A Survey on Prevention Approaches for Denial of Sleep Attacks in Wireless Networks

G.Mahalakshmi[1], Dr.P.Subathra[2]
[1]Assistant Professor, Department of Information Technology, NPR College of Engineering And Technology, TamilNadu, India.
[2]Professor, Department of Computer Science &Engineering, Kamaraj College of Engineering & Technology, TamilNadu, India.

***Abstract*—Wireless sensor network is vulnerable to various attacks due to the deployment in hostile environment. Among various types of security threats, low power sensor nodes are affected by the attacks that cause random drainage of the energy level of sensors. It leads to the death of nodes. The denial of sleep attack is the most dangerous type of attack in this category. Most of the existing approaches to detect denial of sleep attack involve lot of overhead, which lead to poor throughput. In this survey, different approaches for the detection and prevention of denial of sleep attacks in wireless sensor networks are described.**

***Index Terms*—Anomaly detection, denial of sleep attack, frequency hopping, sleep deprivation.**

I. Introduction

Security of Wireless sensor network (WSN) becomes a significant issue with the fast development of WSN that is exposed to a wide range of attacks due to the limited resources and its deployment in the hostile environment. Intrusion detection system is one of the main and effective defensive approach against attacks in WSN. A particular devastating attack is denial of sleep attack (DS attack). It is a specific type of DoS (denial-of-service) attack. The denial of sleep attacks can be categorized into six categories depending on the attack strategy as

- Sleep deprivation attack
- Barrage attack
- Synchronization attack
- Replay attack
- Collision attack
- Broadcast attack.

In DS attack, the main aim of the intruder is to increase the power consumption of the sensor node. Its battery life is also decreased. Due to this attack, the lifetime of WSN is decreased. The attack accomplishes this by making the sensor node busy and preventing it from going into low power sleep mode. So the energy of the sensor nodes is wasted. Large amount of energy consumption is imposed upon the limited power sensor nodes by this attack. This leads to denial of service through denial of sleep.

The sleep deprivation attack is a severe attack in WSN as replacing or recharging node batteries in WSN is not possible. Barrage attack causes its victims to spend more energy by attacking them with legitimate requests. In both barrage attack and sleep deprivation attack, the victim will never enter its low power sleep mode. The aim of the synchronization attack is to cause relative time synchronization problems at the MAC layer. The synchronization attack is hard to detect because it stays within the confines of the protocol. A replay attack is a breach of security in which data is stored without authorization and then retransmitted in order to trick the receiver into energy exhaust operations. In the broadcast attack, the unauthenticated traffic is broadcasted into the network by the attacker node to reduce the lifetime of sensor nodes.

This type of attack is hard to detect as it does not affect legitimate throughput, which might signify an ongoing network attack. The collision attack can be launched by a compromised node that does not follow the medium access control protocol. Collision is caused with neighbor transmissions by sending a short noise packet. Many existing detection approaches depend on deterministic model. But in sensor network, the status of affected nodes changes with time.

The paper is organized as follows. Section 2 describes prevention approaches for denial of sleep attacks in wireless sensor networks. Section 3 presents results and discussion. Section 4 provides conclusion and future enhancement

II Prevention Approaches for Denial of Sleep Attack

2.1 Absorbing Markov Chain (AMC) Model

A mathematical model based on Absorbing Markov Chain (AMC) [1] was used to detect denial of sleep attack in sensor network. The probabilistic nature of sensor nodes was detected by the AMC model. In this approach, denial of sleep attack is detected by considering the expected death time of sensor network under common scenario. The method evaluate the behavior of compromised sensor nodes depending on the Markov chain with an absorbing state. The Absorbing Markov Chain was used to model the behavior of each and every sensor node. Instead of concentrating on single

doi:10.4304/jetwi.6.1.106-110

sensor node's behavior, the network flow is monitored by the approach to detect intrusion.

