© 2014 IJIRT | Volume 1 Issue 5 | ISSN : 2349-6002

MANAGEMENT OF OVERABUNDANCE IN HETEROGENEOUS WIRELESS SENSOR NETWORKS

CH.Sandeep Reddy[1], M. Lalitha[2]
[1]*M.Tech, CSE Dept, KCE, Nizamabad*
[2]*M.Tech, Asst. Professor, KCE, Nizamabad*

***Abstract*— we develop a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval under which the lifetime of a HWSN is maximized. The key concept of our redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. In this paper we propose redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. Furthermore, we consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a HWSN. We then apply the analysis results obtained to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes, to maximize the HWSN lifetime.**

***Index Terms*— Heterogeneous wireless sensor networks; multipath routing; intrusion detection; reliability; security; energy conservation.**

I. INTRODUCTION

HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes. We address the tradeoff between energy consumption vs. QoS gain in reliability, timeliness and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. More specifically, we analyze the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime. We consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to remove malicious nodes from the HWSN. Our contribution is a model-based analysis methodology by which the optimal multipath redundancy levels and intrusion detection settings may be identified for satisfying application QoS requirements while maximizing the lifetime of HWSNs.

We address the tradeoff between energy consumption vs. QoS gain in reliability, timeliness and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. More specifically, we analyze the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime. The solution is formulated as an optimization problem to balance energy consumption across all nodes with their roles. In either work cited above, no consideration was given to the existence of malicious nodes. A two-tier HWSN with the objective of maximizing network lifetime while fulfilling power management and coverage objectives. They determined the optimal density ratio of the two tier's nodes to maximize the system lifetime.

Many wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Due to limited resources, a WSN must not only satisfy the application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. The tradeoff between energy consumption vs. reliability gain with the goal to maximize the WSN system lifetime has been well explored in the literature. However, no prior work exists to consider the tradeoff in the presence of malicious attackers. It is commonly believed in the research community that clustering is an effective solution for achieving scalability, energy conservation, and reliability. Using homogeneous nodes which rotate among themselves in the roles of cluster heads (CHs) and sensor nodes (SNs) leveraging CH election protocols such as HEED for lifetime maximization has been considered.

II. PROBLEM STATEMENT

Recent studies demonstrated that using heterogeneous nodes can further enhance performance and prolong the system lifetime. In the latter case, nodes with superior resources serve as CHs performing computationally intensive tasks while inexpensive less capable SNs are utilized mainly for sensing the environment. The tradeoff issue between energy consumption vs. QoS gain becomes much more complicated when inside attackers are present as a path may be broken when a malicious node is on the path. This is especially the case in heterogeneous WSN (HWSN) environments in which CH nodes may take a more critical role in gathering and routing sensing data. Thus, very likely the system would employ an intrusion detection system (IDS) with the goal to detect and remove malicious nodes. While the literature is abundant in intrusion detection techniques for WSNs, the issue of how often intrusion detection should be invoked for energy reasons in order to remove potentially malicious nodes so that the system lifetime is maximized (say to prevent a Byzantine failure) is largely unexplored. The issue is especially critical for energy constrained WSNs designed to stay alive for a long mission time. Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is that the probability of at least one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focused on using multipath routing to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the tradeoff between QoS gain vs. energy consumption which can adversely shorten the system lifetime.

III. SYSTEM DEVELOPMENT

Multi – Path Routing

Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is that the probability of atleast one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focused on using multipath routing to improve reliability, some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the tradeoff between QoS gain vs. energy consumption which can adversely shorten the system lifetime.

Intrusion Tolerance

Intrusion tolerance through multipath routing, there are two major problems to solve:

(1) How many paths to use and

(2) What paths to use.

To the best of our knowledge, we are the first to address the "how many paths to use" problem. For the "what paths to use" problem, our approach is distinct from existing work in that we do not consider specific routing protocols.

Energy Efficient

There are two approaches by which energy efficient IDS can be implemented in WSNs. One approach especially applicable to flat WSNs is for an intermediate node to feedback maliciousness and energy status of its neighbor nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status. Another approach which we adopt in this paper is to use local host-based IDS for energy conservation.

Simulation Process

The cost of executing the dynamic redundancy management algorithm described above, including periodic clustering, periodic intrusion detection, and query processing through multipath routing, in terms of energy consumption.

IV. RELATED WORK

A. Intra-cluster and Inter-cluster Routing In the description of HEED operation, we assumed single-hop communication among cluster heads and their registered cluster members. This is desirable in source-driven networks, where reports are periodically transmitted by the sensor nodes. In this case, a TDM frame may be constructed at each cluster head to eliminate interference within a cluster. Clearly, constructing TDM frames requires node synchronization, and in lightly-loaded networks, using TDM frames may waste resources. A better approach in this case is to allow channel contention. Multi-hop routing to the cluster head can increase network capacity in this case. The reader should refer to [29], [19], [30] for detailed studies addressing the issue of single-hop versus multi-hop routing in clustered networks.

