International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 5 (2013), pp. 451-458

http://www. irphouse.com /ijict.htm

# Performance Analysis of Heterogeneous Wireless Sensor Network in Environmental Attack

**Manali Singh[1], Khushbu Babbar[2] and Kusum Lata Jain[3]**

*Computer Science Department, Banasthali University*
*C-62, Sarojini Marg, C-Scheme, Jaipur, India.*

**Abstract**

Wireless sensor networks have gained considerable attention in the past few years. They are being used in the domains of battlefield communication, homeland security, pollution sensing, and traffic monitoring. In wireless sensor network (WSN), nodes can be easily compromised by the attacker when deployed in a hostile environment due to the constraints such as limited battery lifetime, memory space and computing capability. This paper presents a performance analysis of a heterogeneous wireless network when attacker changes the environmental values by an artificial event or a miscellaneous node. An attacker forces the node to transmit more sensed data to base station. Attacker produces an event in environment due to which nodes have to sense the environment more than once in the same round that increase the power consumption of the node. This interrupts reduces the network life time and network nodes are not able to perform their function of data collection and reporting to Base Station properly. This paper presents the simulation results on MATLAB. Simulation results show that network lifetime is decreases as the event occur in network.

**Keywords**: WSN, environmental attack, network lifetime, power consumption, base station.

## 1. Introduction

Wireless Sensor networks (WSNs) is a new paradigm of ambient monitoring with many potential applications in the field of mass public and military. The sensing technology combined with processing power and wireless communication makes it

lucrative for being exploited in abundance in future. This network is formed by thousands of small dimension nodes which communicate to Base Station using ad-hoc wireless network and are very much limited by computational, memory and energy resources. The main objective of the sensor nodes is to collect information from its surrounding environment and transmit it to sink, called base station (BS). BS analyzes the gathered information.

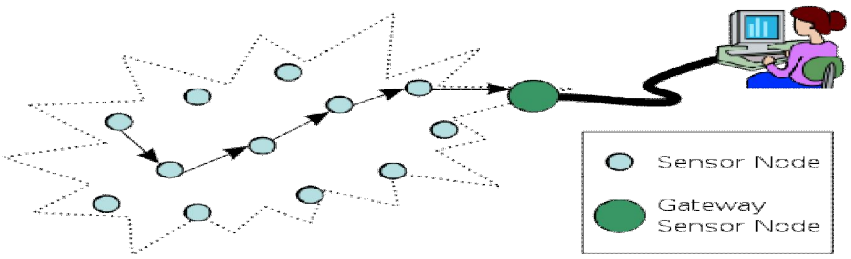


**Fig. 1**: Overview of Wireless Sensor Network.

Because nodes are generally deployed in harsh and hostile terrain so are at risk of physical distortion. Due to this intrinsic nature of networks, WSN becomes vulnerable to many security attacks. This paper presents an attack where intruder forces the sensors to remain awake even after completing their work of sensing environment once in each round so that these sensors waste their energy. Here the attacker changes the environmental values by an artificial event or a miscellaneous node and forces the nodes to transmit more sensed data to base station. So there is large power consumption by limited powered sensor nodes. This interrupt reduces the network life time and network nodes are not able to perform their function of data collection and reporting to Base Station properly because they sense wrong data and also they get dead in very early stages of network life time. This gives rise to DoS (Denial of Service) through Denial of Sleep. This paper presents the simulation result of different scenario for network.

The rest of the paper is structured as follows. In section 2, we briefly review the need of security and approaches for detecting malicious WSN node detection. Section 3 describes the simulation parameters and assumptions made. Section 4 presents the experimental setup and simulation results. Section 5 concludes this paper by describing the summary of results obtained.

