IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 8, August 2015.
www.ijiset.com
ISSN 2348 – 7968

Efficient Security Mechanism for Distributed Sensor Network

C Muruganantham[1], R Geetha[2],

[1]Head of the Department, Computer Science,

Sengunthar Arts and Science College,

Tiruchengode, Tamil Nadu, India.

maraiamcm07@gmail.com

[2]Research Scholar, Department of Computer Science,

Sengunthar Arts and Science College,

Tiruchengode, Tamil Nadu, India.

geetharaja.mca@gmail.com

Abstract

A user would issue a query and expect a response to be returned within the deadline. While the use of fault tolerance mechanisms through redundancy improves query reliability. We develop a mathematical model for the lifetime of the sensor system as a function of system parameters including the "source" and "path" redundancy levels utilized. Data sensing and retrieval in wireless sensor systems have a widespread application in areas such as security and surveillance monitoring. Redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. Lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability. We applied our analysis results to the design of a dynamic redundancy management. The best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

Keywords: Heterogeneous wireless sensor networks, multipath routing, intrusion detection, reliability, security, energy conservation**.**

1. Introduction

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. 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. 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.

2. Related works

Our work also uses multipath routing to tolerate intrusion. However, we specifically consider energy being consumed for intrusion detection, and both CHs and SNs can be compromised for lifetime maximization. In a randomized dispersive multipath routing protocol is proposed to avoid black holes. Moreover, we consider intrusion detection to detect and evict compromised nodes as well as the best rate to invoke intrusion detection to best tradeoff energy consumption vs. security and reliability gain to maximize the system 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

ISSN 2348 – 7968

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 (*Hpfp*) and a false negative probability (*Hpfn*). 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[2] with the goal to prolong the system lifetime. In general there are two approaches by which energy efficient IDS can be implemented in WSNs Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions.

Our solution considers the optimal IDS detection interval that can best balance intrusion accuracy vs. energy consumption due to intrusion detection activities, so as to maximize the system lifetime. The radio range and the transmission power of both CHs and SNs are dynamically adjusted throughout the system lifetime to maintain the connectivity between CHs and between SNs [10]. Any communication between two nodes with a distance greater than single hop radio range between them would require multihop routing. Due to limited energy, a packet is sent hop by hop without using acknowledgment or retransmission [2].The cause could be due to energy exhaustion, packet dropping by malicious nodes, channel/node failure, or insufficient transmission speed to meet the timeliness requirement. Our aim is to find both the optimal redundancy levels and IDS settings under which

3. Proposed method

The tradeoff between energy consumption and QoS gain particularly in reliability. In a randomized dispersive multipath routing protocol is proposed to avoid black holes. A decentralized rule based intrusion detection system is proposed by which monitor nodes are responsible for monitoring neighboring nodes. The intrusion detection where the decision is based on a majority voting of monitoring nodes. The formulated as an optimization problem to balance energy consumption across all nodes with their roles. The objective of maximizing network lifetime. The considers heterogeneous nodes with different densities and capabilities.

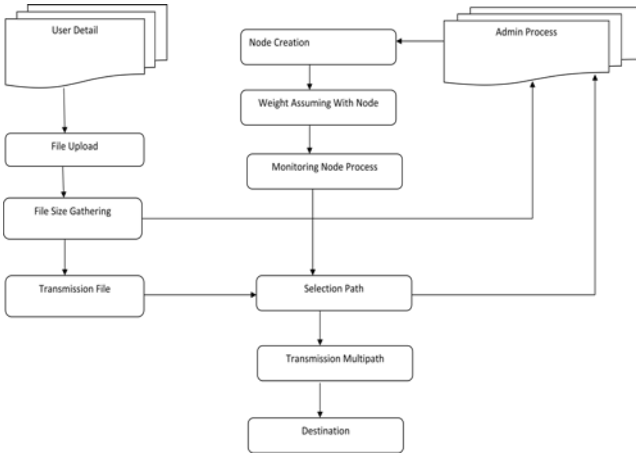

Fig.1 System architecture

3.1 Hash-based coordination

A hash-based selection primitive to eliminate duplicate measurements in the network. Thus eliminating redundant and possibly ambiguous measurements across the network. The packet if the hash falls within the range obtained from the sampling manifest. The hash is used as an index into a table of flows that the router is currently monitoring.

3.2 Network-wide optimization

In optimization framework to specify and satisfy network-wide monitoring objectives while respecting router resource constraints. The output of this optimization is then translated into per-node sampling manifests that specify the set of flows that each node is required to record. A wide range of network topologies and more than twice as many flows compared with traditional uniform packet sampling.

3.3 Network Wide Evaluation

The alternative full coverage solution where each ingress Node is capture all traffic on incoming interfaces. In packet sampling alternatives to uniform packet sampling with a sampling rate of 1-in-100 packets at all routers in the network. A Node processing packets on each interface. We first derive the minimum hop-by-hop transmission speed required to satisfy the query deadline. Here we note that increasing source or path redundancy enhances reliability and security.

3.4 Energy Consumption

We estimate the amounts of energy spent during a query interval. The energy dissipated to run the transmitter and receiver circuitry. All nodes in the system act periodically to a “TD timer” event to adjust the optimal parameter setting in

ISSN 2348 – 7968

response to changing environments. Static design time and pre-stored in a table over perceivable ranges of input parameter values. When a data packet arrival event occurs, each nodes imply follows the prescribed multipath routing protocol to route the packet.

