# A Novel Approach Based Anomaly Detection for Secure Data Aggregation Using HEED Algorithm

S.Kannadhasan[1] J.Sangeetha[2] K.Niranjana[3]

*Abstract:-***Secure Data aggregation in wireless sensor networks (WSNs) have challenging task in Wireless Sensor Networks. WSN have numerous nodes with limited energy in a particular area are the major issues is increasing the network life time. In this paper, we propose the system monitoring modules and intrusion detection modules in WSN. We propose an HEED Algorithm based mechanism to detect false injected data for the following have challenging high potential, high packet loss rate, harsh environment, and sensing uncertainty. HEED Algorithm to create effective local detection mechanisms based the theoretical threshold. We conduct experiments and simulations to evaluate local detection mechanisms under different aggregation functions. Our proposed technique has improved the throughput with reduced packed drop, less number of packet delivery ratio and also less energy consumption in these networks. Our Technique is evaluated through NS2 Network Simulator.**

**Keywords: Intrusion Detection, WSN, HEED Algorithm**

## I.INTRODUCTION

Wireless Sensor Networks are used in many applications in military, data gathering, intrusion and detection monitors a network and so on [1]. Security design like prevention based and detection based are factors used in wireless sensor networks. Prevention based techniques are encryption; authentication etc. to the wireless sensor networks cannot apply with the limited number of resources and broadcast medium. Detection technique is used to identify the attacks in the WSN. There are two different kinds detection technique: anomaly based and signature based. In this paper we will focus the anomaly based detection technique. Most of the WSN researches based on homogeneous and heterogeneous network [2]. In homogeneous networks, all the sensor nodes have the same capability and the heterogeneous network; all the sensor nodes may be varying capabilities in wireless sensor networks.

## II. RELATED WORK

A few protocols only consider secure in-network aggregation based on a prevention-based scheme, in which encryption, authentication, and key management are used. Secure data aggregation is used to reduce the communication overhead in wireless sensor networks. Many aggregation protocols have been proposed to consider secure in-network aggregation based on a prevention-based scheme, in which encryption, authentication, and key management are used. The problem of information aggregation was tackled in which one node is compromised. The protocol might be vulnerable if both a child node and its parent node are compromised. A secure data aggregation protocols frame work was proposed for arbitrary aggregator topologies and multiple malicious nodes was discussed. Wagner used statistical estimation to design more resilient aggregation schemes against malicious data injection attacks.

## III. PROPOSED SYSTEM

Secure hop-by-hop data aggregation protocol based on principles of divide-and conquers and commit-and-attest was then proposed. Wagner used statistical estimation to design more resilient aggregation schemes against malicious data injection attacks .In this paper; we have propose the integration of system monitoring modules and intrusion detection modules in WSNs . We propose an HEED Algorithm based mechanism is used to find the false injected data. HEED Algorithm is used to predict their neighbor networks for each node to transmitted aggregated values. The following challenges occurred in wireless sensor networks have high potential, high packet loss rate, harsh environment, and sensing uncertainty. We illustrate how to use HEED to create effective local detection mechanisms with a theoretical threshold. Overcome the Local detection mechanism using algorithm of combining cumulative summation and generalized likelihood ratio to increase detection sensitivity. Our proposed local detection approaches work together with the system monitoring module to differentiate between malicious events and emergency events under different aggregation functions.

*Manuscript received Mar, 2014.*

*[1] Assistant Professor, Department of ECE, Raja College of Engineering and Technology, Madurai, Tamilnadu, India*

*[2] U.G Student, Department of ECE, Raja College of Engineering and Technology, Madurai, Tamilnadu, India*

*[3] U.G Student, Department of ECE, Raja College of Engineering and Technology, Madurai, Tamilnadu, India*

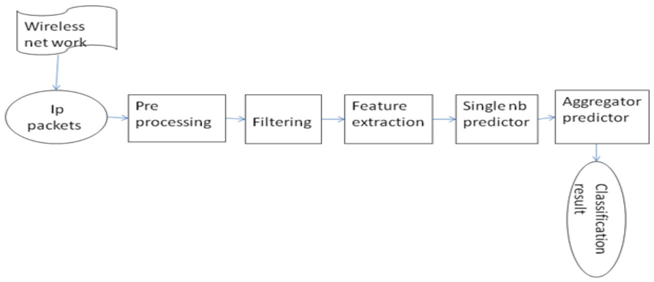

**Figure 1: Block Diagram of Proposed Work**

- ❖ IDM and SMM should work together to provide intrusion detection capabilities for WSNs.
- ❖ To increase detection sensitivity, we further applied.
- ❖ Together with SMM to differentiate between malicious events and emergency events.
- ❖ Also a number of proposed protocols aim to ensure the secrecy and authentication of data

