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. 7, July 2014, pg.594 – 601

RESEARCH ARTICLE

Evaluation for Alive Node on 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: Wireless sensor networks (WSNs) have gained worldwide attention in recent years. Wireless sensor network consists o many nodes. Battery is the main power source in a sensor node. 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 this nature of arrangement, the sensor nodes cannot be recharged again. This paper evaluation the alive nodes of wireless sensor networks to prevent the occurrence of Denial of Sleep Attack.

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

I. INTRODUCTION

A wireless sensor network (WSN) is a network used to monitors the physical conditions, for example temperature, sound, pressure etc or environmental. Wireless sensor can be 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.

Figure 1: Wireless embedded network for precision agriculture. Sensors nodes detect light levels, temperature and soil moisture at hundreds of points across a field and communicate their data over a multi-hop network for analysis. [14]

This figure depicts a precision agriculture deployment. Here hundreds of nodes scattered throughout a field assemble together, establish a routing topology, and transmit data back to a base station (collection point). The application demands for scalable, low-cost, robust, and easy to deploy networks are perfectly met by a wireless sensor network. If any of the nodes would fail, a new topology would be selected and the overall network would continue to deliver data. If more nodes are situated in the field, they only create more potential routing opportunities. [14].

A Wireless Sensor Network typically has little or no infrastructure. It consists of sensor nodes (few tens to thousands) working together to monitor or track a region to obtain data about the environment. There are two types of WSNs:

- ✓ **Structured:** In this, all or some of the sensor nodes are deployed in a pre-planned manner. The positive point of a structured network is that fewer nodes can be deployed with lower network maintenance and management cost. Fewer nodes can be used now since nodes are placed at specific locations to provide coverage while ad hoc deployment can have uncovered areas.[15]

- ✓ **Unstructured:** It contains a dense collection of sensor nodes. Sensor nodes may be used in an ad hoc manner into the field. Once used, the network is left unattended to perform monitoring and reporting functions. In an unstructured WSN, network maintenance such as detecting failures and managing connectivity is difficult since there are so many nodes. [15]

1.1 System Evaluation Metrics:

There are some key evaluation metrics for wireless sensor networks such as lifetime, coverage, response time, temporal accuracy, security, and effective sample rate. Their importance is discussed below:

Lifetime: Expected lifetime is the critical to any wireless sensor network deployment. The goal of both security application and environmental monitoring scenarios is to have nodes placed out in the field, unattended, for months or years. [14]

Coverage: Coverage is the main evaluation metric for a wireless network. It is advantageous to have the ability to deploy a network over larger physical areas. [14]

Response time: System response time is a critical performance metric in our alarm application scenario. When an intrusion is detected, an alarm must be signaled immediately. Having low power operation, nodes must be capable of having immediate, high-priority messages communicated across the network as quickly as possible. [14]

Temporal accuracy: Samples from multiple nodes must be cross-correlated in time in order to determine the nature of phenomenon being measured in environmental and tracking applications. The accuracy of this correlation mechanism will depend on the rate of propagation of the phenomenon being measured. [14]

Security: Wireless sensor networks must be capable of keeping the information they are collecting private from eavesdropping. Despite the seemingly harmless nature of simple temperature and light information from an environmental monitoring application, keeping this information secure can be extremely important. [14]

Effective Sample Rate: The effective sample rate as the sample rate that sensor data can be taken at each individual sensor and communicated to a collection point in a data collection network. Fortunately, environmental data collection applications typically only demand sampling rates of 1-2 samples per minute. [14]

1.2 Applications of Wireless Sensor Network:[1]

WSN applications can be classified into two categories: monitoring and tracking (see Fig. 2):

i. Monitoring applications include outdoor/ indoor health, environmental monitoring, and wellness monitoring, inventory location monitoring, factory and process automation, power monitoring, and seismic and structural monitoring.
ii. Tracking applications include tracking animals, humans, objects, and vehicles.

While there are many different applications, below we describe a few example applications that have been deployed and tested in the real environment. [15]

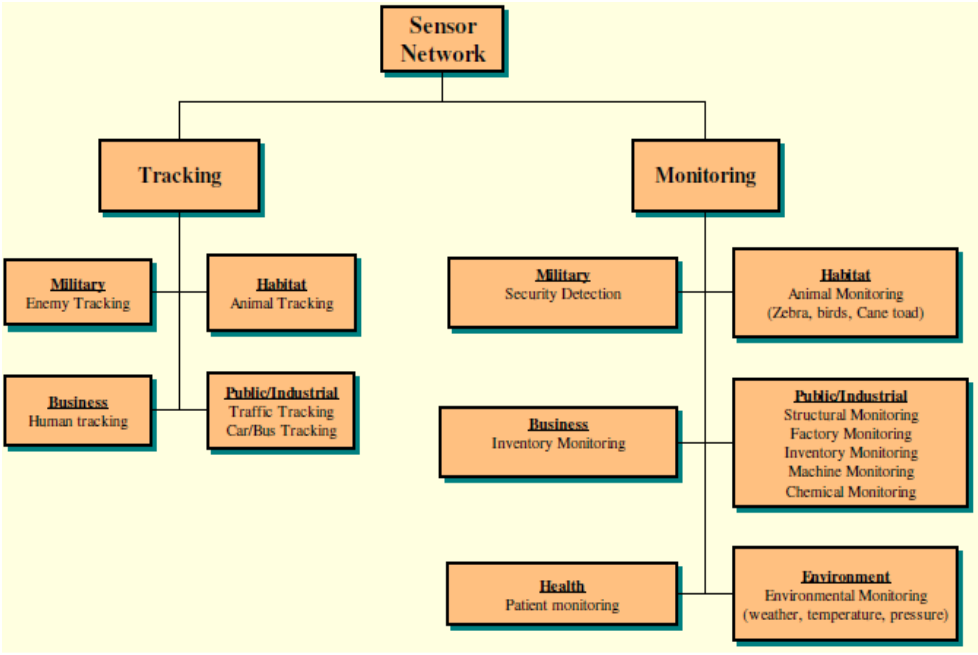

Figure 2: Overview of Wireless Sensor Networks. [15]

