Study of Denial of Service (DoS) Attack in Wireless Sensor Networks with Power Constraints

K Prashanth, S S Nagamuthu Krishnan

Wireless sensor networks (WSN) are highly vulnerable to attacks and constraints on resources like power, processing, and radio signal. In high constraint and vulnerable environments adapting to detection and defence mechanisms is a challenge. In this paper analysis of Distributed Denial of Service detection mechanisms of Sybil, Sinkhole, and Wormhole attack for power optimization is carried out based on the power consumption parameter. Power consumption attributes affects the efficiency of nodes during the time of attacks. Energy utilization and conservation also depend upon certain parameters comprising usage of network, changes in topology, climatic changes, no of sensors connected, memory utilization on sensors, and security issues. The analysis takes various attacks detection mechanisms into consideration and a comparative study is projected upon power optimization parameters. This study could contribute to the aspect of extending the activity of the sensor in various applications such as whether monitoring and recording of wildlife movement.

Keywords: **Sybil Attack, Sink Hole Attack,** ***Wireless Sensor Networks,***

I. INTRODUCTION

Wireless sensor networks (WSN) are formed with spatially distributed sensor nodes, in which data is obtained by observing physical or environmental conditions, by a large number of sensors deployed in a specific area, which also send the sensed data back to the sink or base station. It can experience problems during deployment, due to environmental factors or node hardware and software failures. WSN has constraints like storage, power consumption, data processing, and self-organizing in large scale, real-time data processing in complex environments. The important constraints upon sensor nodes are the low power consumption, as they carry limited and generally irreplaceable power sources. WSN is vulnerable for attacks due to changing topology, wireless communication among various sensor nodes. There are also security threats on WSN due to no infrastructure framework and limited access to physical resources like an energy source, memory capacity, and very low communication bandwidth. Sensor networks have to satisfy the requirements for providing secure communication and data encryption. The security goals of WSNs are authenticity, availability, confidentiality, and integrity [3]. Denial of Service (DoS) attack is a malicious attempt to make a computer system(server or single board or client) or the network disrupt. DOS is to flood with various services to reduce the bandwidth and the resources available on the network. This kind of attack normally hits the efficiency either temporarily or indefinitely. The attacks will be designed and targeted based on the various resources and services. This attack will saturate the victim by excessive communication requests and target the system (victim) cannot respond to the legitimate users at all or respond very slowly to diminishing its efficiency. It may reset the victim or occupy almost all of its resources obstructing its communication path.

There are limitations regarding the power consumption and memory leakage, the optimal working of the nodes will be disrupted during the attacks. There will be additional overhead on the resources of the nodes during the attacks. The various parameters involved to be impacted in different attacks are power consumption, memory, computing power, bandwidth, and computation range. In this, optimization of performance is based on the combination of parameters and control on the nodes during monitoring. During the attack, the detection node will be subjected to the optimization techniques, wherever power is expended. By optimizing certain parameters during the attack with added on defense strategy nodes can be secured.

II. PRELIMINARIES AND RELATED WORK

Wireless Sensor Networks (WSN) is resource-constrained, and security schemes should not introduce much complexity in terms of detecting various attacks. Sensor is a device which senses the information and sends sensed information to a node. A node is a device which comprises resources like processor, memory, battery, A/D converter. These nodes are usually deployed in an open unattended environment and are vulnerable to physical attacks. The broadcast nature of the transmission medium makes the WSN more prone to security attacks. Attacks are broadly classified as Active attacks and Passive attacks. During an active attack, an unauthorized attacker will be listening, monitoring, and can modify the data stream in the communication channel. Some of the identified active attacks are Sybil, Spoofing, Blackhole, Wormhole, Node capture, Replay to say a few. The main challenge in WSNs is to provide an efficient security scheme using the size of the sensor, memory, processing power, and communication capacity [1] [2]. Security is a challenge for the sensor nodes which are wireless and Ad-Hoc. One of the security mechanisms for WSNs is encryption during communication. It would be overhead for the sensor nodes during the receiving and sending.

