National Conference on Emerging Trends in Computer, Electrical & Electronics (ETCEE-2015)
International Journal of Advance Engineering and Research Development (IJAERD)
e-ISSN: 2348 - 4470 , print-ISSN:2348-6406,Impact Factor:3.134

"Intrusion Detection and Multipath Congestion control for Heterogeneous Traffic in Wireless Sensor Network"

Impana Appaji [1]

[1]Assistant Professor
Department of Computer Science & Engineering,
Academy for Technical and Management Excellence college of Engineering,
Mysore, Karnataka, India.

impana.appaji@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, In this paper we propose an efficient scheme to control multipath congestion so that the sink can get priority based throughput for heterogeneous data. We have used packet service ratio for detecting congestion as well as performed hop-by-hop multipath congestion control based on that metric. Finally, simulation results have demonstrated the effectiveness of our proposed approach.

KEYWORDS: Heterogeneous wireless sensor networks (HWSNs); multipath routing; intrusion detection; reliability; security; energy conservation.; Congestion Control ;Multipath Heterogeneous traffic Scheduler.

I. 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.

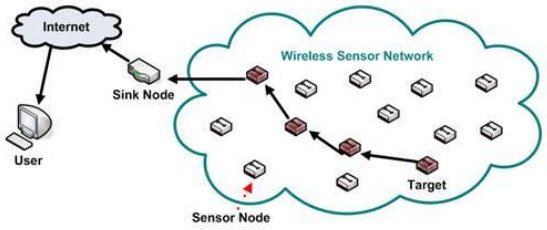

Fig.1: Typical Wireless sensor Network Topology.

In recent years, the use of diverse applications in sensor network is proliferating. Sensor nodes may have multiple sensors (light, temperature, seismic) with different transmission characteristics. Packets from a sensor for an application constitute its data flow. For several classes of applications a sensor node may initiate multiple flows that have diverse requirements in terms of transmission rate, reliability, delay and throughput towards the sink. In our protocol, we have designed a queuing model for generating the heterogeneous traffic within each sensor node according to the priority specified by the sink. In WSN, usually tens or thousands of sensor nodes are deployed scattered way in an area with one or more sinks. Myriad and divergent types of traffic from simple periodic events to unpredictable bursts of messages are generated by sensor nodes. Moreover, for achieving reliability and load balancing, several multipath routing protocols have been proposed. But the limitation of these protocols is traffic

overhead. Thus the occurrence of congestion in this situation is more likely. The situation becomes worse when congestion occurs in multiple paths. In order to achieve the desired rate of heterogeneous traffic by the sink the congestion control over multiple paths is indispensable.

In general, congestion control mechanism has three phases: congestion detection, congestion notification and congestion mitigation through rate control. In this paper, we propose an efficient scheme to perform multipath congestion control for heterogeneous traffic which avoids packet loss and thus enhances the probability of achieving the desired throughput of heterogeneous traffic. Our congestion detection mechanism is chosen based on packet service ratio

II. RELATED WORK

In present research train, lots of work is going on congestion control for wireless sensor network. Scenarios with multipath routing are not considered. It is not clear whether they can be directly applied to WSNs with multipath routing enabled [7]. Moreover, most of the protocols deal with homogeneous traffic. Sensor nodes may have multiple sensing devices (e.g. temperature, light, pressure etc.) and no other protocols except STCP [1] considered multiple sensing devices in the same node. But STCP has some problems:
1) It doesn't consider multipath routing even it doesn't state any explicit and detailed mechanism for single path congestion control. 2) The ACK/NACK based reliability mechanism is not suitable for wireless sensor networks in terms of delay and memory use. Recently a node priority based control mechanism PCCP [2] has been proposed for WSN. It introduces an efficient congestion detection technique addressing both node and link level for detecting congestion. PCCP prioritizes both source and transit traffic but here the limitation of handling multiple sensed data within a node also remains. Besides these, CCF (Congestion Control and Fairness) [3] CODA [4] (Congestion Detection and Avoidance) [4], Fusion [5], Siphon [6] etc. are also remarkable congestion control technique for wireless sensor network but have the limitation of considering only single path congestion and homogeneous traffic.

III. DESIGN CONSIDERATIONS

This section describes the design considerations of our scheme taken into account when constructing the congestion control algorithm, in particular the network and queuing model with some definitions. Protocol. We assume that multiple routes have been established by any multipath routing protocol and path establishment is out of the scope of this paper.