Cluster head overlay (i.e., inter-cluster) routes are used to communicate among clusters, or between clusters and the observer(s). In this case, an ad-hoc routing protocol, such as Directed Diffusion [5] or Dynamic Source Routing (DSR) [31], can be employed for data forwarding among cluster heads. Tiny OS beaconing is the approach currently specified for sensors running Tiny OS. This constructs a breadth-first spanning tree rooted at the base station. In a

clustered network, the beaconing approach can be applied to only the cluster head overlay, instead of the entire network.

If two regular nodes from different clusters attempt to communicate, communication through their cluster heads is sub-optimal if the two regular nodes can directly communicate via a shorter path. This, however, is not the typical communication pattern for sensor network applications, where data is transmitted to an observer which is not close to the target source of data, and data may be aggregated by cluster heads. In addition, since the cluster range is typically limited (compared to the network size), the network can be approximately viewed as a grid-like area, where optimal routes along the grid are computed using routing tables or through reactive routing techniques.

B. Selecting Transmission Ranges Careful selection of the inter-cluster transmission range (Rt) and the intra-cluster transmission range (Rc) is crucial for maintaining network connectivity (as discussed in Section III-D). Reducing interference, maximizing network capacity (concurrent transmissions), and reducing energy consumption are also important objectives to consider when selecting these ranges. Since requirements and transmission patterns (query-based data-driven versus source-driven) widely vary for different applications, determining transmission ranges must be performed on a per-application basis. The network density, radio model, and available number of power levels are constraints that affect the selection process.

A key concern that is common to all applications is that the cluster head overlay, and consequently the entire network, remains connected. This can be achieved if the relationship between the number of nodes in the cluster head overlay n0, and the inter-cluster transmission range Rt satisfy the connectivity condition specified in [32] for unit square region: A method to compute the optimal number of clusters in a sensor network was presented in [8]. The goal of that study was to minimize energy dissipation, and consequently prolong the network lifetime. However, their analysis is specific to the scenario they study in [8], which assumes single-hop transmission is always possible. Selecting the transmission ranges for optimizing a system objective, such as maximizing the network lifetime, is left for future work. This paper only focuses on designing mechanisms for clustering the network for a given (Rc,Rt) pair.

C. Fault Tolerance

HEED clustering is periodically triggered in order to distribute energy consumption among sensor nodes. Re-clustering also provides fault tolerance against unexpected failures, especially failures of cluster heads. In hostile environments (such as military fields), however, unexpected failures may be frequent. This may cause parts of the network to be unreachable. Re-clustering frequency has to be carefully selected in this case to withstand expected failure rates. This is practically difficult for two reasons. First, the failure rates in hostile environments are usually unpredictable and highly variable. This means that frequent re-clustering may result in significant resource waste if the failure rate is low most of the time. Second, frequent re-clustering is not always feasible since it limits the time a sensor is "available" to conduct its primary operations (sensing and data communication), and increases the need for node synchronization. An alternative to frequent clustering is to maintain backup cluster heads. This mitigates the single point of failure problem at each cluster head, since a node can find an alternative path to the observer(s) if its cluster head fails. Finding backup cluster heads that are able to cover the entire cluster (i.e., act as cluster heads for all nodes in the original cluster whose head failed) may not always be feasible, however.

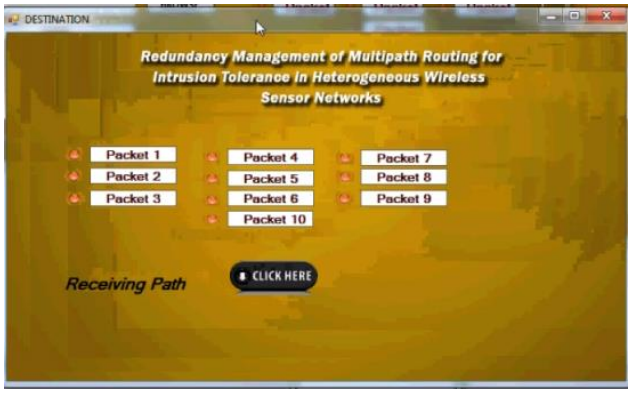
Data dissemination protocols proposed for sensor networks consider energy efficiency a primary goal [6], [5], [40], [7]. SPIN [6] attempts to reduce the cost of flooding data, assuming that the network is source centric

(i.e., sensors announce any observed event to interested observers). Directed diffusion [5], on the other hand, selects the most efficient paths to forward requests and replies on, assuming that the network is data-centric (i.e., queries and data are forwarded according to interested observers). Rumor routing [40] provides a compromise between the two approaches (source-centric vs. data-centric). In [7], 31 the dissemination problem is formulated as a linear programming problem with energy constraints. This approach assumes global knowledge of node residual energy, and requires sensors with specific processing capabilities. In [41], a disjoint path routing scheme is proposed in which energy efficiency is the main parameter.