1.3 Denial of Sleep attack:

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. [16]

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: [16]

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. [13]

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] [16]

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][16]

III. PROPOSED WORK

In this paper, we are presenting a new approach to detect and prevent denial of sleep attack by evaluation 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. [16]
- 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. [16]

- 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. [16]

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 evaluate alive nodes and improve the network life. The work is implemented in matlab environment. [16]

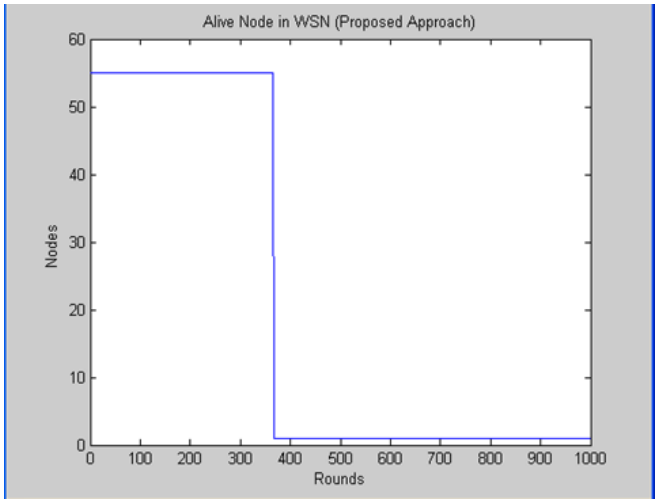

Figure 3 Alive Node Analyses (Proposed Approach)

Figure 3 showing the alive 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 alive node status over the network. Initially all node are alive but as the communication is performed, nodes start losing the energy. After 300 rounds only two nodes are alive.

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 [16]

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

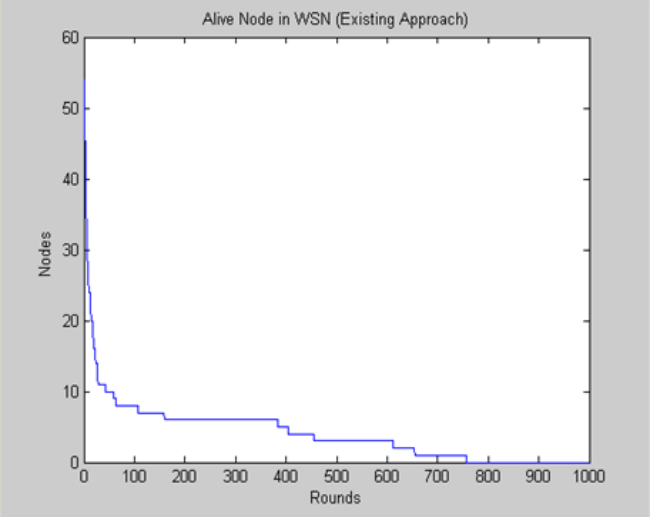

Figure 4.Alive Node Analysis (Existing Approach)

Figure 4 showing the alive 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 alive node status over the network. Initially all node are alive but as the communication is performed, nodes start losing the energy.

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

	Proposed	Existing
0	55	8
100	55	6
200	55	6
300	1	5
400	1	3
500	1	3
600	1	1
700	1	0
800	1	0
900	1	0
1000	1	0

Table2. Alive Node Analysis (Proposed Vs Existing)

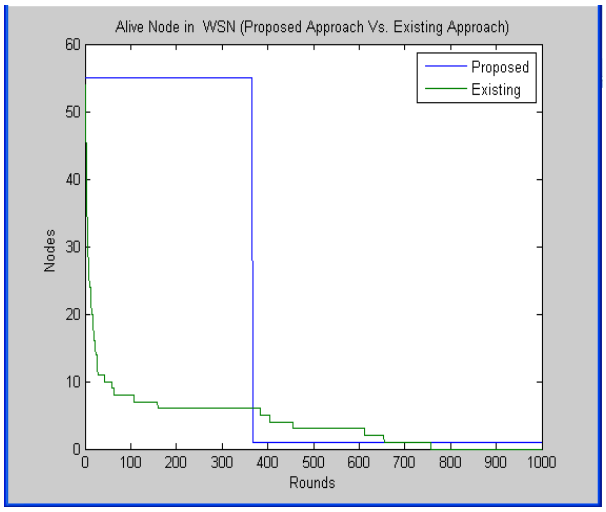

Figure 5: Alive Node Analysis (Proposed Vs. Existing)

Figure 5 showing the alive 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 alive node status over the network. As shown in the figure, the network life in proposed work is higher because nodes are alive for more number of rounds.

V. CONCLUSION

In this paper, we evaluation alive node in wireless sensor network for denial of sleep attack. Here initially alive nodes are less but as the communication is performed, alive nodes are increase and network life time is also increase.

ACKNOWLEDGEMENT

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://www.rtcmagazine.com/articles/view/101228

[14] Jason Lester Hill "System Architecture for Wireless Sensor Network "B.S. (University of California, Berkeley) 1998, M.S. (University of California, Berkeley) 2000

[15] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal "Wireless sensor network survey" Department of Computer Science, University of California, Davis, CA 95616, United States.

[16] Sunita Devi and Anshul Anand "Analysis of Dead Node in Wireless Sensor Network Denial of Sleep Attack" International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 3, Issue. 6, June 2014, pg.633 – 638

