panchard, M. Piorkowski, M. Grossglauser, and J.-P. Hubaux, "Mobiroute: Routing towards a mobile sink for improving lifetime in sensor networks," in *Proc. DCOSS*, 2006, pp. 480-497.

[15] A. Shankar and Z. Liu, "Maximum lifetime routing in wireless ad-hoc networks," in *Proc. IEEE INFOCOM*, Mar. 2004, pp. 1089-1097.

[16] Y. T. Hou, Y. Shi, H. D. Sherali, and S. F. Midkiff, "Prolonging sensor network lifetime with energy provisioning and relay node placement," in *Proc. IEEE SECON*, Sep. 2005, pp. 295-304.

[17] J. Chou, D. Petrovic, and K. Ramchandran, "A distributed and adaptive signal processing approach to reducing energy consumption in sensor networks," in *Proc. IEEE INFOCOM*, Mar. 2003, pp. 1054-1062.

[18] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. HICSS*, Jan. 2000.

[19] O. Younis and S. Fahmy, "Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach," in *Proc. IEEE INFOCOM*, Mar. 2004, pp. 629-640.

[20] N. Li, J. Hou, and J. Sha, "Design and analysis of an MST based topology control algorithm," in *Proc. IEEE INFOCOM*, Mar. 2003, pp. 1702-1712.

[21] J. Pan, Y. Hou, L. Cai, Y. Shi, and S. Shen, "Topology control for wireless sensor networks," in *Proc. ACM MobiCom*, Sep. 2003, pp. 286-299.

[22] S. Singh, M. Woo, and C. S. Raghavendra, "Power-aware routing in mobile ad hoc networks," in *Proc. ACM MobiCom*, 1998, pp. 181-190.

[23] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*, 4th ed. New York: McGraw-Hill, 2002.
[24] W. Wang, V. Srinivasan, and K. C. Chua, "Using mobile relays to prolong the lifetime of wireless sensor networks," in *Proc. ACM MobiCom*, Aug. 2005, pp. 270-283.

AUTHORS

C.Venkatesh, M.E., Ph.D.,
Dean, Faculty of Engineering,
EBET Group of Institutions
Nathakadaiyur- 638 108,
Tirupur District, Tamil Nadu

Dr. C. Venkatesh, graduated in ECE from Kongu Engineering College in the year 1988, obtained his master degree in Applied Electronics from Coimbatore Institute of Technology, Coimbatore in the year 1990. He was awarded Ph D in ECE from Jawaharlal Nehru Technological University, Hyderabad in 2007. He has a credit of two decade of experience which includes around 3 years in industry.

He has 16 years of teaching experience during tenure he was awarded **Best Teacher Award** twice. He was the founder Principal of Surya Engineering College, Erode. He is guiding 10 Ph.D., research scholars. He is a Member of IEEE, CSI, ISTE and Fellow IETE. He has Published 13 papers in International and National Level Journals and 50 Papers in International and National Level conferences. His area of interest includes Soft Computing, Sensor Networks and communication.

S.Anandamurugan.,M.E., (Ph.D).,
Senior Lecturer, CSE,
Kongu Engineering College,
Perundurai, Erode-638 052, India.
Email: valasuanand@yahoo.com

He obtained his Bachelors degree in Electrical andElectronics Engineering from “Maharaja engineering College - Avinashi” under Bharathiyar university and Masters Degree in Computer Science and Engineering from “Arulmigu Kalasalingam College of Engineering – Krishnan Koil” under Madurai Kamaraj University. He is currently doing research in Wireless Sensor Networks under Anna University, Coimbatore. He is a life member of ISTE [**LM 28254]**. He presented 10 papers in National and International Conferences. He has published 30 books.