ISSN:0975-9646

Energy-Efficient and Secure Routing In Wireless Sensor Networks

Asha Devi. A[#1], RameshKumar. M [+2]

[#] *Department of Computer Science and Engineering, Anna University-Chennai, Veltech Multitech Engineering College, Avadi, Chennai, Tamil Nadu, India*

[+] *Department of Computer Science and Engineering, , Anna University-Chennai, Vel Tech Multi Tech Engineering College, Avadi, Chennai, Tamil Nadu, India*

***Abstract*-- The clustered wireless sensor networks are incapable of satisfying the resource efficient routing because of the limited battery power, high overhead and low dependability. Base Station(BS) acts as an intermediate node to monitor the data transaction in the entire network. The BS provides an unique ID and password to all the nodes. It also provides a particular time at which all the nodes should register in the network. An energy-efficient clustering algorithm is used to group the nodes into clusters. The Cluster Head(CH) is identified as the node having maximum connectivity with the BS and all other nodes in the cluster. A Trust System based on the residual energy of each node is used in the network which improves the trustworthiness of the entire network. The BS assigns energy level to each node in the network. For the consequent transmissions, each node sends its residual energy after the previous transmission along with its node-ID to the base station. After a particular time, based on the residual energy of the nodes, the BS selects another CH, and the nodes having minimal energy (very less energy such that further routing through it is impossible) are filtered out. This cycle is repeated at definite intervals. Thus the misbehaving nodes can be identified and more reliable routing can be performed. This results in the design of an energy-efficient, trustworthy and dependable communication model in wireless sensor networks.**

***Keywordss*— Dependable, Trust system, Clustering, Residual energy, Minimal energy**

I.INTRODUCTION

Sensor networks contain hundreds or thousands of nodes, and they may need to be deployed in remote or dangerous environments, allowing users to extract information in ways that would not have been possible otherwise. Many clustering algorithms such as LEACH[1], EEHC[2], EC[3], and HEED[4] can effectively improve network scalability and throughput. Nodes are grouped into clusters, and within each cluster, a node with strong computing power or a node having close proximity to its neighbours and base station(BS) is elected as a cluster head (CH). Usually the nodes closer to the sink will be heavily loaded. An Energy-Efficient Clustering (EC), determines suitable cluster sizes depending on the hop distance to the data sink, while achieving approximate equalization of node lifetimes and reduced energy consumption levels. Trust establishment in a clustered environment is of great importance. Trust is the expectation of one entity about the actions of another. A trust system enables a CH to detect faulty or malicious nodes within a cluster, guides the selection of trusted routing nodes through which a cluster member (CM) can send data to the CH. During intercluster communication, a trust system also aids in the selection of trusted routing gateway nodes or other trusted CHs through which the sender node will forward data to the base station (BS).

Contributions

The main aim is to create a secure trust management system for clustered WSNs which enhances both dependability and resource efficiency. The new system go beyond existing approaches in terms of the following aspects:

A.A Lightweight Scheme For Trust Evaluation Between CMs Or Between CHs.

The BS assigns energy level to each node in the network. For the consequent transmissions, each node sends its residual energy after the previous transmission along with its node-ID to the base station. Therefore it is not necessary that each CM need to maintain the feedback from other CMs. This approach will reduce the communication overhead and eliminate the illeffects of a bad-mouthing attack.

B.A Dependability-Enhanced Trust Evaluating Approach Between CHs.

CHs take on large amounts of data forwarding and communication tasks. Taking this into consideration,a dependability-enhanced trust evaluating approach is defined for the communications between CHs. This approach effectively reduces the networking consumption and thus prevents malicious, selfish, and faulty CHs.

C.A Weighting Method For CH's Trust Aggregation.

A self-adaptive weighting method is used which is different from the traditional methods. Weights are measured on the basis of trust factors rather than assigning subjectively.

D.A Secure Trust System

The BS provides an unique ID and password to all the nodes. It also provides a particular time at which all the nodes should register in the network. These new designs and other specific features (e.g., independent of any specific routing scheme and platform and so forth) collectively makes the design a lightweight, self-adaptive, and dependable solution that can be used in any clustered WSN.

