Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.633 – 638

RESEARCH ARTICLE

Analysis of Dead Node in Wireless Sensor Network Denial of Sleep Attack

Sunita Devi[#1], Anshul Anand[*2]

[1] Shri Baba Mastnath Engineering College
Asthal Bohar, Rohtak, MDU
Haryana (India)
sunitalather.lather@gmail.com

[2] Shri Baba Mastnath Engineering College
Asthal Bohar, Rohtak, MDU, Haryana
Anshulnnd9@gmail.com

Abstract: With the progression of computer networks extending boundaries and joining distinct locations, wireless sensor networks (WSN) comes as a new frontier in developing opportunities to collect and process data from remote locations. Usually, some nodes act maliciously and they are able to do different kinds of DoS attacks. Due to this attack, the nodes consume more energy and the sensor nodes are powered up with batteries but due to unattended nature of arrangement, the sensor nodes cannot be recharged again. This paper analyses the dead nodes of wireless sensor networks to prevent the occurrence of Denial of Sleep Attack.

Keywords: Wireless Sensor Network, Denial of Sleep Attack, Dead Node, Security, Energy

I. Introduction

A wireless sensor network (WSN) is a network which is used to monitors the physical conditions, like temperature, sound, pressure etc or environmental. It is also used to cooperatively pass their data through the network to a main location.

The wireless sensor networks was motivated by military applications such as battlefield surveillance; in present time such networks are used in many industrial such as industrial process monitoring and consumer applications such as control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors.[13][14][15].In this one node is called sensor node and another node is called gateway sensor node.

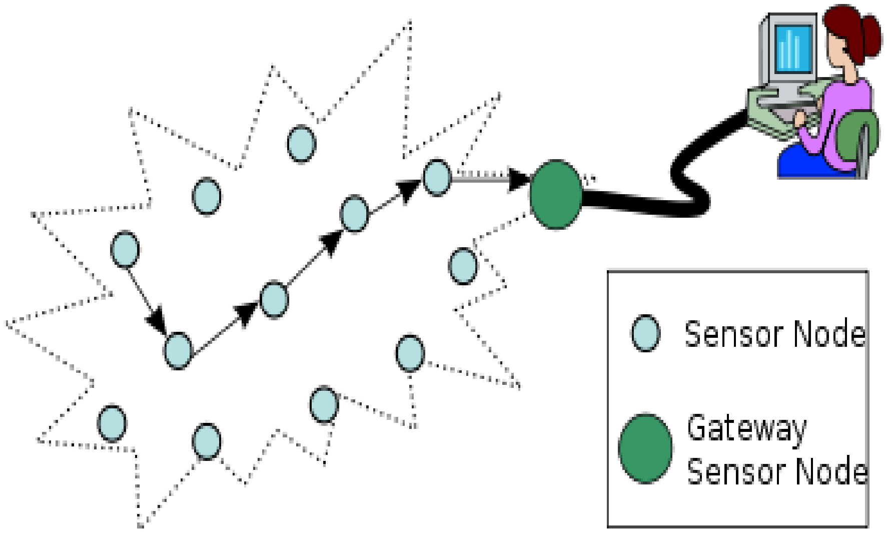

Figure: 1. Architecture of Wireless Sensor Network. [13]

1.1. The main components of sensor node:

- **Controller:** It is responsible for performing tasks, processing data and controlling the functionality of other components in the sensor node.
- **Transceiver:** The transceiver is the combination of transmitter and receiver. Transceivers often lack of unique identifiers. The states of transceiver are transmitting, receive, idle, and sleep.
- **External Memory:** There are two categories of memory based on the purpose of storage are user memory which is used for storing application related or personal data, and program memory which is used for programming the device. It also contains identification data of the device if present.
- **Power Source**: The wireless sensor nodes are placed at very far locations so it is not possible to charge them. This task is very costly and inconvenient. The sensor node needs power for sensing, communicating and data processing. Batteries are the main source of power supply for sensor nodes such as rechargeable and non-rechargeable
- **Sensors:** These are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure. Sensors measure physical data or environmental data of the parameter to be monitored.[13]