To address the security issues and properties of sensor networks can be first, architect the security mechanism for the nodes. The deployment of sensor networks under a single domain administration, the threat model is simplified. It may be possible to exploit redundancy, scale, and the physical characteristics of the environment in the solutions [3] [11] [10].

Manuscript received on January 25, 2021.
Revised Manuscript received on February 17, 2021.
Manuscript published on February 28, 2021.
* Correspondence Author
K Prashanth*, Master of Computer Applications, RV College of Engineering®, Bengaluru, India. Email: prashanthk@rvce.edu.in
Dr. S S Nagamuthu Krishnan, Master of Computer Applications, RV College of Engineering, Bengaluru, India, Email: ssnk@rvce.edu.in

III. ATTACKS AND FINDINGS

Denial of service attack is to adverse normal working process of communication between the nodes or preventing devices from sending traffic. The nodes need to conserve energy during the idle time. So the nodes will be put on sleep mode for some time where the battery depletion can be slowed down. The Denial of Sleep attack which specifically keeps the node awake and intern drains the battery at a faster rate. The energy-efficient protocols are needed to communicate to deploy the sensor nodes on network. The sensor wireless network devices are vulnerable to attacks due to the wireless medium. Any adversary node under the radio range can listen to traffic, packet injection in to well-established computer networks or create collisions in between the devices to disrupt the flow in network. Sensor devices are extremely limited and depleting power supply. [4].

In wireless communication between the sensor nodes the radio coverage and irregularity in radio frequency will affect the performance. Radio frequency irregularity arises from multiple factors like RF sender signal strength, topology, and multiple paths depending on the direction of propagation. Irregularity in radio signals will affect the various upper layer protocols especially location based routing protocols. The efforts are made to study on various aspects which influence irregularity in the communication. It also leads to larger errors in localization and makes it difficult to maintain communication connectivity in topology control. In second scenario, the radio and signal strength is not identical for an individual transmission. [6]. The basic concept of the Sybil attack is pretence of existing identities or forging fake identities through a compromised node. Distributed storage and routing are known attacks. A Sybil attack is a node which is identified at multiple geographical locations. So the node can be hidden with different names. Sybil attack is a threat to protocol where ever it is employed. One of the mitigation process for detection is based on RSSI (Received Signal Strength Indicator) based Sybil attack detection techniques. New types of attacks are being identified are data aggregation, voting, fair resource allocation, and misbehaviour detection. The new defence mechanisms are being proposed like radio resource testing, verification of key sets for random key pre-distribution, registration, and position verification. The most promising method amongst these is the random key pre-distribution which associates a node's keys with its identity [5] [14].The attack is named Denial of Battery (DoB) attack can be caused by deliberate action on resources and services to deplete battery life. The various types of Denial of Battery attack can be listed out as: 1) Service attack; 2) Benign power attack; 3) Malignant power attacks. To estimate the effect of DoB attack corresponding mathematical models based on stochastic processes have been developed. The approach on protection for DoB can be on multilevel independent power control for sensors and also, successful monitoring based on the methods of discord detection. Simulation results demonstrate the good organization of the proposed approach for protection against DoB [17].

A Distributed Denial of Service (DDoS) attack is a synchronized attack on the available services of a given target system or network that is launched indirectly through many cooperated computing systems. It targets on the services of so called the 'primary victim' and attacks will be continued with the compromised system. The objective of DDoS is to deteriorate efficiency on bandwidth and resources. There are various tools available for attackers to organize and launch systematically. Using tools it is easy to implement and can be a disastrous effects. There are methods to mitigate and prevent on DDoS attack, however, many are still being developed and evaluated [13] [17].

The protocol Randomized, Efficient, and Distributed (RED) is capable of detecting node replication attacks. The differences in overhead that is sustained for computations will result in different energy consumption. The operating life of a node depends on its battery; hence different energy consumption will result in different behaviour of node battery exhaustion [7].