## 2. Related Work

Energy is one of the most crucial resources for battery powered in wireless sensor network. Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. Various protocols are available to route the data from node to base station in WSN in an energy

efficient way, enhancing the network survivability. Once the node uses up all its energy, it can no longer perform sensing task and is termed as dead node. WSN are often deployed in a hostile environment and work without human supervision, individual nodes can be easily compromised due to limitations of computational, memory and energy resources. There are number of attacks that can be launched against a WSN when certain number of sensor nodes has been compromised. some of these attacks are HELLO flooding attack, sink hole attacks, Sybil attack, black hole attack, worm hole attacks , Dos attacks. So security in WSN is one of the most important topics in WSN research community. It becomes critical to detect and isolate compromised nodes in order to avoid being misled by the falsified information injected by the adversary and also work in power saving mode. Researchers have suggested detecting malicious node using signal strength. In this every node monitors its surroundings and whenever a transmission is detected by a sensor node, it would check if the signal strength of the transmitting node is compatible with originator' node's geographical position. But this approach introduces large overhead so is not efficient. Karlof and Wagner suggested to construct efficient random sampling mechanism and interactive proofs, then user can verify that the answer given by the aggregator is good approximation of the true value even when a fraction of sensor nodes are compromised.

## 3. Network Preliminaries for the Proposed Work

Simulation is performed in MATLAB. In simulation network 100 nodes are deployed in uniform random distribution. The network is a heterogeneous network in terms of energy. Each of these nodes is assigned with random energy to create a heterogeneous WSN. The network works in rounds. In each round the nodes send the sensed data to the base station. Energy model is used as LEACH. A malicious environment node is introduced in the system on random basis. This malicious node produces an event in environment due to which nodes need to sense the environment more than once in a round that increase the power consumption of the node. The number of rounds in which this intrusion effect is forced on nodes is selected randomly. This interrupts reduces the network life. Network lifetime is round in which first dead node occurs in the network and used as performance criteria. The nodes get dead at early stages of network life time and also falsified information is injected by the adversary.

## 4. Simulation Parameters

Table 1 shows the simulation parameters.

**Table 1**: Simulation Parameters.

| **Parameter** | **Values** |
|---|---|
| Simulation Round | 1000 |
| Topology Size | 200 x 200 |
| Number of nodes | 100 |
| Initial node power | Random |
| Nodes Distribution | Nodes are uniformly randomly distributed |
| Energy for Transmission (ETX) | 50*0.000000001 |
| Energy for Reception (ERX)/ Sensing Energy | 50*0.000000001 |
| Energy for Data Aggregation (EDA) | 5*0.000000001 |

## 5. Simulation Results

Simulation shows the following results in different scenario

### 5.1 When number of rounds in which intrusion occurs varies:

In 10 runs of simulation scenario with the malicious environment simulation results shows that network life is decreases as the number of random round is increased. Table 2 and Fig.2 shows the result of effect on first dead node by varying the intruded rounds.

**Table 2**: First dead node' round number with variation in intrusion rounds.

| Simulation run | First dead when no malicious environment introduced | When malicious environment is introduced | | |
|---|---|---|---|---|
| | | First dead for 100 random rounds of intrusion | First dead for 200 random rounds of intrusion | First dead for 300 random rounds of intrusion |
| 1 | 463 | 77 | 93 | 55 |
| 2 | 396 | 81 | 84 | 70 |
| 3 | 307 | 52 | 85 | 68 |
| 4 | 345 | 72 | 72 | 66 |
| 5 | 276 | 130 | 80 | 73 |
| 6 | 301 | 51 | 57 | 85 |
| 7 | 279 | 62 | 64 | 90 |

| | | | | |
|---|---|---|---|---|
| 8 | 368 | 56 | 87 | 71 |
| 9 | 466 | 95 | 72 | 67 |
| 10 | 277 | 80 | 61 | 64 |