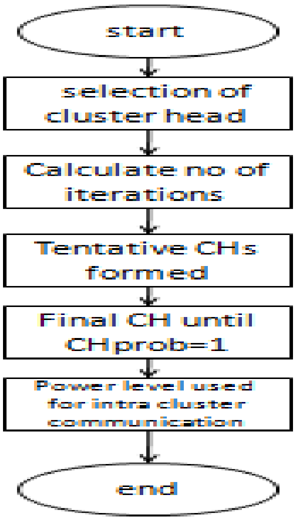
start
selection of cluster head
Calculate no of iterations
Tentative CHs formed
Final CH until CHprob=1
Power level used for intra cluster communication
end

**Figure 2: Flow Chart of Heed Algorithm**

```
1: Compute $yk= zk − ˆx−k$ at time $tk$
2: Compute $\mu ˆ 1 = 1w\_ki=k−w+1\ yi$ when $k \geq w − 1$
3: Compute $SN = b\sigma\_N\ i=0(yi −\mu 0 −v/2) = b\sigma Ni=0(yi −v/2)$
4: if ($SN > h$) then
5: $A$ raises an alert on $B$;
6: else
7: $A$ thinks that $B$ functions normally;
8: end if
```

## IV. RESULTS AND DISCUSSION

**Table 1: Simulation Parameters of Anomaly Detection**

The Energy Efficient Performance based secure data transmitted using HEED Algorithm.

| SIMULATION PARAMETER | SIMULATION VALUES |
|---|---|
| Simulation standard | IEEE 802.15.4 |
| Antenna type | Wireless/Two ray ground |
| Antenna orientation | Omni directional |
| Layer | Link layer |
| Simulation range | 1500m * 1500m |
| No of nodes | 23 |
| Base protocol | Adhoc on demand vector |
| Algorithm | Heed Algorithm |
| Channel | Wireless channel/physical |

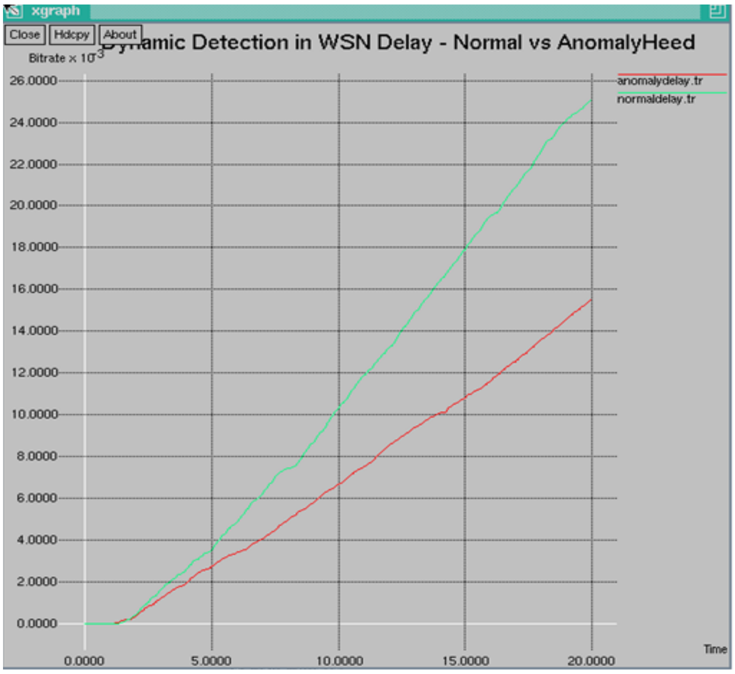

**Figure 2: Packet Drop**

The numbers of valid packets are dropped in the malicious nodes shows in the figure 2.

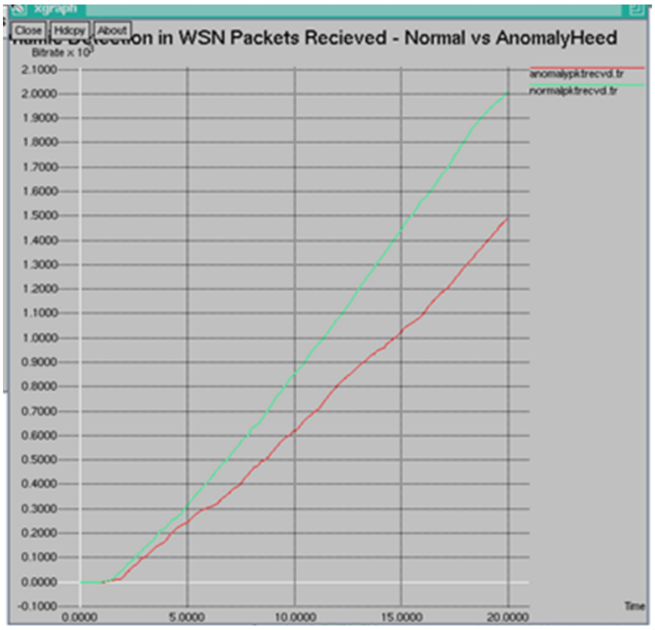

**Figure 3: Packet Delivery Ratio**

From the Figure 3 shows that the number of packets received for the total number of packets transmitted.