The Sink Hole Attack (SHA) gets trust on the surrounding nodes and starts with routing algorithms. The major advantage of compromising these with nodes is to spoof or replay an advertisement extremely high quality route to Base Station (BS). In some protocols quality on end-to-end with acknowledgement information is checked due to that a reliable and sustainable route to destination. SHA is achievable through wormhole also to get trust on routing algorithm. There are various protocols which identifies the route based on node power to reach accuracy. So during this kind of situation the malicious node can achieve the trust and redirect all the packets. Here malicious node takes control on routing and packets. Packet sniffing, dropping of packets, replay of same packets to various nodes can be done to depletion of battery on each and every node [8]. The attacker will always check with security in spite of how efficient the protocol is, the attacker work smart on achieving stepwise process for gaining trust on nodes. Once the trust is gained the attacker drastically decreases the level of channel confidentiality provided by the key pre-deployment schemes. In this paper energy efficient secure key pre deployment scheme (ESP) is proposed with combination of following properties: 1) energy efficient key discovery phase, 2) node to node authentication, 3) highly resistant to smart attacks. It is concerning with the efficiency of the key discovery phase mechanism, a pseudo-random key deployment scheme, ESP, which minimizes the computations and the communications required to establish pairwise keys, is highly resilient against the smart attacker model and provides a degree of probabilistic authentication that defends the network against several attacks including the Sybil attack. Analytical evaluation and extensive simulations support these claims [9].

The sensor nodes possess different limitations like energy, memory, computing power, communication bandwidth, and communication range. Since the WSN environment is resource-constrained encryption and decryption mechanisms have to be very simple and energy-efficient [13].

During the time of attacks, there is a huge utilization of power for detection and defense. It is not only dependent on the resources but also the throughput and delay [13] [14] [19]. The challenge is resiliency against node capture attacks [8]. In the Sybil attack, a node can generate and control a large number of logical identities on a single physical device. This gives an illusion in the network as if there are different legitimate nodes. The attacker bluffs the neighbour nodes through multiple identities [7].

Another form of attack is a replay attack, where the transmission is maliciously or fraudulently repeated or delayed [1]. Some of the approaches used for solving the problems are packet authentication and packet timer techniques [11].

Attacks like Sybil and flooding attacks will utilize the node parameters of memory, computation power, and energy [21]. This will lead to the depletion of the battery and place overhead on the computational power. Some of the attacks are major work on computation power with floods of oversized packets, just to reduce the communication breakdown. Energy utilization and conservation depends on certain things like time used on the network. The change in topology and climatic conditions will mostly affect the increase in power usage. The sensors which are connected to the node will have memory and processing power utilization. Security is a major part of the power and processing usage during the time of attack [22].

IV. ATTACKS IN WIRELESS SENSOR NETWORKS

The major challenge in the Wireless sensor network is securing the nodes with various attacks with limited resources. Here is a list of various attacks, countermeasures, and findings towards power optimization during the attacks.

Table 1: Network layer attacks with detection techniques

Network layer Attacks	Detection Techniques
Sinkhole	Hop count based detection, Agent-based detection, Cryptography based detection, Sequence number based detection [25]
Sybil	Trusted Certificate, Resource Testing, Economic Incentives, Received Signal Strength Indicator (RSSI) [27]
Wormhole	Geographical leash, Temporal leash [29]

Optimization of power parameters as mentioned below is one of the various possible ways to achieve efficiency on the nodes during the time of occurrence of the attacks.

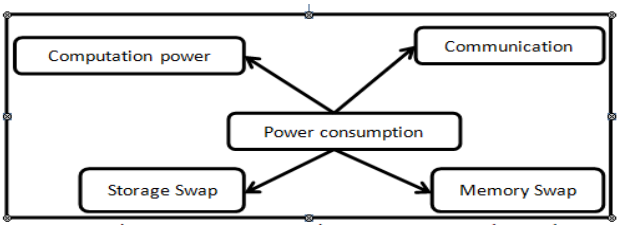

Fig 1. Power consumption parameters on the Node

A brief description on the significance of these parameters is discussed below.