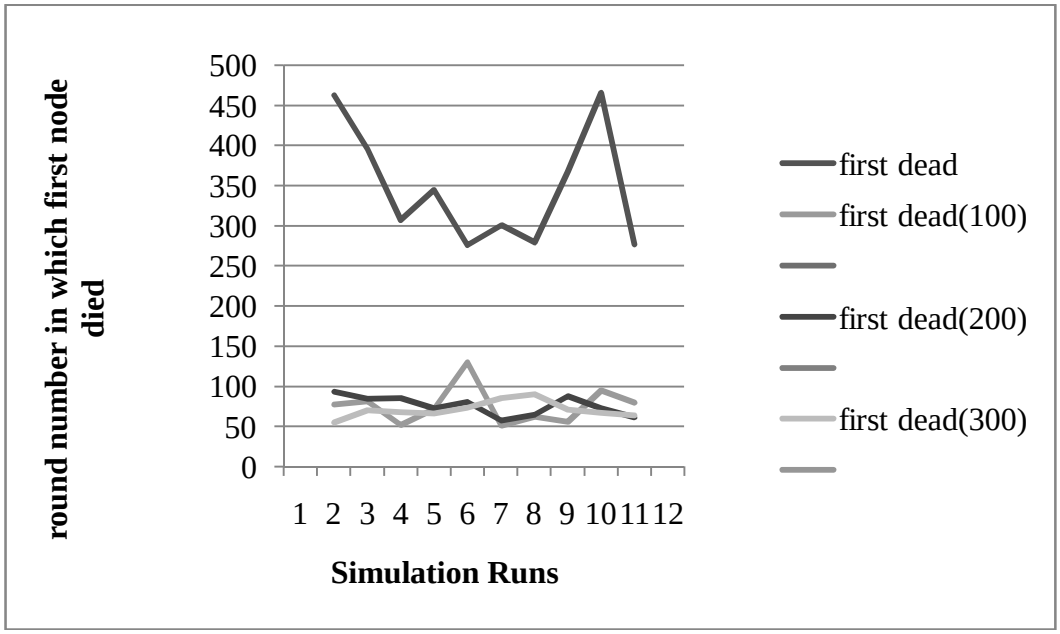


**Fig. 2**: First dead node' round number with variation in intrusion rounds.

**5.2 When number of time malicious event is sensed by nodes:**
In this scenario, attacker forces all the nodes to sense data more than once instead of one. Table 3 and Fig 3. Shows the result of effect on first dead by varying number of times malicious event is sensed.

**Table 3**: Effect on first dead node by varying times of event sensing.

| Simulation run | First dead when no malicious environment | When malicious environment is introduced | | |
|---|---|---|---|---|
| | | First dead for 5 times event sensing | First dead for 4 times event sensing | First dead for 3 times event sensing |
| 1 | 463 | 77 | 75 | 220 |
| 2 | 396 | 81 | 76 | 112 |
| 3 | 307 | 52 | 84 | 218 |
| 4 | 345 | 72 | 60 | 201 |
| 5 | 276 | 130 | 72 | 154 |

| | | | | |
|---|---|---|---|---|
| 6 | 301 | 51 | 143 | 123 |
| 7 | 279 | 62 | 99 | 180 |
| 8 | 368 | 56 | 88 | 184 |
| 9 | 466 | 95 | 69 | 166 |
| 10 | 277 | 80 | 89 | 101 |