II.SYSTEM MODEL

A.Network Topology Model and Assumptions

The BS provides an unique ID and password to all the nodes. It also provides a particular time at which all the nodes should register in the network. All the nodes register in the network using the ID and password issued by the BS at the particular time provided. This helps in the identification of unauthorized or malicious nodes. Then the nodes are grouped into clusters and the cluster head is chosen. The cluster head is chosen based on the node having highest connectivity to all other nodes within the cluster or to the base station. So if the source wants to send the data to the destination node which is located in another network, first the data will be sent to the cluster head of the sender node's network. From that cluster head, the data will be passed to the cluster head of the destination node. Then the destination node's cluster head will re-send the data to the destination node via the best route.

Thus clustering effectively improves network scalability and energy-efficiency[15]. Therefore, in this model, nodes are grouped into clusters using an energy efficient clustering(EC) algorithm. This algorithm determines suitable cluster sizes depending on the hop distance to the data sink, while achieving approximate equalization of node lifetimes and reduced energy consumption levels. The hot-spot issue is particularly significant around sink nodes where large amounts of data are merged. In fact, as the hop distance to a sink decreases, the load on relay nodes quickly intensifies. Hence, there is an obvious relationship between the hop-distance to a data sink and the amount of data that has to be relayed. To obtain a well-balanced network load, this relation should be studied analytically. In doing so, the energy consumption of data communication and of control overhead caused by route discovery and any other procedures should be taken into account.

We propose a scalable, distributed, and energy-aware clustering algorithm, *Energy-efficient Clustering* (EC). EC determines suitable cluster sizes considering their hop distances to the data sink. By tuning the probability that a node becomes a CH, EC effectively controls cluster sizes, which allows an approximately uniform use of the overall energy resources of a WSN. However, EC is adaptable to any data delivery protocol used for data collection to a sink node.

B. Trust Decision Making

CHs take on large amounts of data forwarding and communication tasks. Taking this into consideration, a dependability-enhanced trust evaluating approach is defined for the communications between CHs. This approach effectively reduces the networking consumption and thus prevents malicious, selfish, and faulty CHs.

A Trust System based on the residual energy of each node is used in the network which improves the trustworthiness of the entire network. The BS assigns energy level to each node in the network. For the consequent transmissions, each node sends its residual energy after the previous transmission along with its node-ID to the base station. Therefore it is not necessary that each CM need to maintain the feedback from other CMs. This approach will reduce the communication overhead and eliminate the illeffects of a bad-mouthing attack.

After a particular time, based on the residual energy of the nodes, the BS selects another CH, and the nodes having minimal energy (very less energy such that further routing through it is impossible) are filtered out. This cycle is repeated at definite intervals. Thus the misbehaving nodes can be identified and more reliable routing can be performed.

III. RESULT ANALYSIS AND SIMULATION

For even moderately-sized networks with tens of nodes, it is extremely difficult to analytically model the interactions between all the nodes. Therefore, network simulator Ns2 is used to evaluate the performance of the model. For our experiments, we used a 100-node network where nodes were randomly distributed between (x=0 ,y=0) and (x=100 , y=100) with the BS at location (x=50 ,y=175). The bandwidth of the channel was set to 1 Mb/s, each data message was 500 bytes long, and the packet header for each type of packet was 25 bytes long. We assume a simple model for the radio hardware energy dissipation where the transmitter dissipates energy to run the radio electronics and the power amplifier, and the receiver dissipates energy to run the radio electronics.

The BS provides an unique ID and password to all the nodes. It also provides a particular time at which all the nodes should register in the network. All the nodes register in the network using the ID and password issued by the BS at the particular time provided. This helps in the identification of unauthorized or malicious nodes. Then the nodes are grouped into clusters and the cluster head is chosen.