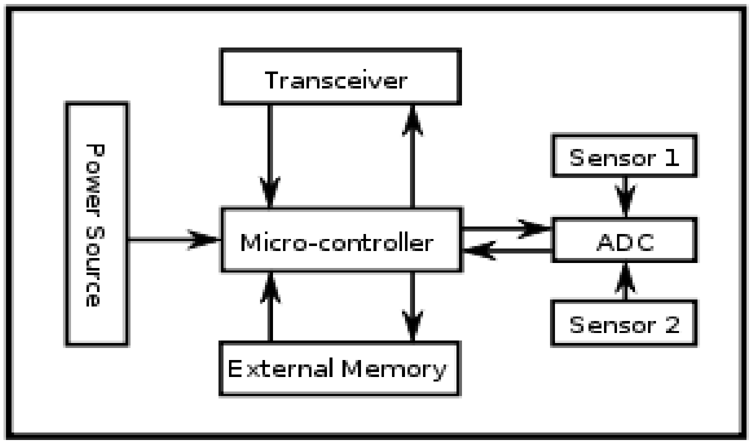

Figure 2: Components of Wireless Sensor Network.

1.2 Applications of Wireless Sensor Network:[1]

a) Structural Health Monitoring
b) Data logging
c) Machine health monitoring
d) Water quality monitoring
e) Landslide detection

f) Forest fire detection
g) Air pollution monitoring
h) Area monitoring
i) Health care monitoring
j) Natural disaster prevention

1.3 <u>Denial of Sleep attack:</u>

Attacks which target the battery exhaustion of nodes are known as attacks on “system lifetime.” Attacker would bother which can be explained with this example: Suppose, a sensor network is arranged as an early-warning system for biological or chemical attacks. The sensor network is widely distributed so it would be almost impossible for a terrorist to physically destroy it. An easier solution would perhaps be to add a few misbehaving nodes that stress the legitimate sensors to work continuously until their batteries are totally exhausted. Then the terrorist could proceed with his real-world attack, undetected.

There is a difficult ways in the case of sensor networks. These devices play three roles: one as data collectors, second as processors and third as forwarders. The goal of the network is to work as long as possible, so that information can be transfer from the objects to the sinks. But in order to stay active for a longer lifetime, the objects “want” to participate in the network as little as possible. Because of this the nodes are conflicted and set the stage for battery attacks. Weak forms of denial of sleep attack are selfish behavior and “unfairness” in cooperative protocols and there are many others more advanced such as sleep deprivation attacks. LLP for channel arbitration can even be manipulated to exhaust batteries or simply degrade network performance. Such as:

Channel jamming which make nodes, retransmit data and increase transmission power to overcome noise.

Interrogation is another point. In this, a selfish node may continuously request channel reservation. In cooperative medium access control protocols neighbor nodes are forced to reply to those requests and thus eventually consume all their energy reserves. [1][3][12]

II. LITERATURE REVIEW

Various researches had been node in the area of wireless sensor network.

Michael Brownfield models the network lifetimes of leading WSN medium access control (MAC) protocols, and proposes a new MAC protocol. David R. Raymond uses simulation to examine tradeoffs and to demonstrate the potential benefits of the CARL mechanism providing support for adaptive rate-limiting at the MAC layer.[1][2]

Denial of Sleep Attack is a subset of Denial of Service Attack. Christoph Krauß studied denial of service attack and discuss possible solutions to prevent false exclusions of non-compromised nodes and propose an extended scheme.[3] Maryam Mohi models the interaction of nodes in WSN and intrusion detection system (IDS) as a Bayesian game formulation and use this idea to make a secure routing protocol.[5] Maneesha V. Ramesh performed work using symmetric-key algorithm instead of NN for detecting DoS attack.[7]

