ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 1, January 2014**

# A Survey on the Solutions for the Problems of Denial of sleep Attacks

RamandeepKaur, Vinodsharma

Student, Dept. of C.S.E., Guru Kashi University, Talwandisabo, Punjab, India

Assistant Professor, Dept of C.S.E., Guru Kashi University,Talwandisabo, Punjab, India

**ABSTRACT:** Wireless Sensor Network (WSN) is heading to lead in the name of technology. Either it is a mobile or a car or the any security technique, sensors are used widely. Though low power of sensor nodes is great disadvantage many research is done to overcome this disadvantage. This paper has described some of the recent research made in sensor network. Energy-constrained is main focus considered in each research and analyzing energy in the network with and without attack. DOS attack is analyzed in this paper.

**Keywords**: Wireless Sensor Network, Denial of sleep, Medium Access Control (MAC)

## I. INTRODUCTION

Wireless sensor network (WSN) consist of several nodes where each node is connected to one or more sensor. Many people consider that wireless sensor network security is similar to WiFi applications. Compared to Wifi, it needs real-time deterministic performance. These are constrained in computational capabilities such as bandwidth and frequent powered battery changes. WSN is easily accessible and are having fixed field and are resistant to attacks.

WSN communication is very easy to attack. Some of the attacks. Some of the attacks on wsn are eavesdropping, data injection and traffic analysis attacks. The combination of these factors demands security for sensor networks at design time to ensure security to operate like secrecy of sensitive data and privacy to people in sensor nodes. Providing security in sensor network is even more difficult than MANETS due to resource limitations of nodes.

For large scale it is impractical to monitor and protect each individual sensor from physical or logical attack. Host based attacks on sensor network are User compromise, hardware and software compromise.


Fig no.1.1: Communication between wsn nodes

Above given fig no 1.1 shows that communication between wsn nodes are performed using the wsn gateway. The gateway is used to communicate with users. And WSN node communicate with each other using antenna attached each sensor node .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 1, January 2014**

Other than this there are many research conducting on the sensor in the real world because of increasing demand of the wireless sensors. Sensor network is also called dust network because of the small size of sensors. Other than this sensor network have the property of power consumption constrains for nodes using batteries or energy harvesting, and ability to cope with node failures.

## II. PROBLEM DEFINITION

### A. Wireless sensor network

Wireless sensor network (WSN) is vulnerable to attacks due its energy constraints. Wireless sensor network consists of several nodes where each node is connected to one or more sensor. Due to limited range,power, and processing constraints and its cost sensors are out of reach of real world. Other than this, there are large number of nodes in a network which lacks their global id and are prone to failure. For conserving the energy of sensor network, there is a modes of wsn nodes. Various modes are active mode and sleep mode. Active mode of wsn node is to show that wsn node is ready to receive and send data. Whereas, sleep mode show that wsn node is not ready to receive or send the data. There are diferent levels of energy consumption in each of modes. Some analysis of these have been made and are shown below

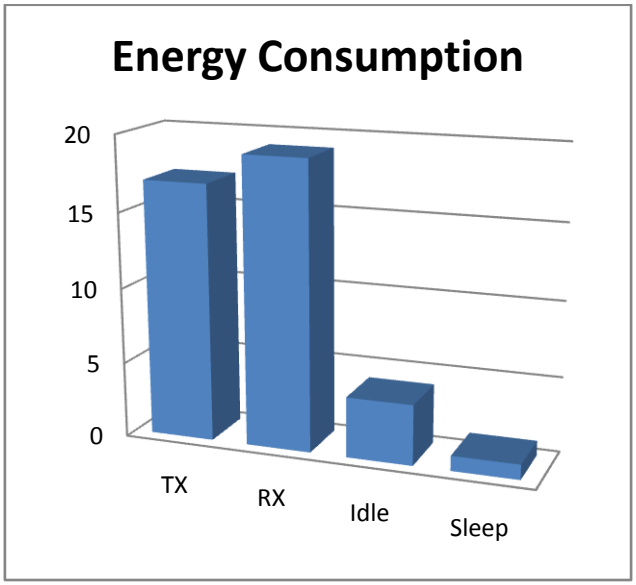


Fig 2 Energy Consumption

Fig 2 shows Sensor Network Energy consumption during te transmission and receiving of the packets and the various moods of sensor node energy consumption is also shown. This graph shows that energy consumed during sleep mode is very less than the energy consumed during the idle state of the sensor node. So its better to keep the sensor node in sleep mode when no packet r message is arriving in order to conserve the energy of the sensor node and hence the sensor network.

