ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 94-97 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Supervision termination for multipath routing with intervention detection in wireless sensor networks

Anil kumar.K[1]
Department of CSE, St Ann's college of Engineering and Technology chirala ,India
k.anil504@gmail.com[1]

Eswar.K[2]
Department of CSE, St Ann's college of Engineering and Technology chirala ,India
kodali_eswar@yahoo.co.in[2]

Abstract- Research problems are to enhance an Intrusion Detection System (IDS) of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes. Also, to address the energy consumption and QoS gain in reliability, delay and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. The proposed research is a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes.To propose redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipathrouting to answer user queries in the presence of unreliableand malicious nodes. The key concept of our redundancymanagement is to exploit the tradeoff between energyconsumption vs. the gain in reliability, timeliness, andsecurity to maximize the system useful lifetime. Weformulate the tradeoff as an optimization problem fordynamically determining the best redundancy level to applyto multipath routing for intrusion tolerance so that the queryresponse success probability is maximized while prolongingthe useful lifetime. To demonstrate the utility of the hierarchical trust management protocol, it can be apply to trust-based intrusion detection and trust-based geographic routing. For trust-based intrusion detection, there exists an optimal trust threshold for minimizing false positives and false negatives probability. Furthermore, trust-based intrusion detection outperforms traditional anomaly-based intrusion detection approaches in both the detection probability and the false positive probability. The proposed research also present a new multipath routing protocol which provides strong fault tolerance by increasing the number of constructed paths up to four times, as well as tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs. The protocol relies on a new multipath constructions paradigm that is defined specifically for heterogeneous WSN. The approach leverages a reasonable increase in the network lifetime and a higher resilience and fault tolerance.

Keywords- Intrusion detection system (IDS), multipath routing, fault tolerance, trust management, heterogeneous WSN (HWSN)

I.INTRODUCTION

A Wireless Sensor Network(WSN) consists of spatially distributed autonomous wireless sensor nodes. A node in a Wireless network is able to collect the information from sensors, process it and communicate wirelessly with other nodes in the network. It is used to monitor physical or environmental condition such as temperature, sound, vibration, pressure and pass their data through the network. A WSN is a self configuring network of small sensor nodes communicating among themselves using radio signals and deployed in quantity to sense monitor and understand the physical world. WSN are called motes. WSN has wide range of application to industry, science, transportation, civil infrastructure and security. Heterogeneous Wireless Sensor Network (HWSN) consists of sensor nodes with different capacity, different computing power and different sensing range. Sensor node are battery powered device, hence it reduce the energy consumption

1.1Idleness 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.

Disadvantages:

- Surplus of the monitoring module by control treatments.
- Surplus 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.

1.2 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 adverselyshorten the system lifetime. The research problem we are addressing in this paper is effective idleness 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 idleness 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.

2. Related Works

The prior work performed a trade-off analysis of energy consumption vs. QoS gain in reliability, timeliness, and security for idleness 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 idleness level in terms of path idleness (*mp*) and source idleness (*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

Our description:

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.

2.1 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.

2.2 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.

2.3 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.

3.Performance Evaluation

We developed a novel probability model to analyze the best idleness level in terms of path idleness (*mp*) and source idleness (*ms*), as well as the best intrusion detection settings in terms of the number of voters (*m*) and the intrusion invocation interval (TIDS).

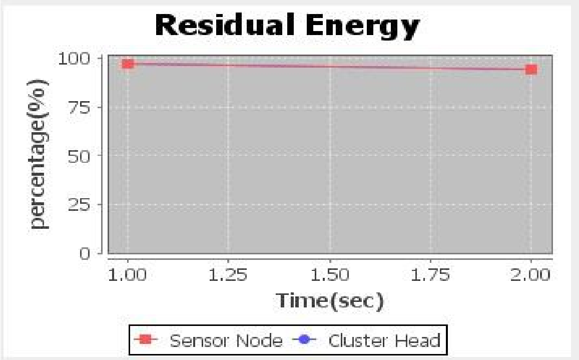

Fig.1: Initial Energy of the SN and CH.

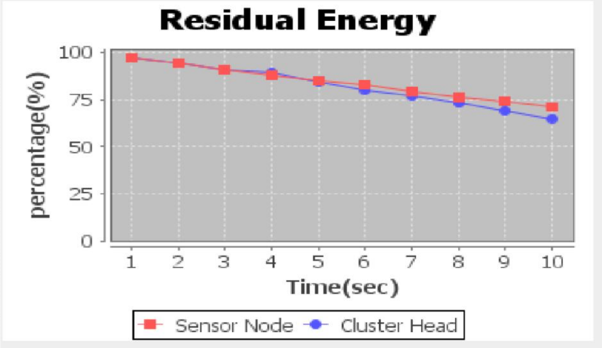

Fig.2: Energy of the CH decreases by Time

3.1 Energy Conservation 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.

4.Future Work

In order to achieve higher reliability and load balancing various multipaths 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.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.

5. Conclusion

In HSWN, performance of a trade-off analysis of energy consumption vs. QoS gain in reliability, timeliness, and security for idleness 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.

6. References

[1] Hamid Al-Hamadi and Ing-Ray Chen, "Idleness 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. 216230, 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

Authors

I. ANILKUMAR KAKARAPARTHI is a studentOf Computer Science Engineering from **ST.ANN'SCOLLEGEOFENGINEERING&TECHNOLOGY,CHIRALA.** Presently pursuing M.Tech (CSE) fromthis college. He received B.Tech from JNTUK in the year of 2012.

II. K ESWAR is a Associate Professorof**ST.ANN'SCOLLEGEOFENGINEERING&TECHNOLOGY,CHIRALA.** He has presented nearly 6 various International journals, 6 International conferences .He is gained 10years Experience on Teaching . He is a good researcher in Information Security.