International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 14 (2014), pp. 1379-1386

http://www. irphouse.com

Effective Redundancy Management of Multipath Routing against Packet Modifier and Packet Sniffing Attack

Impana Appaji [1] and Vani H.Y [2]

[1, 2] Sri Jayachamarajendra College of Engineering,
Department of Information Science & Engineering, Mysore, Karnataka, India.
impana.appaji@gmail.com[1], vanihy@yahoo.com [2]

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.

KEYWORDS: Heterogeneous wireless sensor networks (HWSNs); multipath routing; intrusion detection; reliability; security; energy conservation.

INTRODUCTION

Many wireless sensor networks (WSNs) [4] are deployed in an unattended environment in which energy replenishment is 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.

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.

ABOUT THE PROJECT

Many wireless sensor networks (WSNs) [4] are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Multipath routing [2] is considered an effective mechanism for fault and intrusion tolerance [3] 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 trade-off between QoS gain v//s. energy consumption which can adversely shorten the system lifetime. The research problem we are addressing in this paper is effective redundancy management of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes. We address the trade-off 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 [2]. 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.

EXISTING SYSTEM

The prior work performed 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 [2] to answer user queries. We developed a novel probability model to analyze the best redundancy level in terms of path redundancy (*mp*) and source redundancy (*ms*) [1], as well as the best intrusion detection settings in terms of the number of voters (*m*) [1] and the intrusion

invocation interval (TIDS) 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. But it cannot perform extensive malicious attacks and insidious attackers.

Disadvantages:

- It's difficult to detect extensive malicious attacks and insidious attackers
- No security for file

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.

Advantages:

- Security and Reliability, Easily detect insidious attackers.
- Best intrusion detection in packet dropping, bad mouthing attacks, packet modifier and packet sniffing attack.

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.

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 [3]. However, we specifically consider energy being consumed for intrusion detection, and both CHs and SNs can be compromised for lifetime maximization.

INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) has the goal to detect and remove malicious nodes. A voting-based distributed intrusion detection algorithm is applied to remove malicious nodes from the HWSN. To remove malicious nodes from the system, a voting based distributed IDS is applied periodically in every TIDS time interval. A CH is being assessed by its neighbour CHs, and a SN is being assessed by its neighbour SNs. In each interval, *m* neighbour nodes (at the CH or SN level) around a target node will be chosen randomly as voters and each cast their votes based on their host IDS results to collectively decide if the target node is still a good node.

SYSTEM ARCHITECTURE

Data flow Diagram

The sender (Source) can transmit a data to the Receiver (Sink) without any intrusion of other malicious node i.e. Hacker System. To avoid this problem the sender uses a Multipath routing to transfer the data securely with the help of the transferring and monitoring agent called Cluster Head.

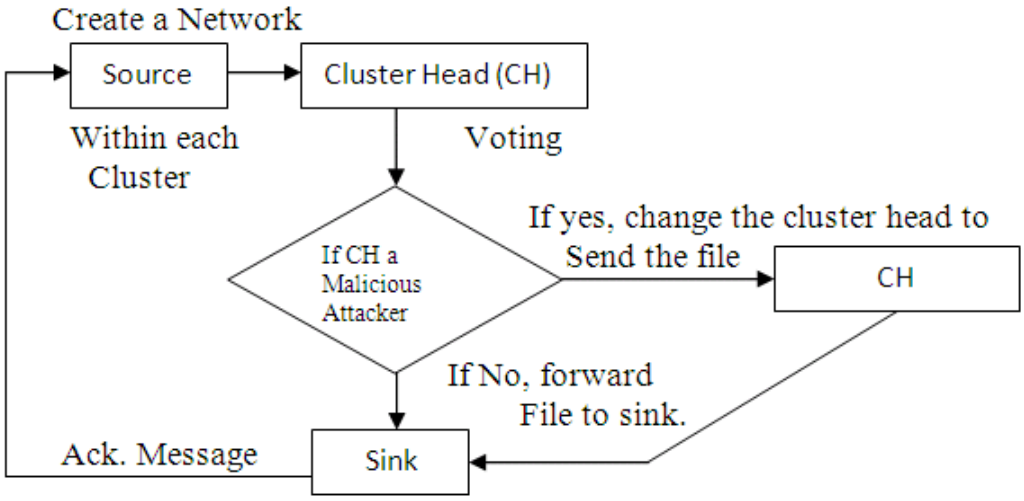

Fig.1: Dataflow diagram for the overall architecture

In the HWSN the each system is considered as the node. The Cluster node is chosen based on LEACH Algorithm.

ARCHITECTURE DIAGRAM

In Architecture Diagram Fig.2 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.

