SE2R2: Secure Energy Efficient and Reliable Routing Protocol in Presence of Phishing Attacks for WSNs

Shishir Mathew[1], Mamatha Jadav V[2]

[1]Dept. of Computer Science and Engineering, MSRIT, Bangalore, Karnataka, India
[2]Asst. Professor, Dept. of Computer Science and Engineering, MSRIT, Bangalore, Karnataka, India

---

Abstract - *Phishing is a form of social engineering. It is an attempt to acquire or steal sensitive information such as usernames, passwords and other sensitive information for malicious reasons. In wireless sensor networks(WSNs), the sensor nodes are durable, economical and are designed to be disposed. Energy is limited for wireless sensor networks and has to be managed optimally. Data delivery at the base station(BS) is expected to be reliable. Efficient energy of any application of WSNs is important. Routing in WSNs is very important. Therefore, routing should be done in a sensitive manner so that the energy is saved. We present a secure routing protocol for WSNs which is energy efficient and reliable in its routing technique.*

Key Words: NS2, M-LEACH, Phishing, Base Station, Deputy Cluster Head.

1.INTRODUCTION

In wireless sensor networks(WSNs), the sensor nodes are durable, economical and are designed to be disposed. Energy is limited for wireless sensor networks and has to be managed optimally. Data delivery at the base station(BS) is expected to be reliable. Efficient energy of any application of WSNs is important. Routing in WSNs is very important. Therefore, routing should be done in a sensitive manner so that the energy is saved.

The existing system focuses on minimizing delay and maximizing end-to-end throughput. There are more design objectives to worry about other than delay and throughput. Objectives like energy constraint and signal interference are to be considered as well. Energy efficiency is important because unsupervised sensor nodes are present in WSNs. Routing protocols like Multi-Speed and Multi-Path are designed for WSNs. Recent work on energy efficiency include Directed Alternative Spanning Tree and Energy-Efficient routing algorithm. The proposed routing protocol, where the packets move to the base station(BS) through dense energy area and thus protect the nodes with relatively low residual energy. Some protocols increase the lifetime of the network but the data delivery is unreliable. Mobility of the nodes and the base station is also not considered in protocols. The Modified-LEACH(M-LEACH) ensures the mobility of the nodes in WSNs but not in base station.

Disadvantages:

- Energy inefficiency.
- Signal interference.
- Managing mobility of the nodes and maintaining connectivity through alternate paths.
- Minimizing message overhead.
- Less reliable wireless links.

2. RELATED WORK

[2]. "W. Heinzelman, A. Chandrakasan, and H. Balakrishnan"

The paper "Energy-efficient communication protocol for wireless micro sensor networks", proposed LEACH. LEACH is a clustering-based protocol. It utilizes randomized rotation of cluster heads (Base Station). It evenly distributed the energy load in the network. Scalability and robustness is maintained.

Disadvantages:

- Energy and Communication cost.
- Overhead of dynamic cluster formation.
- Performance has to be improved.

[3]. "S. Lindsey and C. S. Raghavendra"

The paper "PEGASIS: Power-efficient gathering in sensor information systems", proposed PEGASIS. PEGASIS is chain-based protocol which is improvement over the LEACH. The nodes communicate only with a close neighbor. The nodes take turns while transmitting to the base station.

Disadvantages:

- Lifetime of the system is less.
- Network quality is not quite good.
- Energy load balance.

[4]. "A. Manjeshwar and D. P. Agarwal"

The paper "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks", proposed TEEN. TEEN (Threshold sensitive Energy Efficient Sensor Network protocol) classify sensor networks into proactive and reactive networks based on their mode of functioning. It evaluates the

performance of the protocol for simple temperature sensing application. Its performs better than LEACH.

Disadvantages:

- Energy consumption.
- Response time is low.
- Accuracy.

3. PROPOSED SYSTEM

We proposed a secure energy efficient and reliable routing protocol for WSNs. The proposed protocol SE2R2 is hierarchical and cluster-based. The protocol obtains fault tolerance by providing alternative routes. When any fault is detected in existing route to forward data to destination.

The cluster head (CH) aggregates the data to remove redundancy. Then it forward the aggregated data to BS. Clusters contain at least one CH node. These CHs are assisted by two deputy cluster head (DCH) nodes. All these functions are performed in the presence of phishing nodes or the misbehavior nodes but our protocol is successful in removal of the misbehavior nodes as it has the phishing attacks detection and prevention mechanism.

The performance is compared with the M-LEACH on simulations in NS2. The proposed protocol SE2R2 outperforms M-LEACH with respect to packet delivery ratio, packet drop, average energy and throughput.

Advantages:

- Deputy cluster head and Cluster Head Panel which increases the lifetime of the network.
- Efficient data delivery by base station.
- The protocol ensures reliability.
- Data delivery at the base station is reliable.
- Data forwarding.
- Better throughput, average energy, packet drop and delivery ratio than M-LEACH.