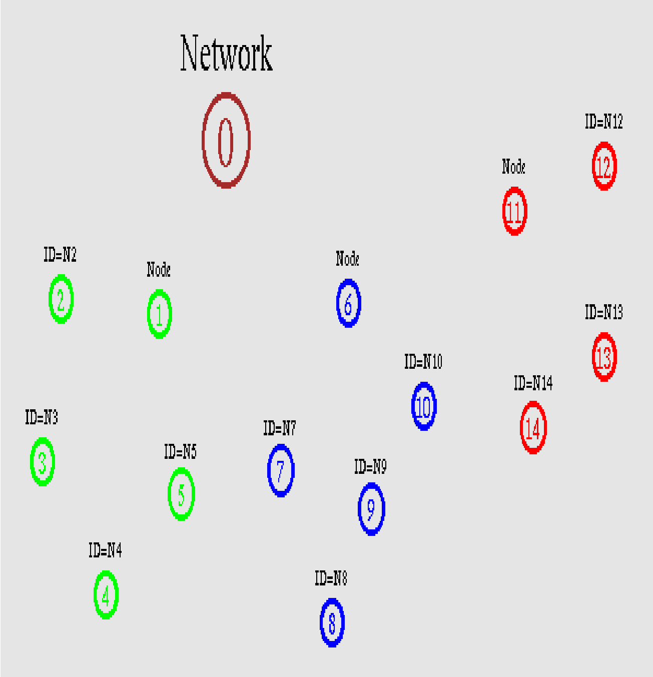

Fig 1 Node registration

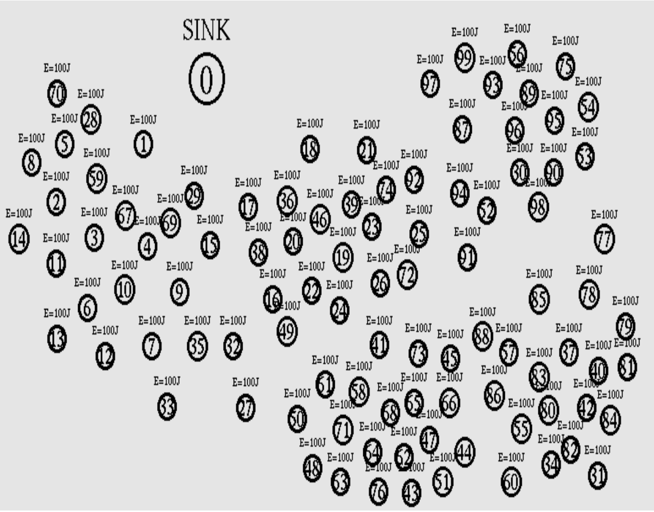

Fig 2 Assigning energy level to all the nodes

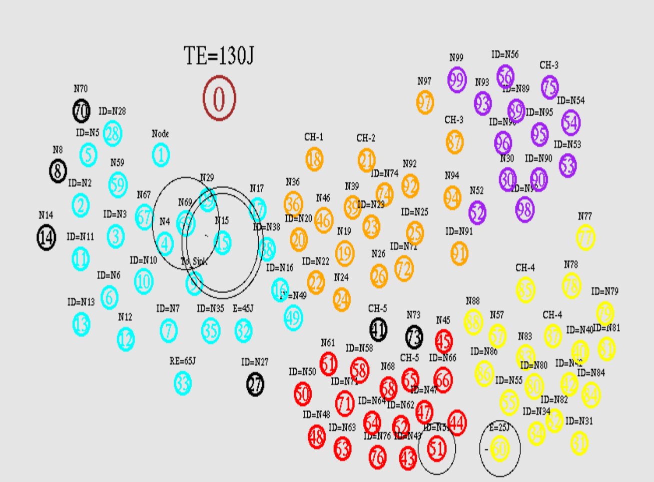

Fig 3 Total energy dissipiated by a single transmission

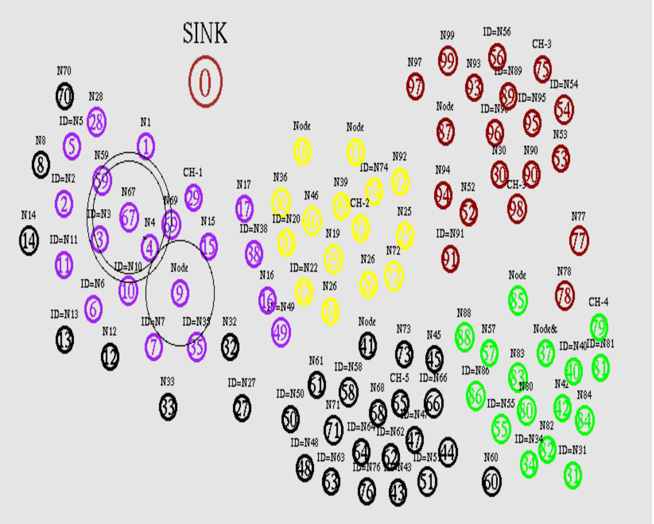

Fig 4 The final network of nodes after transmission

The BS assigns energy level to each node in the network. For the consequent transmissions, each node sends its residual energy after the previous transmission along with its node-ID to the base station. After a particular time, based on the residual energy of the nodes, the BS selects another CH, and the nodes having minimal energy (very less energy such that further routing through it is impossible) are filtered out. This cycle is repeated at definite intervals.

IV. Conclusion

This model can greatly improve system efficiency while reducing the effect of misbehaving nodes. By adopting a dependability-enhanced trust evaluating approach for cooperation's between CHs, this trust model can effectively detect and prevent malicious, selfish, and faulty CHs. After a particular time, based on the residual energy of the nodes, the BS selects another CH, and the nodes having minimal energy (very less energy such that further routing through it is impossible) are filtered out, the misbehaving nodes can be identified and more reliable routing can be performed. Also, nodes get registered into the network using the ID and password issued by the BS which makes the model more secure. The proposed secure protocol can be used in most applications, not only one-to-one secure transmission, but also broadcasting and multicasting. Theory as well as simulation results show that this model demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs. These new designs and other specific features collectively makes the model a lightweight, self-adaptive, and dependable solution that can be used in any clustered WSN.

References

[1] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks,"*IEEE Trans. Wireless commun.*, vol. 1, no. 4, pp. 660–670,Oct. 2002.

[2] D. Kumar, T. C. Aseri, and R. B. Patel, "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," *Comput. Commun.*, vol. 32, no. 4, pp. 662–667, Apr. 2009.