In this approach, the expected absorption time of senor network is examined which denotes the network lifetime. If the network state tends to death fast when compared to common death time of sensor network, then the network is affected by denial of sleep attack. The method was more accurate than the deterministic model.

2.2 Hierarchical Framework based on Distributed Collaborative Approach

A hierarchical framework based on distributed collaborative approach [2] was used for the detection of sleep deprivation attack in WSN. The method utilized anomaly detection approach in two steps to minimize the probability of false intrusion and to provide a reliable and energy effective heterogeneous WSN. The values are compared with predefined parameters specified in normal profile to detect the anomaly. The responsibility of each node changes dynamically to minimize the burden of a single node. In order to reduce the attack, the method physically prevents malicious nodes from the network and denies fake packets. Cross layer energy-efficient security mechanism [3] was used for the protection of network from denial of sleep attack. Simulation showed that the approach achieved significant performance in avoiding network nodes from distinct denial of sleep attacks. The cross layer interaction concept was used to prevent sensor nodes from energy exhaust attacks.

The cross layer information i.e. one hop routing table from the network layer was used by MAC layer to identify attackers. If the sender does not belong to the routing path of the receiver node, all received RTS packets are rejected. The Received Signal Strength Indication (RSSIs) of received packets are then computed and compared with RSSI of neighborhood routing node in order to prevent network nodes from malignant denial of sleep attacks such as replaying attacks. The approach is well suited for resource constrained WSNs as it requires low additional cost.

2.3 Lightweight hierarchical model for HWSNET

Heterogeneous wireless sensor network (HWSNET) is more suitable for real life applications when compared to the homogeneous counterpart. Security of HWSNET becomes a significant issue with the fast development of HWSNET. A lightweight, hierarchical model [4] was used for the insomnia detection of sensor nodes affected by sleep deprivation attack in HWSNET. The approach used cluster based method in an energy effective manner in order to build a five layer hierarchical network to increase the network scalability and lifetime. Here the sensor network is partitioned into clusters which are again divided into sectors.

Partitioning the sensor field preserves communication bandwidth and prevents redundant exchange of messages among senor nodes. In this approach, energy efficiency was accomplished by keeping a minimum number of sensors active. A dynamic model was designed to overcome the sudden death of intrusion detection system (IDS) enabled sensor nodes that are responsible for all detection tasks, due to power exhaustion. Anomaly detection technique was used in the approach in such a way that the phantom intrusion detection was avoided.

2.4 Swarm based Defense Approach

A swarm based defense approach [5] for denial of sleep attack utilizes an anomaly detection model to determine the affected traffic between the nodes. Depending on this, frequency hopping approach was initiated. Ant agents of swarm intelligence are then applied to gather the frequency hopping time and communication frequency. The faulty channel is identified depending upon the frequency hopping time. And when the administer node gets this data, it deletes the faulty channel. The simulation results showed that the approach is effective in faulty channel detection. Less energy is consumed as the data about all the attackers can be known by utilizing ants. A framework for preventing denial of sleep attack [6] consists of four key components

- Strong link-layer authentication
- Anti-replay protection
- Jamming identification and mitigation
- Broadcast attack defense

Strong link-layer authentication is the most significant and first component of denial-of-sleep defense and must be included into any WSN that might be exposed to attack.

2.5 Secure Topology Maintenance Protocol (Sec-TMP)

The scalable Secure Topology Maintenance Protocol (Sec-TMP) [7] was resilient to sleep deprivation attacks. Sec-TMP does not require underlying routing and pair-wise node confidentiality. It was highly scalable as the newly deployed nodes were involved in the TMP (topology maintenance protocol) by the pre-existing nodes in the network. It utilizes one-hop communications. A novel approach for detection of sleep deprivation attacks [8] depends on wireless sensor network (WSN) clustering. It includes recursive clustering of sensors till a required granularity is achieved. The approach is applied with two distinct clustering algorithms. Fast and Flexible Unsupervised Clustering Algorithm (FFUCA) was used. To launch the sleep deprivation attack, the adversary nodes become cluster heads.