3.5 System classification

If traffic occurs in the network means, the monitoring System find out the attacker system by using this system classification. Source IP and Port details notify the attacker system among the network. The system classification data classification is done.

The computational procedure essentially has a complexity of *O* (*mp*×*ms*) as it exhaustively searches for the best (*mp*, *ms*) pair, given a set of input parameter
values as listed as well as instance values of *m* (the number of voters for intrusion detection) and *TIDS* (the intrusion detection interval) characterizing a HWSN. A query response propagates over SNs for source redundancy (*ms*) and over CHs for path redundancy (*mp*). Hence, *ms* directly affect energy consumption of SNs and *mp* directly affects energy consumption of CHs. The effect of (*mp*, *ms*) on the CH/SN energy, query reliability, and CH/SN radio range, respectively, for the case in which *Tcomp* = 4 days and *TIDS*= 10 hrs. A relatively high *mp* leads to quick energy depletion of a CH node. Similarly, a relatively high *ms* leads to quick energy depletion of a SN. While energy determines the number of queries the system is able to execute, the system lifetime largely depends on query reliability. The effect of (*mp*, *ms*) on query reliability. The combination of (4, 3) has the highest query reliability over other combinations of (2, 5) or (5, 2) in this test scenario. The system dynamically adjusts the radio range of CHs and SNs to maintain network connectivity based on as nodes are being removed from the system because of failure or eviction that the rates at which radio ranges of CHs and SNs increase are highly sensitive to *mp* and *ms*.

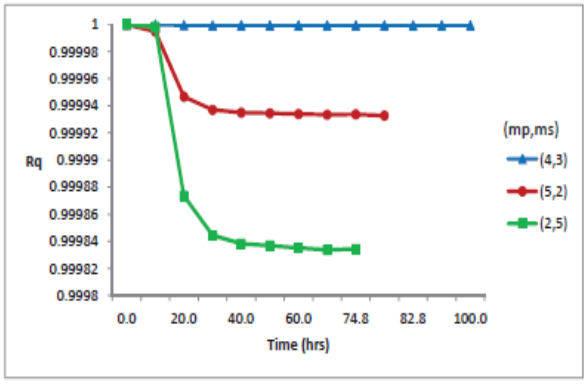

Fig.2 Effect of (*mp*, *ms*) on query reliability (*Rq*).

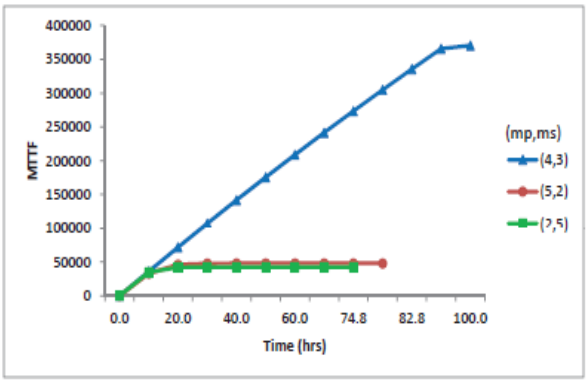

Fig.3 Effect of (*mp*,*ms*) on MTTF

4. Conclusion

We performed a tradeoff analysis of energy consumption vs. QoS gain in reliability. Wireless sensor networks utilizing multipath routing to answer user queries. A novel probability model to analyze the best redundancy level in terms of path redundancy. We applied our analysis results to the design of a dynamic redundancy management algorithm. 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.

5. Acknowledgments

I wish to thank my institution, ‘Sengunthar Arts and Science College, ‘giving me the opportunity to write a research paper. A special thanks to my Head of the Department, C. Muruganantham for encouraging me and to C. Muruganantham for him support and guidance throughout and without whom, this work would have not been possible. Last but not the least; I would like to thank the authors of the various research papers that I have referred to, for the completion of this work.

6. References

[1] Hamid Al-Hamadi and Ing-Ray Chen, 2013 “Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks” IEEE Transactions On Network And Service Management, vol. 10, no. 2 pp-189-203.
[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.

ISSN 2348 – 7968

[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. Dependable Secure Computing, vol. 8, no. 2, pp. 161–176, 2011.
[4] 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.
[5] 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.
[6] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. 2007 European Wireless Conf.
[7] 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.
[8] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," IEEE Commun. Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008.
[9] 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.
[10] D. Somasundaram and R. Marimuthu, "A multipath reliable routing for detection and isolation of malicious nodes in MANET," in Proc. 2008 Int. Conf. Computing, Commun. Netw., pp. 1–8.
[11] R. Machado, N. Ansari, G. Wang, and S. Tekinay, "Adaptive density control in heterogeneous wireless sensor networks with and without power management," IET Commun., vol. 4, no. 7, pp. 758–767, 2010.
[12] E. Stavrou and A. Pitsillides, "A survey on secure multipath routing protocols in WSNs," Comput. Netw., vol. 54, no. 13, pp. 2215–2238, 2010.
[13] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, 2010.
[14] F. Bao, I. R. Chen, M. Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manage., vol. 9, no. 2, pp. 161–183, 2012.
[15] C. J. Fung, Z. Jie, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," IEEE Trans. Netw. Service Manage., vol. 8, no. 2, pp. 79–91, 2011.