[3] Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, "An energy-efficient clustering solution for wireless sensor networks," *IEEE Trans.Wireless Commun.*, vol. 10, no. 11, pp. 3973–3983, Nov. 2011.

[4] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for Ad-Hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, Oct. 2004.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 3, pp. 1–37, May 2008.

[6] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 2, pp. 184–197, Apr. 2012.

[7] A.Rezgui andM. Eltoweissy, " mRACER: A reliable adaptive service driven efficient routing protocol suite for sensor-actuator networks,"*IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 5, pp. 607–622, May 2009.

[8] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," *Wireless Netw.*, vol. 16, no. 5, pp.1493–1510, Jul. 2010.

[9] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. ACM Workshop Security of ad hoc and Sensor Networks (SASN'04)*, Oct. 2004, pp. 66–67.

[10] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and localized trust management scheme for sensor networks security," in *Proc. Third IEEE Int. Conf. Mobile Ad-Hoc and Sensor Systems (MASS'06)*, Oct. 2006, pp. 437–446.

[11] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in *Proc.*

Second IEEEWorkshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 10–22.

[12] A. Boukerche, X. Li, and K. EL-Khatib, “Trust-based security for wireless ad hoc and sensor networks,” *Computer Commun.*, vol. 30, pp. 2413–2427, Sep. 2007.

[13] R. A. Shaikh, H. Jameel, B. J. d’Auriol, H. Lee, and S. Lee, “Group-based trust management scheme for clustered wireless sensor networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[14] L. Qing, Q. Zhu, and M. Wang, “Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks,” *Computer Commun.*, vol. 29, pp. 2230–2237, 2006.

[15] A. Bari, A. Jaekel, and S. Bandyopadhyay, “Clustering strategies for improving the lifetime of two-tiered sensor networks,” *Computer Commun.*, vol. 31, pp. 3451–3459, 2008.

[16] A. Perrig, R. Szewczyk, V. Wen, D.Culler, and J. D. Tygar, “SPINS: Security Protocols for Sensor Networks”, *Wireless Networks*, 2002, pp 521-534

[17] S. Michell, K. Srinivasan, “State Based Key Hop Protocol: A Lightweight Security Protocol for Wireless Networks”, *1st ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, Venice, Italy. October 4, 2004, pp 112-118.