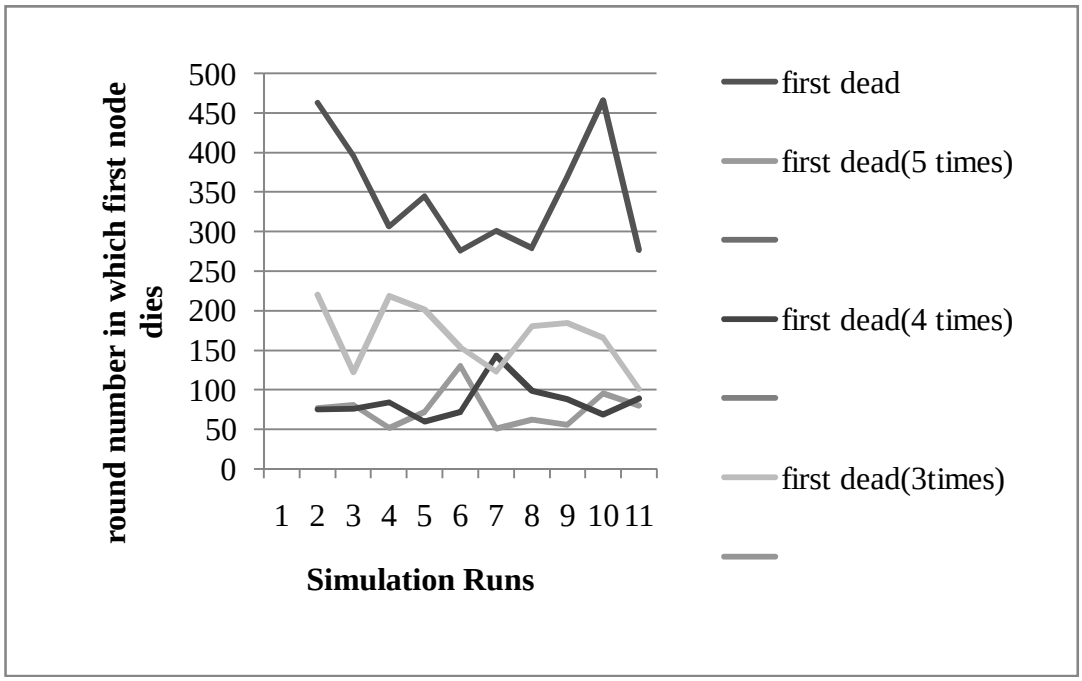


**Fig. 3**: Effect on first dead node by varying times of event sensing.

## 6. Conclusion

In this paper, we have shown the effect of malicious environment on heterogeneous WSN. The basic idea is that when malicious event is introduced, working of sensors gets interrupted because of which the sensors are not able to perform their work of data collection properly and die in very early stages of network life. According to results obtained, it is observed that when no malicious environment was introduced, the first node died at minimum of 276 round and maximum of 466 round but after introducing malicious environment, first node died at minimum 51, 57 and 55 round number and maximum 130, 93 and 90 round number for 100,200 and 300 random rounds respectively in which interruption occurred. And first dead node was obtained at minimum 51, 60 and 101round number and maximum of130, 143 and 220 round number for varying number of times event was sensed as 5 times, 4 times and 3 times respectively. This means that a node has been compromised or is out of function which compromises the security of data also.

## References


[1] B.Sun, K.Wu and U. Pooch(2002), Secure Routing against Black-hole Attack in Mobile Ad Hoc Networks, *Proceedings of Communication and Computer Networks*

[2] C. Karlof and D. Wagner(2003), Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, *Journal of Ad Hoc Networks, Elsevier.*

[3] Idris M.Atakli, Hongbing Hu, Yu Chen,Wei-Shinn Ku and Zhou Su(2008), Malicious node detection in Wireless Sensor Networks using Weighted Trusted Evaluation, *SpringSim*

[4] J.Newsome, E.Shi, D.Song and A. Perrig(2004), The Sybil Attack in Sensor Networks: Analysis and Defense, *International Symposium on Information Processing in Sensor Networks*, **1**.

[5] OMKAR Pattnaik, Sasmita Pani(2012), Application of IDS in WSN: a survey , *IJRCCT*, **7,** *1,*

[6] Meena Malik, Dr. Yudhvir Singh and Anshu Arora(2013), Analysis of LEACH protocol in Wireless Sensor Networks, *International Journal of Advanced Research in Computer Science and Software Engineering*, **3**, *2.*

[7] M.S. Islam and S.A. Rahman(2011), Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches, *International Journal of Advanced Sciences and Technology*, **36**, pp 1-8

[8] Nabil Ali Alrejah, S.Khan and Bibal Shams (2013), Intrusion Detection Systems in Wireless Sensor Networks: a review, *International Journal of Distributed Sensor Networks*.

[9] Raymond and David R.(2008), Denial-of-service in Wireless Sensor Networks: Attacks and Defenses, *Pervasive Computing, IEEE*, **7**, *1*.

[10] Siebe Datema(2005), A case study of Wireless Sensor Network attacks, *Delft University of Technology*.

[11] S. Khan, K. K. Loo, and Z. U. Din(2010), Framework for intrusion detection in IEEE 802.11 wireless mesh networks, *International Arab Journal of Information Technology*, **7**, *4*, pp. 435–440.

[12] W.Junior, T. Figueriredo, H.C. Wong and A. Lourier(2004), Malicious Node Detection in wireless Sensor Networks, *the 18th International Parallel and Distributed Processing Symposium (IPDPS"04).*

[13] Y.Hu, A.Perrig and D.johnson(2003), Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, *IEEE INFOCOM*.