Computation: In this aspect, the processor will be at computing steps and radio will be in an idle state, so the time dedicated before preamble for the computing and after the computing state. The time taken for computing and complexity of computing is an aspect which is to be considered. Energy for computation is the time taken for computation step into the steps for the computation so it adds to idle time for the radio signal.

Storage: It is a combination of computation and idle time for processor and storage. Energy for storage usage is calculated based on the time taken for the processor to execute steps for computing and storage.

Memory Swap: Memory swap is used where the temporary storage for computation is required. Energy for the storage usage will be calculated based on the time taken for the processor to execute steps for computing and time consumed for memory to swap, clear.

Communication: Communication is based on the transmitter, receiver, and computation time required for processing. The communication will also be more on the error correction, receiving acknowledgment, and re-transmission time. Time consumed for radio signal active is based on the size of the packet and the time for sending the packets to the other side. [20] The parameters involved in the different attacks are computing power, energy, memory, communication bandwidth, and storage.

Hence the need of the day is to optimize these parameters, in such a way that the primary purpose of the sensor nodes in WSN is not compromised.

V. CONCLUSION

In this paper, a survey on the various WSN attacks detection and with parameters which affects power depletion on the node. And also various different contributions done on power optimization on network layer attacks in WSN are discussed. There are various different challenges in optimizing the power parameters during attacks and handling the various aspects of energy constraints. The problem which is still open ended for research is optimizing the parameters of power consumption during the time of attacks.

REFERENCES

1. Zhou, Hai-Ying, et al. "Modeling of node energy consumption for wireless sensor networks." *Wireless Sensor Network* 3.1 (2011): 18.
2. Zhang, Fan, Reiner Dojen, and Tom Coffey. "Comparative performance and energy consumption analysis of different AES implementations on a wireless sensor network node." *International Journal of Sensor Networks* 10.4 (2011): 192-201.
3. Chou, Pai H., and Chulsung Park. "Energy-efficient platform designs for real-world wireless sensing applications." *ICCAD-2005. IEEE/ACM International Conference on Computer-Aided Design, 2005.*. IEEE, 2005.
4. Raymond, David R., et al. "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols." *IEEE transactions on vehicular technology* 58.1 (2008): 367-380.
5. Newsome, James, et al. "The sybil attack in sensor networks: analysis & defenses."*Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, 2004.
6. Abbas, Sohail, Madjid Merabti, and David Llewellyn-Jones. "Signal strength based Sybil attack detection in wireless Ad Hoc networks."*Developments in eSystems Engineering (DESE), 2009 Second International Conference on*. IEEE, 2009.
7. Conti, Mauro, et al. "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks." *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2007.
8. Salehi, S. Ahmad, et al. "Detection of sinkhole attack in wireless sensor networks." *2013 IEEE international conference on space science and communication (IconSpace)*. IEEE, 2013.
9. Pietro, R. D., Mancini, L. V., & Mei, A. "Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks." Wireless Networks, 12(6), 709–721.
10. Feng, Yuxiang, et al. "A replay-attack resistant authentication scheme for the internet of things."*Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on*. Vol. 1. IEEE, 2017.