Clustering can be a side effect of other protocol operations. For example, in topology management protocols, such as GAF [10], SPAN [11], and ASCENT [9], nodes are classified according to their geographic location into equivalence classes. A fraction of nodes in each class (representatives) participate in the routing process, while other nodes are turned off to save energy. In GAF,

geographic information is assumed to be available based on a positioning system such as GPS. SPAN infers geographic proximity through broadcast messages and routing updates. GAF, SPAN, and ASCENT share the same objective of using redundancy in sensor networks to turn radios on and off, and prolong network lifetime. In CLUSTERPOW [3], nodes are assumed to be non-homogeneously dispersed in the network. A node uses the minimum possible power level to forward data packets, in order to maintain connectivity while increasing the network capacity and saving energy. The Zone Routing Protocol (ZRP) [42] for MANETs divides the network into overlapping, variable-sized zones.

V. RESULTS



VI. CONCLUSION

We developed a novel probability model to analyze the best redundancy level in terms of path redundancy ($m\ p$) and source redundancy (m), as well asthe best intrusion detection settings in terms of the number of voters (m) and the intrusion invocation interval (_ s) under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes. In this paper we performed a tradeoff analysis of energy consumption vs. QoS gain in reliability, timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. Finally, we applied our analysis results to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

REFERENCES

[1] 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, 2004.

[2] E. Felemban, L. Chang-Gun, and E. Ekici, "MMSPEED: multipath Multi- SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 5, no. 6, pp. 738-754, 2006.

[3] I. R. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query- Based Wireless Sensor Networks," IEEE Trans. on Dependable and Secure Computing, vol. 8, no. 2, pp. 161-176, 2011.

[4] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," 24th Annu. Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM), 2005, pp. 878-890 vol. 2.

[5] H. M. Ammari and S. K. Das, "Promoting Heterogeneity, Mobility, and Energy-Aware Voronoi Diagram in Wireless Sensor Networks," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 7, pp. 995-1008, 2008.

[6] X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," IEEE 61st Vehicular Technology Conference, 2005, pp. 2528-2532.

[7] S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor

networks," IEEE Wireless Commun., vol. 14, no. 5, pp. 56-63, 2007.
[8] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," 13th European Wireless Conference, Paris, France, 2007.
[9] J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks," IEEE Trans. Rel., vol. 59, no. 1, pp. 231-241, 2010.
[10] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," 1st ACM Workshop on Quality of Service & Security in Wireless and Mobile Networks, Montreal, Quebec, Canada, 2005.
[11] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 6- 28, 2008.
[12] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Trans. Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, 1982.
[13] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," J. Netw. Comput. Appl., vol. 33, no. 4, pp. 422-432, 2010.
[14] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," Computer Communications, vol. 29, no. 2, pp. 216-230, 2006.
[15] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing Geographic Routing in Wireless Sensor Networks," 9th Annu. Cyber Security Conf. on Information Assurance, Albany, NY, USA, 2006.
[16] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1320-1330, 2006.
[17] Y. Lan, L. Lei, and G. Fuxiang, "A multipath secure routing protocol based on malicious node detection," Chinese Control and Decision Conference, 2009, pp. 4323-4328.
[18] D. Somasundaram and R. Marimuthu, "A Multipath Reliable Routing for detection and isolation of malicious nodes in MANET," International Conference on Computing, Communication and Networking, 2008, pp. 1- 8.
[19] H. Su and X. Zhang, "Network Lifetime Optimization for Heterogeneous Sensor Networks With Mixed Communication Modes," IEEE Wireless Communications and Networking Conference, 2007, pp. 3158-3163.
[20] I. Slama, B. Jouaber, and D. Zeghlache, "Optimal Power management scheme for Heterogeneous Wireless Sensor Networks: Lifetime Maximization under QoS and Energy Constraints," Third International Conference on Networking and Services (ICNS) 2007, pp. 69-69.

AUTHOR DETAILS:

First Author: ***CH. Sandeep Reddy*** is currently M.Tech student in Computer Science and Engineering Department from Kshatriya College of Engineering. And his research interested areas are in the field of Cloud Computing, Mobile Computing, Networking and Information Security.

Second Author: ***M. Lalitha*** working as an Asst. Professor in Kshatriya College of Engineering, Armoor. She has completed her M.Tech CSE and she has 5+ years of teaching experience. Her research interested areas are Data Mining, Network Security and Cloud Computing.