But the problem arises when it is impossible to understand at what time sensor nodes are kept sleep mode and if sensor node is in sleep mode and there is a packet arrived at the sensor node it is unable to send that packet or their more energy is consumed.

So there are many attacks which tries to keep the sensor node awake so as to simply consume the energy of the nodes.

Various attacks on sensor networks are:

- Wormhole attack
- Hello attack
- Sybil attacks
- Dos attacks

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 1, January 2014**

- Selective forwarding
- Acknowledgement spoofing

B. Denial of sleep attack

It is a technique which prevents the radio from going into sleep mode. Many techniques introduced its impact on battery –powered mobile devices. An attacker might uses jamming attack to consume the energy and battery of the sensor but it would take about months to completely deplete the targeted devices whereas denial of sleep attack is a clever attack that keeps the sensor nodes radio ON that drain the battery in only few days. Several solutions have been proposed to solve these types of attack but each has limited feature which are only concern to the particular layer. In this paper we are only concern with the denial of sleep attack which is type of denial of service attack on data link layer.

C. Wormhole attack

In this assault, ambusher record parcel at one area of the system and tunnels them to an alternate area by retransmitting them. The least difficult occurrence of this assault is a solitary hub arranged between two different hubs sending messages between the two of them. Nonetheless, wormhole assaults more usually include two removed malevolent hubs plotting to understate their separation from one another by transferring parcels along an out-of-band channel accessible just to the aggressor. An ambusher arranged close to a base station may have the capacity to totally upset steering by making an overall put wormhole. An aggressor could persuade hubs who would regularly be numerous jumps from a base station that they are one and only or two jumps away by means of the wormhole. This can make a sinkhole: since the aggressor on the other side of the wormhole can falsely give a great track to the base station, conceivably all movement in the encompassing region will be drawn through if exchange tracks are fundamentally less engaging.

D. Hello attack

Numerous conventions oblige hubs to show Hello parcels to declare themselves to their neighbors, and a hub gaining such a bundle might accept, to the point that it is inside radio run of the sender. This supposition might be false: a portable computer class assaulter Tv steering or other data with vast enough transmission power could persuade each hub in the system that the foe is its neighbor.

E. Sybil attacks

It is one of the serious attack on sensor network where sensor node illegimately taking on multiple identities. This attack disturbs the aggression, fair resource allocation, and changes the routing. Some validation techniques may be undertaken to prevent this attack. Various prevention techniques are direct vs indirect validation, identity vsunidentity validation.

F. Selective forwarding attack

Multi-bounce systems are frequently dependent upon the presumption that taking part hubs will reliably forward gained messages. In a specific sending assault, noxious hubs might decline to send certain messages and basically drop them, guaranteeing that they are not engendered any further. A basic manifestation of this ambush is the point at which a malignant hub carries on as a dark opening and declines to advance each bundle .

## III. SECURITY REQUIREMENTS

A sensor network is a type of network which share commonality between sensor nodes. The requirement of each sensor node is different as each sensor node possess the unique functionality according to the scope of the system. On the basis of which the following subsections explain the main MAC security attacks in detail.

A. Data freshness

In this way, information freshness was measured just regarding inactivity or postponement of bundles appropriated at the base station, where thecenter is on to what extent a hub may as well hold up before it totals information bundles such that postpone is decreased. Indeed, they don't address if sufficient nformation from a zone or source has been

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 1, January 2014**

accepted as wanted by the requisition. To make strides information freshness, it is vital for the information parcels to achieve the base station dependability.

B. Data confidentiality

Classifiedness forestalls touchy data from arriving at the wrong individuals, while determining that the right individuals can actually get it. An exceptional sample is a record number or tracking number when saving money online. A extremely key part of ensuring data privacy might be encryption. Encryption guarantees that just the right (individuals who knows the key) can read the data. Encryption is VERY prevailing in today's surroundings and might be found in practically every significant convention being used. An exceptionally noticeable sample will be Ssl/tls, a security convention for correspondences over the web that has been utilized within conjunction with countless conventions to guarantee security.