11. Santhi, G., and R. Sowmiya. "A survey on various attacks and countermeasures in wireless sensor networks." *Int J Comput Appl* 159.7 (2017): 0975-8887.
12. Sonu Duhan, Padmavati Khandnor, "Intrusion detection system in wireless sensor networks: A comprehensive review", *Electrical Electronics and Optimization Techniques (ICEEOT) International Conference on*, pp. 2707-2713, 2016.
13. Shakhov, Vladimir, and Vladimir Popkov. "Performance analysis of sleeping attacks in wireless sensor networks." *Computational Technologies in Electrical and Electronics Engineering, 2008. SIBIRCON 2008. IEEE Region 8 International Conference on*. IEEE, 2008.
14. Sonu Duhan, Padmavati Khandnor, "Intrusion detection system in wireless sensor networks: A comprehensive review", *Electrical Electronics and Optimization Techniques (ICEEOT) International Conference on*, pp. 2707-2713, 2016.
15. Buch, Dhara, and D. C. Jinwala. "Denial of Service Attacks in Wireless Sensor Networks."*Institute of Technology, Nirma Universiry Ahmedabad–382* 481 (2010): 09-11.
16. Naik, Anil S., and R. Murugan. "Security Attacks and Energy Efficiency in Wireless Sensor Networks: A Survey."*International Journal of Applied Engineering Research* 13.1 (2018): 107-112.
17. Specht, Stephen M., and Ruby B. Lee. "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures." *ISCA PDCS*. 2004.
18. Alomari, Esraa, et al. "Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art."*arXiv preprint arXiv:1208.0403* (2012).
19. Kamboj, Priyanka, et al. "Detection techniques of DDoS attacks: A survey."*Electrical, Computer and Electronics (UPCON), 2017 4th IEEE Uttar Pradesh Section International Conference on*. IEEE, 2017.
20. Hsueh, Ching-Tsung, Chih-Yu Wen, and Yen-Chieh Ouyang. "A secure scheme for power exhausting attacks in wireless sensor networks."*Ubiquitous and Future Networks (ICUFN), 2011 Third International Conference on*. IEEE, 2011.
21. A. S. Hampiholi and B. P. Vijaya Kumar, "Efficient routing protocol in IoT using modified Genetic algorithm and its comparison with existing protocols," 2018 3rd International Conference on Circuits, Control, Communication and Computing (I4C), Bangalore, India, 2018, pp. 1-5, doi: 10.1109/CIMCA.2018.8739759.
22. Gungor, Vehbi C., and Gerhard P. Hancke. "Industrial wireless sensor networks: Challenges, design principles, and technical approaches." *IEEE Transactions on industrial electronics* 56.10 (2009): 4258-4265.
23. Santhi, G., and R. Sowmiya. "A survey on various attacks and countermeasures in wireless sensor networks." *Int J Comput Appl* 159.7 (2017): 0975-8887.
24. Sharma, Shivani, et al. "Classification of Security Attacks in WSNs and Possible Countermeasures: A Survey." *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 2019.
25. A. Mathew and J. S. Terence, "A survey on various detection techniques of sinkhole attacks in WSN," *2017 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, 2017, pp. 1115-1119, doi: 10.1109/ICCSP.2017.8286550.
26. Shafiei, Hosein, et al. "Detection and mitigation of sinkhole attacks in wireless sensor networks." *Journal of Computer and System Sciences* 80.3 (2014): 644-653.
27. Balachandran, Nitish, and Sugata Sanyal. "A review of techniques to mitigate sybil attacks." *arXiv preprint arXiv:1207.2617* (2012).
28. Meghdadi, Majid, Suat Ozdemir, and Inan Güler. "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks." *IETE technical review* 28.2 (2011): 89-102.
29. B. Bhushan and G. Sahoo, "Detection and defense mechanisms against wormhole attacks in wireless sensor networks," *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, Dehradun, 2017, pp. 1-5, doi: 10.1109/ICACCAF.2017.8344730.

AUTHORS PROFILE

Prashanth K, received MCA degree from Siddaganga Institute of Technology, Tumkur, in 2005. He is currently working as Assistant Professor with a RV College of Engineering, Bengaluru.

S. S. Nagamuthu Krishnan, received MCA degree from Karunya Institute of Technology, Coimbatore, the M Phil. (Computer Science) degree from Dr. GRD college of Engineering, Coimbatore, and the Ph.D. Degree in Computer Science from Bharathiar University, Coimbatore. He is currently working as Assistant Professor with RV College of Engineering, Bengaluru.