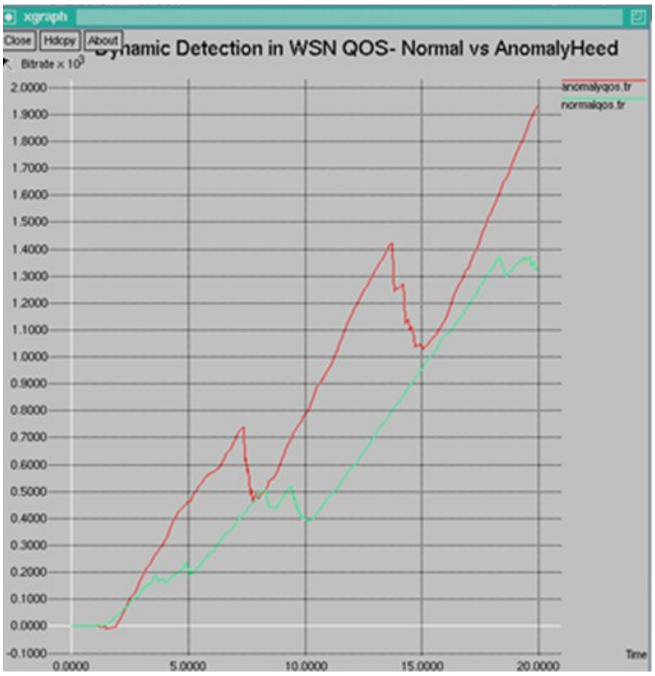

**Figure 4: Quality of Services**

Figure 4 shows the Quality of Services of Normal Vs Anomaly Detection using Heed Algorithm

## V. CONCLUSION

Wireless Sensor Network has the challenge energy consumption of nodes have higher to increase the network life time in wireless sensor networks. The proposed technique which considers parameters like packed drop, packet delivery ratio, secure data transmitted, energy consumption using HEED Algorithm to classifies anomaly detection of the given sensor nodes in wireless sensor networks. Simulation results show that the proposed technique has lesser amount of energy consumption which results in increase of network life time.

## REFERENCES

[1] Bo Sun, Member, IEEE, Xuemei Shan, Kui Wu, Senior Member, IEEE, and Yang Xiao, Senior Member, IEEE,” Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks”, IEEE SYSTEMS JOURNAL, VOL. 7, NO. 1, MARCH 2013

[2] M. Basseville and I. V. Nikiforov, Detection of Abrupt Changes: Theory and Application. Englewood Cliffs, NJ: Prentice-Hall/Simon and Schuster Company, 1993.

[3] D. Wagner, “Resilient aggregation in sensor networks,” in Proc. ACMSASN, 2004, pp. 78–87.

[4] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An interleaved hop-by hop authentication scheme for filtering false data injection in sensor networks,” in Proc. IEEE Symp. Security Privacy, May 2004, pp. 260– 272.

[5] C. Castelluccia, E. Mykletun, and G. Tsudik, “Efficient aggregation of encrypted data in wireless sensor networks,” in Proc. MOBIQUITOUS, Jul. 2005, pp. 109–117.

[6] H. Cam, S. Ozdemir, P. Nair, and D. Muthuavinashiappan, “Espda: Energy efficient and secure pattern-based data aggregation for wireless sensor networks,” in Proc. IEEE Sensors, Oct. 2003, pp. 732–736.

[7] B. Krishnamachari and S. Iyengar, “Distributed Bayesian algorithms for fault-tolerant event region detection in wireless sensor networks,” IEEE Trans. Comput., vol. 53, no. 3, pp. 241–250, Mar. 2004.

[8] T. Clouqueur and K. Saluja, “Fault tolerance in collaborative sensor networks for target detection,” IEEE Trans. Comput., vol. 53, no. 3, pp. 320–333, Mar. 2004.

[9] D. Dong, Y. Liu, and X. Liao, “Self-monitoring for sensor networks,” in Proc. ACM MobiHoc, May 2008.

[10] J. Lin, L. Xie, and W. Xiao, “Target tracking in wireless sensor networks using compressed KF,” Int. J. Sensor Netw., vol. 6, nos. 3–4, Nov. 2009.

[11] K. Premkumar, A. Kumar, and J. Kuri, “Distributed detection and localization of events in large ad hoc wireless sensor networks,” in Proc. 47th Annu. Allerton Conf. Communications Control Comput., Sep.–Oct. 2009, pp. 178–185.

[12] I. Krontiris, Z. Benenson, T. Giannetsos, F. C. Freiling, and T. Dimitriou, “Cooperative intrusion detection in wireless sensor networks,” in Proc. 6th EWSN.