International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Multipath Intrusion Tolerance Redundancy Management in Heterogeneous WSN

Shaik Nagul Meera[1]& P.Kusuma[2]
[1]PG Scholar,Dept of CSE, Chalapathi Institute Of Technology,Guntur ,Andhra Pradesh,
Email: nagulmeera008@gmail.com
[2]Professor,Dept of CSE, Chalapathi Institute Of Technology,Guntur,Andhra Pradesh,
Email: kusuma.polanki@gmail.com

Abstract:
A heterogeneous wireless sensor networks (HWSNs) consists of two or more types of nodes. The redundancy management of various wireless sensor networks uses multipath routing to answer user queries in the presence of defective and malicious nodes. The fixed method uses a novel probability model to analyze the best redundancy level in terms of path redundancy (mp) and source redundancy (ms), as well as the best interruption detection settings in terms of the number of voters (m) under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security, so the above problem can be solved using packet modifier and packet sniffing attack, by making use of Shamir secret sharing algorithm and by adding checksum. 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.
Keywords: Heterogeneous wireless sensor networks; multipath routing; intrusion detection; reliability; security

Introduction:

Many wireless sensor networks (WSNs) are deployed at the environment where the energy replenishment is very difficult but it is 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. In the literature the trade-off between energy consumption v/s. reliability gains, with the goal to maximize the WSN system lifetime has been well explored. However, in literature no work exists to consider the tradeoff in the presence of malicious node which are responsible for packet loss also which are harmful to the network. It is considered that clustering is one of the best solutions to achieve the scalability, reliability and energy conservation in wireless sensor network. If the homogeneous network is consider then the cluster head (CH) is selected among all nodes which rotate in the network.

REDUNDANCY WSN:

A WSN [1, 4] is a special type of Ad hoc networks containing several sensor nodes which are able to collect data and to transmit it using a multi-hop routing protocol to the collection point called Sink node. The important density of sensor nodes implies the existence of redundant nodes. Generally, the breakdowns in a WSN can be caused by the mobility or the exhaustion of the nodes energy. These breakdowns must be detected and solved in an acceptable time without affecting quality of service. This centralization of diagnosis and reconfiguration operations in only one module (Sink in general) presents the following major disadvantages:

- Overload of the monitoring module by control treatments.

- Overload of all the nodes in network by the control and reconfiguration messages, which increases considerably energy consumption especially in the case of large scales networks. So WSN life time is reduced.

- The failure detection can be delayed because Transmission times.

- The failure of the monitoring module paralyzes the operation of the entire network.

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.

RELATED WORK:

Over the past few years, many protocols exploring the tradeoff between energy consumption and QoS gain particularly in reliability in HWSNs have been proposed. In [19], the optimal communication range and communication mode were derived to maximize the HWSN lifetime. In [20], the authors devised 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 this the author propose a novel distributed clustering approach for long-lived ad hoc sensor networks. The proposed approach does not make any assumptions about the presence of infrastructure or about node capabilities, other than the availability of multiple power levels in sensor nodes. Authors present a protocol, HEED (Hybrid Energy-Efficient Distributed clustering), that periodically selects cluster heads according to a hybrid of the node residual energy and a secondary parameter, such as node proximity to its neighbors or node degree. R. Chen et al. proposed Adaptive fault-tolerant QoS control algorithms for maximizing system lifetime of query- based wireless sensor networks, n this paper, we develop adaptive fault-tolerant quality of service (QoS) control algorithms based on hop-by-hop data delivery utilizing source and path redundancy, with the goal to satisfy application QoS requirements while prolonging the lifetime of the sensor. S. Bo, L. Osborne et al. proposed Intrusion detection techniques in mobile ad hoc and wireless sensor networks, In this paper, first author briefly introduce mobile ad hoc networks and wireless sensor networks and their security concerns. Then, they focus on their intrusion detection capabilities.

Analysis of Existing System:

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 node. In the context of secure multipath routing for intrusion tolerance, [22] provides an excellent survey in this topic. In [15] the authors considered a multipath routing protocol to tolerate black hole and selective forwarding attacks. The basic idea is to use overhearing to avoid sending packets to malicious nodes. In [14] the authors considered a disjoint multipath routing protocol to tolerate intrusion using

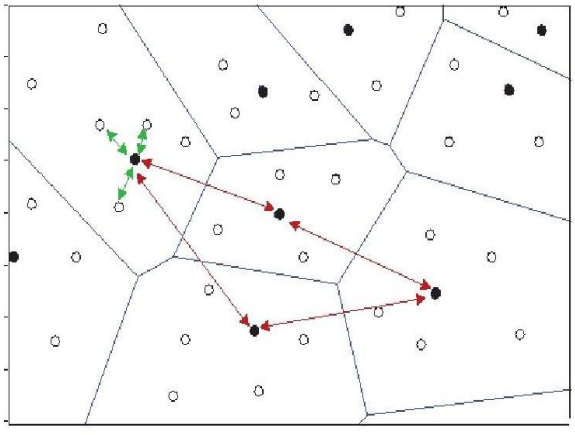
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

multiple disjoint paths in WSNs. Our work also uses multipath routing to tolerate intrusion.