4. RESULTS

Simulation Environment:

No. of nodes	82
Terrain	1102 x 780
MAC	802.11
Initial energy	100 Joules
Simulation time	50.5 Sec
Propagation	TwoRayGround
Routing	DSDV

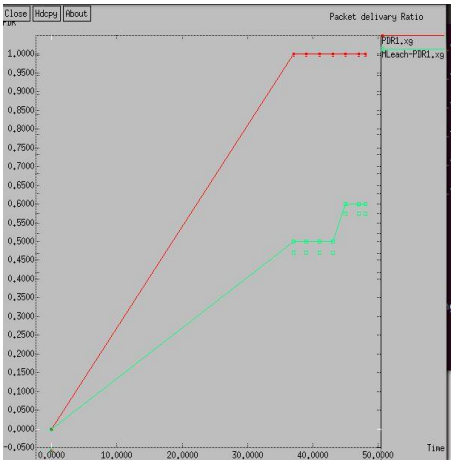

Figure 1: Packet Delivery Ratio

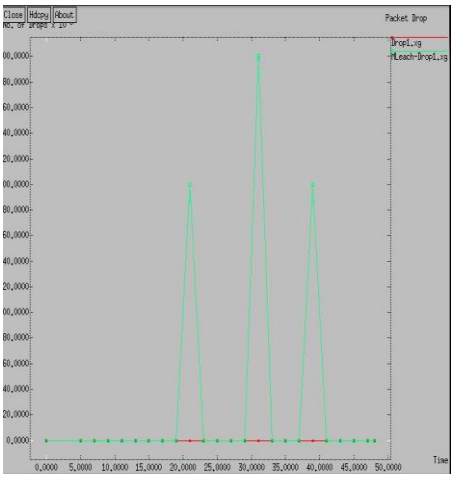

Figure 2: Packet Drop

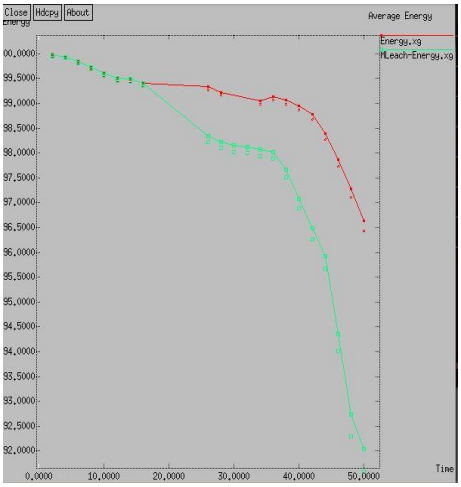

Figure 3: Average Energy

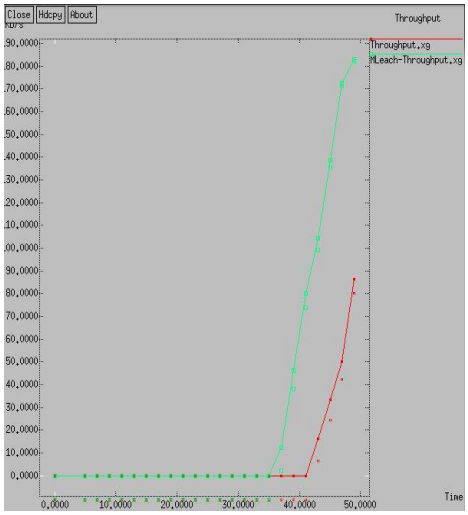

Figure 4: Throughput

5.CONCLUSION

The proposed protocol SE2R2 is more secure and efficient based on the analysis we been through. It's a systematic hierarchical representation of the nodes in the network where we clearly understand the flow of the data way more efficient. The routing is so reliable as it includes different levels of cluster management nodes. The CH collects all the data and forwards to the DCH and finally to the BS. The analysis of the performance is seen in the simulation results in the NS2 where we compared the proposed protocol to the M-LEACH. The proposed protocol gets away with more points than M-LEACH. The proposed protocol is ready for future tests like performance with high mobility nodes and others as they come.

ACKNOWLEDGEMENT

This work has been carried out as a part of Computer Science department, M S Ramaiah Institute of Technology, Bangalore. We thank Management, Principal, HOD and Mamatha Jadav V, Asst. Professor Dept. of Computer Science and Engineering MSRIT for their support and guidelines.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A surveyon sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proc.33rd Annu. HICSS, 2000, pp. 1–10.

[3] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in Proc. IEEE Aerosp. Conf., 2002, pp. 1125–1130.

[4] A. Manjeshwar and D. P. Agarwal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," in Proc. 15th IPDPSWorkshops, 2000, pp. 2009–2015.

[5] A. Manjeshwar and D. P. Agarwal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in Proc. IPDPS, 2002.

[6] D. B. Johnson, and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in Mobile Computing. Norwell,MA, USA: Kluwer Publishers, 1996, pp. 153–181.

[7] C. Perkins and E. Royer, "Ad hoc on demand distance vector routing," in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., 1999, pp. 90–100.

[8] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in Proc. Conf.Commun. Archit. , Protocols Appl., 1994, pp. P234–P244.

[9] C. Siva Ram Murthy and B. S. Manoj, Ad hoc Wireless Networks: Architectures and Protocols, 1st ed. Delhi, India: Prentice-Hall, 2004.