Manju.V.C performed a work," Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks" which refer to denial of sleep attack and propose effective solution to defend against this attack on a sensor network.[12]

III.PROPOSED WORK

In this paper, we are presenting a new approach to detect and prevent denial of sleep attack by analyses the dead node in wireless sensor network. The presented work is performed in a clustered network and it includes three phases:

- In first phase, the analysis within the cluster will be performed by analyzing the number of communication and the time constraint to analyze the energy reduction rate of a node. If the energy reduction rate is abnormal, will identify the particular node or the cluster as the infected node or cluster.
- In second stage, it tries to handle the node at the cluster level by blocking the node. The particular cluster will be analyzed again to identify the energy consumption over that cluster.
- If it is more than average then in third stage, re-clustering will be performed by considering that all nodes will not again form the same cluster.

The presented work gives the balanced formation of the clusters over the network and provide the equalize consumption of energy over the clusters. The presented work includes the detection as well as prevention approach to take the quick decision so that the network life will be improved. The presented work is effective to improve the network life. The work is implemented in matlab environment.

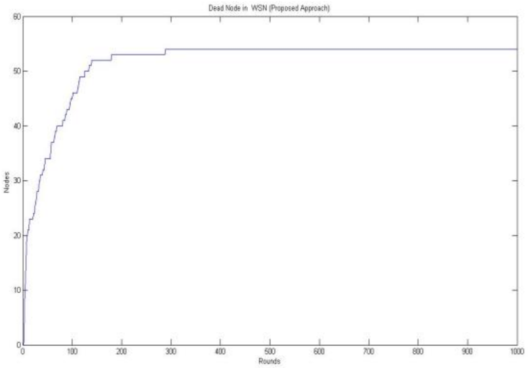

Figure 3 .Dead Node Analysis (Proposed Approach)

Figure 3 showing the dead node analysis in proposed approach. Here x axis represents the rounds and y axis represents the nodes over the network. The curve over the graph is showing the dead node occurrence over the network. Initially No node is dead but as the communication is performed, nodes start losing the energy. As shown in the figure, upto 300 rounds all nodes get dead.

IV. SIMULATION RESULTS

The simulation scenario parameters of presented work are listed here under

Parameter	Value
Number of Nodes	100
Probability of Selection	.1
Energy	0.5
Transmission Energy	50*0.000000001
Receiving Energy	50*0.000000001
Forwarding Energy	10*0.000000001
Topology	Random

Table1.Simulation Scenario Parameters

The results of existing work in which standard energy based approach is defined for election of centroid. The graph related to dead nodes.

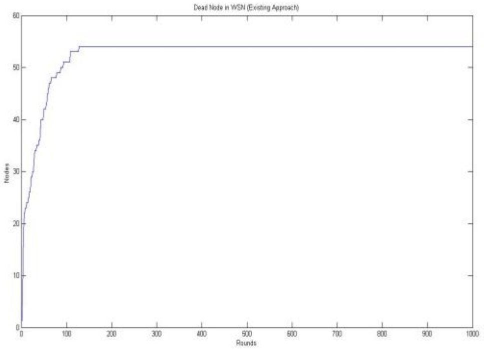

Figure 4.Dead Node Analysis (Existing Approach)

Figure 4 showing the dead node analysis in existing approach. Here x axis represents the rounds and y axis represents the nodes over the network. The curve over the graph is showing the dead node occurrence over the network. Initially No node is dead but as the communication is performed, nodes start losing the energy. As shown in the figure, upto 150 rounds all nodes get dead.

The dead node analysis of existing and proposed approach is shown in table 2.