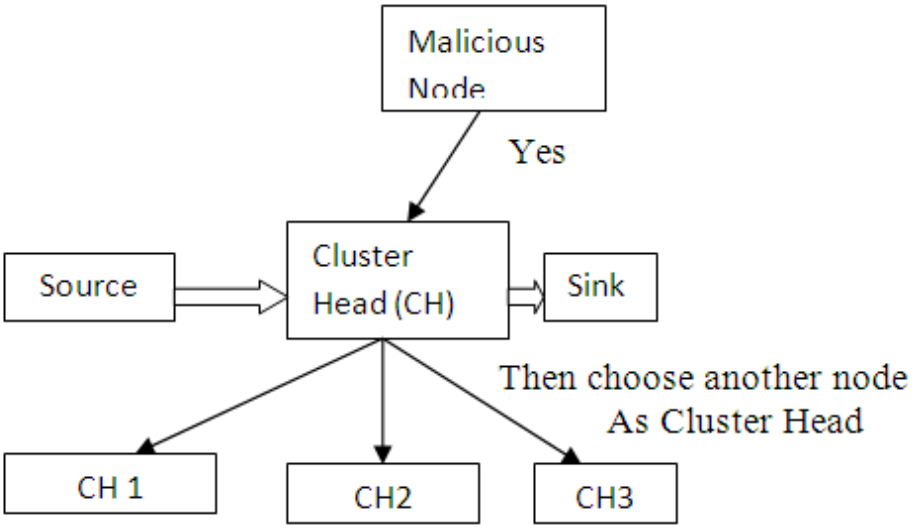

Fig.2: Architecture Diagram

Table1: Describes the simulation results.

	NODES	CLUSTERS	CLUSTER HEAD	RESULT
Creating network	50 nodes are created.	Forming clusters	Choose CH in each cluster	True
	If more than 200 nodes are created	Nil	Nil	False
Attacker	Identifying the attacker node by implementing IDS	Nil	If, CH is attacker, choose another SN as CH	True
Sending message	To sink, Using Shamir secret sharing algorithm	Nil	Sending message through cluster head	True
Sink	Original message is obtained and validated using checksum.	Nil	Nil	True
	If the checksum does not match, packet is dropped	Nil	Nil	True

SOFTWARE DESCRIPTIONS

Coding: Java, Platform: Jdk, Tool: Netbean IDE, OS: Windows OS, Chart: JFreeChart Simulator: Jprowler, Front end: Swings.

PERFORMANCE EVALUATION

We developed 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 intrusion detection settings in terms of the number of voters (*m*) and the intrusion invocation interval (TIDS).

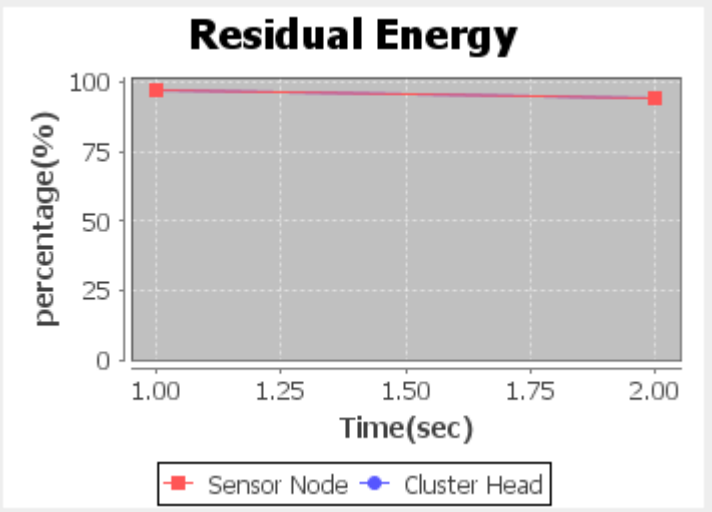

Fig.3: Initial Energy of the SN and CH.

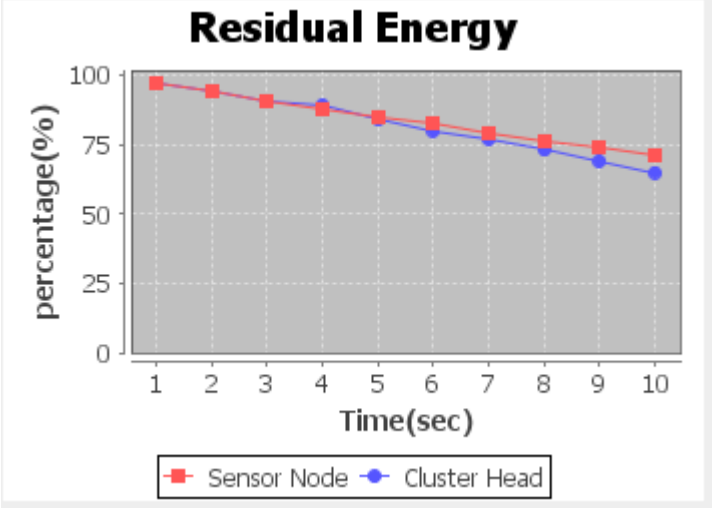

Fig.4: Energy of the CH decreases by Time.

ENERGY CONVSERVATION CONSUMPTION

In general 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 neighbour 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, coupled with voting to cope with node collusion for implementing IDS function. 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.

CONCLUSION AND FUTURE WORKS

CONCLUSION

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 forIntrusion Tolerance in Heterogeneous Wireless Sensor Networks" *IEEE Trans. networking*, vol. VOL: 10 NO: 2 YEAR 2013.

[2] 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.

[3] 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.

[4] 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.