PROPOSED SYSTEM:

In proposed system, 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 [3]. Another direction, the problem statement can be solved using packet modifier and packet sniffing attack. Here, the source node will split the packet using Shamir secret sharing algorithm and sends the share into the multiple path. The individual share of packet generated by Shamir ensures security. In-addition we add checksum in the packet to verify if any modification of packet is done in transit by the attacker. The modified packets are dropped and with minimum number of packets reconstruction of the packets is done at the sink. Finally, At least one path exists from source to sink by implementing Intrusion detection system through voting, in presence of malicious attacker.

SYSTEM MODEL:



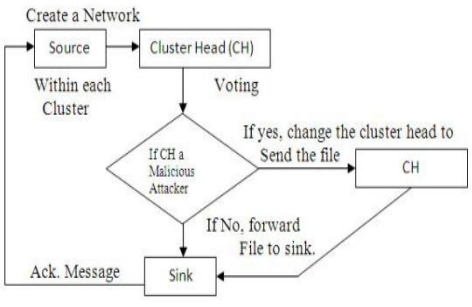
A HWSN comprises sensors of different capabilities. We consider two types of sensors: CHs and SNs. CHs are superior to SNs in energy and computational resources. Anycommunication between two nodes with a distance greater than single hop radio range between them would require multi-hop routing. Due to limited energy, a packet is sent hop by hop without using acknowledgment or retransmission [2] All sensors are subject to capture attacks, i.e., they are vulnerable to physical capture by the adversary after which their code is compromised and the become inside attackers. Since all sensors are randomly located in the operational area, the same capture rate applies to both CHs and SNs, and, as a result, the compromised nodes are also randomly distributed in the operation area. Due to limited resources, we assume that when a node is compromised, it only performs two most energy conserving attacks, namely, bad-mouthing attacks (recommending a good node as a bad node and a bad node as a good node) when serving as a recommender, and packet dropping attacks [25] when performing packet routing to disrupt the operation of the network.

ROUTING TRANSACTION:

File transfer is a generic term for the act of transmitting files from source to destination or sender to receiver or client to server over a computer network like the Internet. There are numerous ways to transfer files over a network. Computers which provide a file transfer service are often called file servers. Depending on the client's perspective the data transfer is called uploading or downloading.

SYSTEM ARCHITECTURE:

Dataflow diagram for the overall architecture

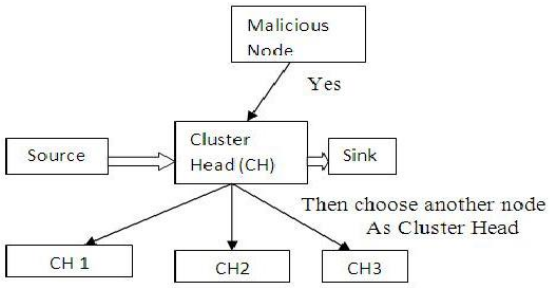


International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

MULTIPATH ROUTING:

The 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. In the context of secure multipath routing [2] for intrusion tolerance, provides an excellent survey in this topic. The authors considered a multipath routing protocol to tolerate black hole and selective forwarding attacks. The basic idea is to use overhearing to avoid sending packets to malicious nodes. Our work also uses multipath routing to tolerate intrusion.

ARCHITECTURE DIAGRAM:



In Architecture Diagram clearly shows that the cluster head is chosen based on the LEACH algorithm. And each node is taking a part as a monitoring agent and also they can be act as a routing node. The cluster head is changed dynamically to avoid the redundancy in the path and also for to avoid the Hackers to track the path.

In HSWN, performance of a trade-off 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, At least one path exists from source to sink by implementing Intrusion detection system through voting, in presence of malicious attacker.

FUTURE WORK

In order to achieve higher reliability and load balancing various multipath routing protocols have been proposed in Wireless Sensor Network. Moreover, wireless sensor network typically incorporates heterogeneous applications within the same network. A sensor node may have multiple sensors i.e. light, temperature, seismic etc with different transmission characteristics. We propose an efficient scheme to control multipath congestion so that the sink can get priority based throughput for heterogeneous data. In addition to packet modifier and packet sniffing attack, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.

Future work

To improve the fairness, analysis of the impact of other parameters on the proposed scheme's performance and implementing this scheme on a real sensor test-bed and compare the results with those obtained in the simulations.

REFERENCES:

[1] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 10, NO. 2, JUNE 2013.

[2] E. Felemban, L. Chang-Gun, and E. Ekici, "MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness inwireless 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-TolerantQoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks," IEEE Trans. on Dependable andSecure 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

[5] 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

[6] 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.

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

[8] 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

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