2.6 Random Vote, Round Robin and Hash-based Scheme

Three clustering approaches for mitigating sleep deprivation attack: the random vote, round robin and hash-based scheme were analyzed [9]. These approaches prevent the adversary from becoming a cluster head and also minimizes the impact of sleep deprivation attack. The random vote scheme randomizes the cluster head selection. The round robin scheme was used to overcome the lack of scalability problem in random vote clustering algorithm. In round robin scheme, clusters were maintained for long periods of time. The round robin scheme consists of two phases

- Bootstrapping phase
- Maintenance phase

Initial clusters were formed in bootstrapping phase. In the maintenance phase, the precise membership of each

cluster is updated due to addition of new nodes, removal of nodes from network and node mobility. The round robin scheme requires only a single iteration for selecting cluster head. But, a list indicating nodes in cluster at all times must be maintained at each sensor node in the round robin scheme. The excessive overhead inherent in the round robin scheme is overcome by the hash-based cluster head selection scheme. Dynamic clustering in an attack and fault tolerant manner is performed without excessive overhead.

Many denial of sleep attacks don't require a constant signal. So it is difficult to recognize the traffic as malicious and to identify the attacking node through its emitted transmissions [10]. The denial of sleep attack focuses MAC protocols. A clever denial of sleep attack keeps the radios of sensor nodes on and their batteries are drained in few days. The denial of sleep attack is mitigated by a framework including authentication at link layer, protection of broadcast attack and tamper resistance.

2.7 Isolation Table Intrusion Detection System (ITIDS)

Isolation tables and routing tables [11] are combined to detect anomalies. Isolation Table Intrusion Detection System (ITIDS) detects malicious nodes depending on attack behaviors. The malicious node is detected through its unusual behavior. The sensor node behaviors are compared with the attack behaviors for determining anomalous information. If the node is anomalous, it is isolated and recorded in isolation table. In ITIDS, sensor nodes of all kinds are concerned by monitoring task and control each other to detect denial of sleep attack. There are four characteristics of ITIDS

- Base station (BS)
- One Primary Cluster Head (PCH)
- Several Secondary Cluster Heads (SCHs)
- The remaining senor nodes are MNs (member nodes)

The approach consists of four stages. Initially, the system predefines IDS. MNs are monitored by SCH. Then PCH is monitored by SCHs and MNs. Lastly, IDS backups the isolation table in base station.

2.8 Ant-based Routing Algorithm

An ant-based routing algorithm [12] was used to detect denial of sleep attacks in WSN. The denial of sleep attacks are detected by using age, energy and reliability as parameters. The impact of distributed denial of service attacks on the performance of WSN is evaluated by using OPNET modeler. Packet authentication is used to prevent the denial of sleep attack [13]. Continuous resetting of sleep timers and link-layer authentication is used to protect from denial of sleep attack.

2.9 Secure Wake up Scheme

A secure wake up scheme [14] activates a sensor node by a secure wake up radio from a sleep state only if messages from legitimate and authenticated nodes are pending. The approach uses a lightweight security verification scheme which can be performed without requiring the change of node to its active state. The network can be protected from the sleep deprivation attack by moving the authentication from application level to physical level. Time synchronized one-time-password scheme [15] provide a secure wake up authentication.

The scheme under denial of sleep attack consume less power than the self-discharge of the batteries. The main idea is to keep the node always in the sleep mode and wake it up only as and when communication is essential. An additional receiver is used that remains in idle mode and uses only small amounts of energy. The communication requests are captured by this receiver. It also wake up the parts of node that are currently in rest in order to receive data.

All incoming requests to the wake up receiver on the physical layer are authenticated to prevent the adversaries targeting to drain the energy. The request that wireless sensor nodes utilize to wake up each other is known as token. The unnecessary traffic is reduced by computing the tokens instead of exchanging them. The counter-synchronized one time password is used for token generation.