	Existing	Proposed
0	0	0
100	48	44
200	52	52
300	54	52
400	54	53
500	54	54
600	54	54
700	54	54
800	54	54
900	54	54
1000	54	54

Table2. Dead Node Analysis (Existing Vs. Proposed)

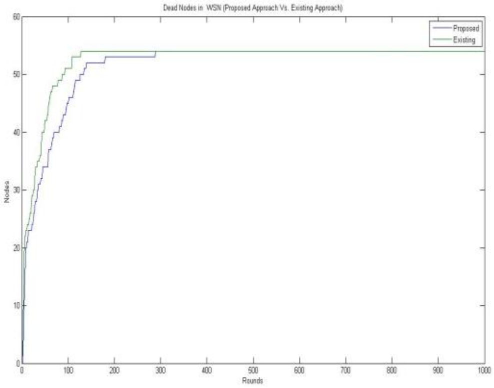

Figure 5.Dead Node Analysis (Existing Vs. Proposed)

Figure 5 showing the dead node analysis in existing approach. Here x axis represents the rounds and y axis represents the nodes over the network. The curve over the graph is showing the dead node occurrence over the network. As shown in the figure, in existing approach nodes start getting dead earlier to the proposed approach and life of network in proposed work is improved.

V. CONCLUSION

In this paper, we analyses the dead node in wireless sensor network for denial of sleep attack. Here initially no node is dead but as the communication is performed, nodes start losing the energy and increase the rounds when all nodes dead.

ACKNOWLEGEMENT

The work presented here is carried out using MATLAB environment at Shri Baba Mastnath Engineering College Rohtak, Haryana, India.

REFERENCES

[1] Michael Brownfield," Wireless Sensor Network Denial of Sleep Attack", Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY 0-7803-9290-6/05@2005 IEEE

[2] David R. Raymond, " Clustered Adaptive Rate Limiting: Defeating Denial-of-Sleep Attacks in Wireless Sensor Networks", 1-4244-1513-06/07@ 2007 IEEE

[3] Christoph Krauß," An Enhanced Scheme to Defend against False-Endorsement-Based DoS Attacks in WSNs", IEEE International Conference on Wireless & Mobile Computing, Networking & Communication 978-0-7695-3393-3/08© 2008 IEEE

[4] Chakib BEKARA," Mitigating Resource-draining DoS attacks on Broadcast Source Authentication on Wireless Sensors Networks", 2008 International Conference on Security Technology 978-0-7695-3486-2/08 © 2008 IEEE

[5] Maryam Mohi," A Bayesian Game Approach for Preventing DoS Attacks in Wireless Sensor Networks", 2009 International Conference on Communications and Mobile Computing 978-0-7695-3501-2/09 © 2009 IEEE

[6] Na Ruan," DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things", 2012 International Conference on Selected Topics in Mobile and Wireless Networking 978-1-4673-0937-0/12 ©2012 IEEE

[7] Maneesha V. Ramesh," Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks", 2012 Fourth International Conference on Computational Intelligence and Communication Networks 978-0-7695-4850-0/12 © 2012 IEEE

[8] Lynda Mokdad," Performance evaluation of security routing strategies to avoid DoS attacks in WSN", Globecom 2012 - Next Generation Networking and Internet Symposium 978-1-4673-0921-9/12©2012 IEEE

[9] Antoniel da Silva Rego," BEE-C: A Bio-inspired Energy Efficient Cluster-based Algorithm for Data Continuous Dissemination in Wireless Sensor Networks", ICON 2012 978-1-4673-4523-1/12©2012 IEEE

[10] D. Mansouri," Detecting DoS attacks in WSN based on Clustering Technique", 2013 IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS 978-1-4673-5939-9/13 ©2013 IEEE

[11] Roshan Singh Sachan," A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN", International conference on Communication and Signal Processing, April 3-5, 2013, India 978-1-4673-4866-9/13©2013 IEEE

[12] Manju.V.C," Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks", Proceedings of2013 IEEE Conference on Information and Communication Technologies (ICT 2013) 978-1-4673-5758-6/13 © 2013 IEEE

[13] http://en.wikipedia.org/wiki/Wireless_sensor_network

[14] http://en.wikipedia.org/wiki/Sensor_node

[15] http://www.rtcmagazine.com/articles/view/101228