International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 443 - 445

Review on Intrusion Tolerance Multipath Routing in Heterogeneous Wireless Sensor

Suchit Gajbhiye
Dept of computer science & Engg.
Wainganga college of Engineering
Nagpur, Maharashtra
suchitgajbhiye@gmail.com

***Abstract*—** Multipath routing to answer user queries in the presence of unreliable and malicious nodes. 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. 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 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. In Proposed System, the optimal communication range and communication mode were derived to maximize the HWSN lifetime. In intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a hierarchal HWSN with CH nodes having larger energy and processing capabilities than normal SNs. 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.

Keyword : *Heterogeneous WSN (HWSN),Intrusion detection system(IDS), Multipath Routing.*

*****

I. INTRODUCTION

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. 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. 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 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. 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.

For the issue of 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.

II. PROBLEM DEFINATION

Malicious attacks in addition to packet dropping and bad mouthing attacks, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.

Another direction is to consider smart and insidious attackers which can perform more targeted attacks, capture certain strategic nodes with higher probability, alternate between benign and malicious behavior and collude with other attackers to avoid intrusion detection. investigate the use of trust/reputation management.

III. LITERATURE REVIEW

In Existing System, effective redundancy management of a clustered 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.

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. 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. 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 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. We then apply the analysis results obtained to the design of a dynamic redundancy management lgorithm to identify and apply the best design parameter settings at runtime in response to environment changes, to maximize the HWSN lifetime.

IV. PROPOSED SYSTEM

In Proposed System, the optimal communication range and communication mode were derived to maximize the HWSN lifetime. In intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a hierarchal HWSN with CH nodes having larger energy and processing capabilities than normal SNs.

- 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.

V. CONCULSION

we plan to explore more extensive malicious attacks in addition to packet dropping and bad mouthing attacks, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. Another direction is to consider smart and insidious attackers which can perform more targeted attacks, capture
certain strategic nodes with higher probability, alternate between benign and malicious behavior and collude with other attackers to avoid intrusion detection. Lastly, we plan to investigate the use of trust/reputation management

REFERENCES

[1] 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. Dependable Secure Computing, vol. 8, no. 2, pp. 161–176, 2011.

[2] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in Proc. 2005 IEEE Conf. Computer Commun., vol. 2, pp. 878–890.

[3] H. M. Ammari and S. K. Das, "Promoting heterogeneity, mobility, and energy-aware Voronoi diagram in wireless sensor networks," IEEE

[4] Trans. Parallel Distrib. Syst., vol. 19, no. 7, pp. 995–1008, 2008.

[5] X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," in Proc. 2005 IEEE Veh. Technol. Conf., pp. 2528–2532.

[6] S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," IEEE Wireless Commun. Mag., vol. 14, no. 5, pp. 560–563, 2007.

[7] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. 2007 European Wireless Conf.

[8] 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. Reliab., vol. 59, no. 1, pp. 231–241, 2010.

[9] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," 13th European Wireless Conference, Paris, France, 2007.

[10] 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.

ISSN: 2321-8169
443 - 445

[11] 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 wirelessc sensor networks," 1st ACM Workshop on Quality of Service & Security in Wireless and Mobile Networks, Montreal, Quebec, Canada, 2005.

[12] 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.