2.10 Storm Control Mechanism

Storm control mechanism [16] was used to mitigate flooding and denial of sleep attacks. The frequency of the received packets is tracked by the system. An alert is triggered when it goes beyond a configured limit. The node sends alert to the base station and shuts its wireless transceiver for a predefined period of time. The storm control mechanism was implemented in TinyOS as a security layer incorporated in the communication stack. TOSSIM is used to test the implementation.

2.11 Clustered Adaptive Rate Limiting (CARL) Approach

Clustered Adaptive Rate Limiting (CARL) [17] approach depends on current host-based intrusion detection methods to prevent denial of sleep attacks. It is a rate limiting approach. In this adaptive rate limiting approach, network traffic is restricted when enough malicious packets are sensed in order to suspect that there is presence of attack. It can be also utilized to maintain better throughput and network lifetimes at a time even during sleep deprivation attack. A fake schedule switch scheme with RSSI measurement [18] defends denial of sleep attack. The scheme is implemented in S-MAC protocol. a quickest intrusion detection scheme, markov decision process (MDP) [19] keeps a minimal number of sensors active. The approach ensures energy expenditure for sensing, communication and computation is reduced. It also ensures that the network lifetime is reduced. A secure intrusion detection system [20] was used for denial of sleep attack prevention in WSN.

III RESULTS AND DISCUSSION

The results of the survey are shown in table 1. Various approaches for the prevention of denial of sleep attacks in wireless networks are depicted. AMC model evaluates the behavior of compromised sensor nodes to detect denial of sleep attack. Hierarchical framework based on

distributed collaborative approach uses anomaly detection approach to detect sleep deprivation attack. Swarm based defense approach uses ant agents of swarm intelligence. The lack of scalability problem in the random vote scheme and excessive overhead inherent in round robin scheme is overcome by hash based scheme. FFUCA algorithm was used in recursive clustering of sensors approach. Routing and isolation tables are used in ITIDS technique.

TABLE 1:

TECHNIQUES FOR PREVENTION OF DENIAL OF SLEEP ATTACKS

Authors	Year and reference	Technique	performance
Bhattasali and Chaki	2012 [1]	Absorbing Markov Chain (AMC) model	The behavior of compromised sensor nodes is evaluated based on Markov chain
Bhattasali et al.	2012 [2]	Hierarchical framework based on distributed collaborative approach	Uses anomaly detection approach to detect sleep deprivation attack.
Boubiche et al.	2012 [3]	Cross layer energy-efficient security mechanism	Uses cross layer interaction concept to prevent sensor nodes from energy exhaust attacks.
Bhattasali and Chaki	2011 [4]	Lightweight hierarchical model for HWSNET	Detects insomnia of sensor nodes affected by sleep deprivation attack
Periyanayagi and Sumathy	2013 [5]	Swarm based defense approach	Uses ant agents of swarm intelligence
Gabrielli et al.	2009 [7]	Scalable Secure Topology Maintenance Protocol (Sec-TMP)	Highly scalable and uses one-hop communication
Fouchal et al.	2013 [8]	Recursive clustering of sensors	Uses Fast and Flexible Unsupervised Clustering Algorithm (FFUCA)
Pirretti et al.	2006 [9]	Hash-based scheme	Overcome lack of scalability problem and excessive overhead inherent
Chen et al.	2010 [11]	Isolation Intrusion Detection System for hierarchical WSN	Routing tables and isolation tables are combined to detect anomalies
Juneja et al.	2010 [12]	Ant-based routing algorithm	Uses age, energy and reliability as parameters
Rughinis and Gheorghe	2010 [16]	Storm control mechanism	The storm control mechanism is implemented in TinyOS

CONCLUSION

The paper comprises the survey results in prevention approaches for denial of sleep attack in wireless sensor networks. The survey describes various methods and techniques such as AMC model, cross layer security mechanism, swarm based defense approach, ITIDS, storm control mechanism, ant-based routing algorithm. The results of the survey show that the solutions, which require large scale alterations are unrealistic. As a future work, the prevention of denial of sleep attacks can be performed with minimum changes, cost and resources

REFERENCES

[1] T. Bhattasali and R. Chaki, "AMC Model for Denial of Sleep Attack Detection," *Journal of Recent Research Trends (JRRT),* pp. 1-4, 2012.