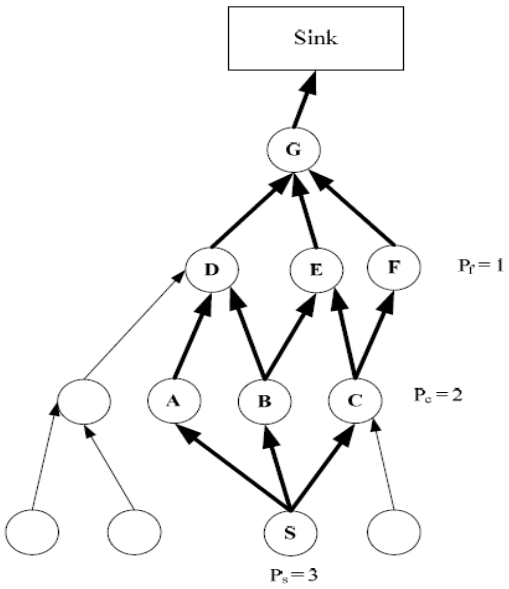

Fig.2: Network Model

In Figure 2 the highlighted links represents the established multipath route where a node is disseminating its traffic towards multiple parents (if any). We further assume that while establishing the route the sink dynamically assigns individual priority for the heterogeneous application data. Each sensor node can transmit route data of its children nodes as well as its originating data. So at any given time a sensor node may act as a source node and a forwarding node. We denote the number of the parent nodes as Pi. As shown in Figure 2, node S has 3 parent nodes, C has 2 and node F has 1.

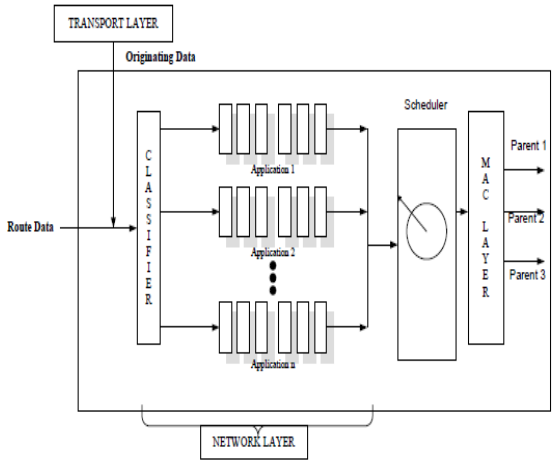

Fig.3: Queuing Model on a Particular Node.

3.1 Network Model

Here, we consider the congestion control for multi-hop multi path routing. The network model is shown in Figure 2, where each node can sense heterogeneous application data simultaneously. In our protocol we assume that every sensor node in the network has equal number and same types of sensors. All nodes are supposed to use CSMA like MAC protocol. We assume that multiple routes have been established by any multipath routing protocol and path establishment is out of the scope of this paper. In Figure 2, the highlighted links represents the established multipath route where a node is disseminating its traffic towards multiple parents (if any). We further assume that while establishing the route the sink dynamically assigns individual priority for the heterogeneous application data. Each sensor node can transmit route data of its children nodes as well as its originating data. So at any given time a sensor node may act as a source node and a forwarding node. We denote the number of the parent nodes as Pi. As shown in Figure 2, node S has 3 parent nodes, C has 2 and node F has 1.

3.2 Queuing Model

Figure 3, depicts the queuing model on a particular node for multipath routing. We assume that each node *i* has *n* number of equal sized queues for *n* types of data. For example, if a sensor node has 3 sensors for sensing temperature, light and humidity then it will have 3 separate queues for each of the sensory data. As shown in the Figure 3, a classifier has been provisioned in network layer. The purpose of this classifier is to classify the heterogeneous traffic of both originating and route data and place them in their corresponding queue. It can easily perform that by looking in the packet header which includes the type of data it carries.

The further description of queuing model proceeds through the following definitions:

1) Originating Rate: The rate at which the sensor node originates data is known as originating rate denoted a I *or* R for
node i .

2) Scheduling rate: In our protocol we introduce a scheduler between network and MAC layer which maintains the queues as shown in Figure 3. We can define i *sch* R as – how many packets the scheduler schedules per unit time from the priority queues. The scheduler sends the packets to the MAC layer from which these are delivered to multiple parents.

3) Intra Queue Priority: The queues shown in Figure 3 are priority queues. More priority is given for route data than originating data because route data have already traversed several paths, so its loss causes more wastage of network resources. We denoted this priority as intra queue priority. The classifier can assign the priority between route data and originating data by examining the source address in the packet

IV. 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:**

1. Overload of the monitoring module by control treatments.
2. 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.

3. The failure detection can be delayed because Transmission times.
4. The failure of the monitoring module paralyzes the operation of the entire network.

V. 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.

VI. 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

VII. 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.

We propose an efficient scheme to perform multipath congestion control for heterogeneous traffic which avoids packet loss and thus enhances the probability of achieving the desired throughput of heterogeneous traffic. Our congestion detection mechanism is chosen based on packet service ratio. We have used packet service ratio for detecting congestion as well as performed hop-by-hop multipath congestion control based on that metric.

VIII. 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.

8.1 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.

8.2 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.

