RESEARCH ARTICLE OPEN ACCESS

Redundancy Management of Multipath Routing In Heterogeneous WSN

Manisha Dangi, Prof. R.K.Krishna
Department of Computer Science and Engineering
RCERT Chandrapur, Gondwana University
M.H, India

ABSTRACT

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 algorithm to identify and apply the best design parameter settings at runtime in response to environment changes, to maximize the HWSN lifetime.

Keywords:- HWSN, WSN

I. INTRODUCTION

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.

Over the past few years, numerous protocols have been proposed to detect intrusion in WSNs. [7, 11] provide excellent surveys of the subject. In [10], a decentralized rule-based intrusion detection system is proposed by which monitor nodes are responsible for monitoring neighboring nodes. The monitor nodes apply predefined rules to collect messages and raise alarms if the number of failures exceeds a threshold value. Our host IDS essentially follows this strategy, with the flaws of the host IDS characterized by a false positive probability (H) and a false negative probability (H). In [10], however, no consideration is given about bad-mouthing attacks by compromised monitor nodes themselves, so if a monitor node is malicious, it can quickly infect others. In [8], a collaborative approach is proposed for intrusion detection where the decision is based on a majority voting of monitoring nodes. Their work, however, does not consider energy consumption issues associated with a distributed IDS, nor the issue of maximizing the WSN lifetime while satisfying QoS requirements in security, reliability and timeliness. Our voting-based IDS approach extends from [9] with considerations given to the tradeoff between energy loss vs. security and reliability gain due to employment of the voting-based IDS with the goal to prolong the system lifetime.

II. 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.

III. MODULES DESCRIPTION

1. Multi - Path Routing
2. Intrusion Tolerance
3. Energy Efficient
4. Simulation Process

Multi-path Routing

In this module, 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

In this Modules, 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

In this module, 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

In this module, 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. CONCLUSION

A trust threshold can be designed in static manner or dynamic manner. Static trust threshold might be optimal only for limited cases that we consider in the simulation. As a result, it may not be good for unconsidered situations. Meanwhile, dynamic trust threshold that adaptively changes according to situations in our network may have reasonably good results, although it may not be optimal for all situations. However, since dynamic trust threshold will be frequently computed, it must be designed in an energy-efficient way. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

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 MultiSPEED protocol for QoS guarantee of reliability and. Timeliness iwireless 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 QueryBased 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. JointConf. of the IEEE Computer and Communications Societies (INFOCOM)*, 2005, pp. 878-890 vol. 2.

[5] [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

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