[2] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network," *arXiv preprint arXiv:1203.0231,* 2012.

[3] D. E. Boubiche, A. Bilami, and S. Athmani, "A Cross Layer Energy Efficient Security Mechanism for Denial of Sleep Attacks on Wireless Sensor Network," in *Networked Digital Technologies*, ed: Springer, 2012, pp. 151-164.

[4] T. Bhattasali and R. Chaki, "Lightweight hierarchical model for HWSNET," *Networking and Internet Architecture,* pp. 1-14, 2011.

[5] S. Periyanayagi and V. Sumathy, "Swarm Based Defense Technique for Denial-of-Sleep Attacks in Wireless Sensor Networks," *International Review on Computers & Software,* vol. 8, 2013.

[6] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," *Vehicular Technology, IEEE Transactions on,* vol. 58, pp. 367-380, 2009.

[7] A. Gabrielli, M. Conti, R. Di Pietro, and L. V. Mancini, "Sec-tmp: a secure topology maintenance protocol for event delivery enforcement in wsn," in *Security and Privacy in Communication Networks*, ed: Springer, 2009, pp. 265-284.

[8] S. Fouchal, D. Mansouri, L. Mokdad, and M. Iouallalen, "Recursive - clustering - based approach for denial of service (DoS) attacks in wireless sensors networks," *International Journal of Communication Systems,* 2013.

[9] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," *International Journal of Distributed Sensor Networks,* vol. 2, pp. 267-287, 2006.

[10] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *Pervasive Computing, IEEE,* vol. 7, pp. 74-81, 2008.
[11] R.-C. Chen, C.-F. Hsieh, and Y.-F. Huang, "An isolation intrusion detection system for hierarchical wireless sensor networks," *Journal of Networks,* vol. 5, pp. 335-342, 2010.
[12] D. Juneja, N. Arora, and S. Bansal, "An Ant-Based Routing Algorithm for Detecting Attacks in Wireless Sensor Networks," *International Journal of Computational Intelligence Research,* vol. 6, 2010.
[13] S. Saha, "ZIGBEE OPNET Modeller: An Efficient Performance Analyzer for Wireless Sensor Networks."
[14] R. Falk and H.-J. Hof, "Fighting insomnia: a secure wake-up scheme for wireless sensor networks," in *Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on*, 2009, pp. 191-196.
[15] A. Kavoukis and S. Aljareh, "Efficient time synchronized one-time password scheme to provide secure wake-up authentication on wireless sensor networks," *arXiv preprint arXiv:1302.1756,* 2013.
[16] R. Rughinis and L. Gheorghe, "Storm control mechanism in wireless sensor networks," in *Roedunet International Conference (RoEduNet), 2010 9th*, 2010, pp. 430-435.
[17] D. R. Raymond and S. F. Midkiff, "Clustered adaptive rate limiting: Defeating denial-of-sleep attacks in wireless sensor networks," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*, 2007, pp. 1-7.
[18] C. Chen, L. Hui, Q. Pei, L. Ning, and P. Qingquan, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," in *Information Assurance and Security, 2009. IAS'09. Fifth International Conference on*, 2009, pp. 446-449.
[19] K. Premkumar and A. Kumar, "Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks," in *Proc. IEEE Infocom*, 2008.
[20] P. Sharma, N. Sharma, and R. Singh, "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network," *International Journal of Computer Applications,* vol. 41, pp. 16-21, 2012.