IX. SOFTWARE DESCRIPTIONS

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

X. 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).

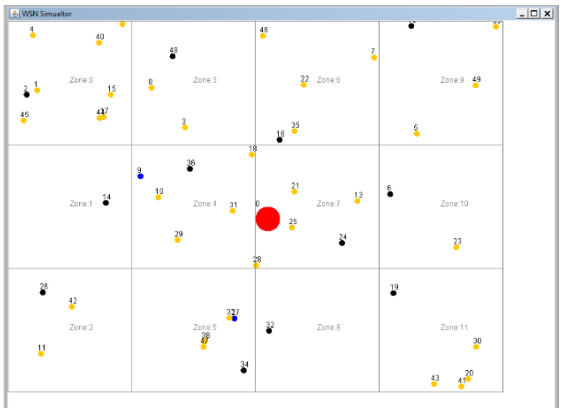

Fig.4: Network of Nodes

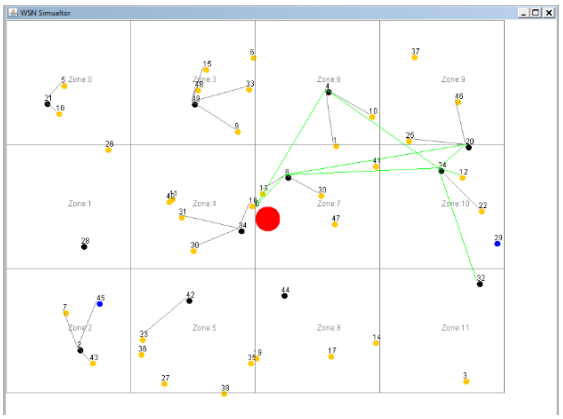

Fig.5: Construction of Path from Source to Sink.

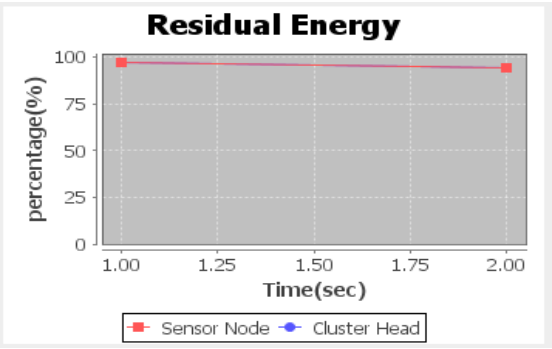

Fig.6: Initial Energy of the SN and CH.

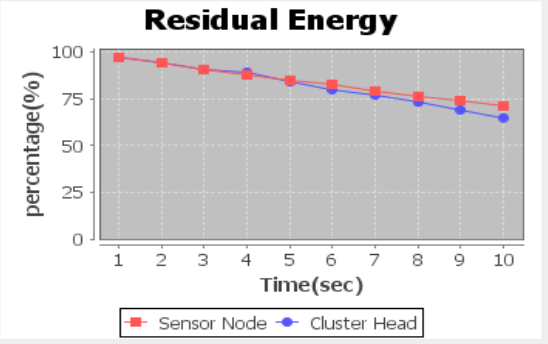

Fig.7: Energy of the CH decreases by Time.

XI. 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.

XII. CONCLUSION AND FUTURE WORKS

12.1 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.

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 and thus we have 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.

12.2 FUTURE WORK

In order to **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] Y.G.Iyer, S. Gandham and S. Venkatesan, "STCP: A Generic Transport Layer Protocol for Wireless Sensor Networks," Proc. IEEE ICCCN 2005. San Diego, CA, Oct. 17-19, 2005

[2] C. Wang et al., "Upstream Congestion Control in Wireless Sensor Networks Through Cross-Layer Optimization," IEEE Journal on Selected Areas in Communications, Vol.25, No.4, May 2007.

[3] C.T. Ee and R. Bajcsy, "Congestion control and fairness for many-toone routing in sensor networks," in Proc. ACM Sensys, Nov. 2004.

[4] C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, "CODA: Congestion detection and avoidance in sensor networks," in Proc. ACM SenSys, Nov.2003.

[5] B. Hull, K. Jamieson, and H. Balakrishnan, "Mitigating congestion in wireless sensor networks," in Proc. ACM Sensys, Nov. 2004.

[6] C.-Y. Wan, S. B. Eisenman, A. T. Campbell, and J. Crowcroft, "Siphon: Overload traffic management using multi-radio virtual sinks in sensor networks," in Proc. ACM SenSys, Nov. 2005. [7] C. Wang, B. Li, K. Sohraby, M. Daneshmand, and Y. Hu, "A Survey of transport protocols for wireless sensor networks," IEEE

Network, vol.20, no. 3, pp. 34-40, May/June 2006. ISBN

[7] 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.

[8] 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.

[9] 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.

[10] 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.

xxxxxx