C. Authentication

A message verification code (MAC) is a symmetric cryptographic component that takes as include a k-bit mystery key and a message, and yields a l-bit verification tag. To trade bona fide messages, a sender and recipient must impart the same mystery key. Utilizing the mystery key, the sender registers the message's verification tag (or MAC) and adds it to themessage. To confirm the validness of a message, the beneficiary registers the message's MAC with the mystery key and thinks about it

to the definitive MAC added with the message. For any message, a safe MAC capacity anticipates an agressor without earlier information of the mystery key from processing the right MAC. A MAC accomplishes genuineness for focus to-focus interchanges since a collector realizes that a message with the right MAC must have been produced either without anyone else present or by the sender.

D. Data integrity

Information respectability in sensor systems is required to guarantee the unwavering quality of the information and alludes to the capacity to affirm that a message has not been messed around with, adjusted or changed. Regardless of the possibility that the system has secrecy measures, there is still a probability that the information trustworthiness has been bargained by modifications. The honesty of the system will be into a bad situation when:

- A noxious hub display in the system infuses false information.
- Unstable conditions because of remote channel cause

harm or misfortune of informat.

E. Availability

Accessibility verifies if a hub can utilize the assets and if the system is accessible for the messages to impart. Be that as it may, disappointment of the base station or bunch guide's accessibility will inevitably debilitate the whole sensor system. Accordingly accessibility is of essential imperativeness for administering an operational system.

F. Self-organization

The procedure in which pattern at the worldwide level of a framework rises singularly from various connections around the easier level components of the system. Moreover, the standards determining the communications around the framework's parts are executed utilizing just nearby information, without reference to the worldwide example. While appealing, it appears to us that this definition pushes back the issue to characterizing different terms- e.g. levels of organization, emergence, example, and neighborhood vs. worldwide information. These terms are exceptionally challenging to characterize precisely, perhaps more troublesome than the expression "self-association" itself.

## IV. LITERATURE REVIEW

As of late, there have been a few existing answers for illuminate the Denial of sleep ambushes issue by adding security to Wsn keeping in mind the end goal to prevent/detect assaulter. Nonetheless, a large portion of them have some

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 1, January 2014**

discriminating impediments. They are portrayed underneath in minimized structure with their qualities and confinements as takes after:

A. Wireless sensor network denial of sleep attack

Brownfield et al. [4] proposed new Mac convention which mitigates a significant number of the impacts of dissent of slumber ambushes by bringing together group administration. Mac has some vigor sparing characteristics which develop the system lifetime, as well as the concentrated building design makes the system lifetime more impervious to foreswearing of slumber assaults. Other than single period and synchronization message, it has two discord period and distinctive systems for sending the message inside the bunches and outside the bunch through the passage hub. The Mac convention Performance Results demonstrate that G-Mac performs signifantly superior to different conventions in each movement circumstances. The void system case shows the convention overhead and sit still listening impacts resolved by the adequate obligation cycle-Mac has .95% obligation cycle is weighted normal of obligation cycle of door hub and different hubs. Attacker can pick up access to system through entryway hub. At the same time agressor can just influence one hub at once on the grounds that hubs exchange the entryway obligations based upon incremental build in electric storage device levels.

B. Effect of Denial of sleep attacks on wireless sensor network MAC protocols

David R. Raymond et al. [5] arranges sensor organize foreswearing of-slumber assaults regarding an ambusher's learning of the medium access control (Mac) layer convention and capacity to detour validation and encryption conventions. Ambushes from every order are then displayed to show the effects on four sensor system Mac conventions, i.e., Sensor Mac (S-Mac), Timeout Mac (T-Mac), Berkeley Mac (B-Mac), and Gateway Mac (G-Mac). Executions of chosen strike on Mac, T-Mac, and B-Mac are portrayed and examined in portion to accept their viability and break down their effectiveness. And it indicates that the most productive assault on S-Mac can keep a group of hubs astir 100% of the time by an assailant that dozes 99% of the time. Ambushes on T-Mac can keep chumps alert 100% of the time while the assailant rests 92% of the time. With learning of convention due to contrasts exist in bundle structure and timing between Wsn Mac conventions, and even without capacity to infiltrate encryption; all remote sensor system Mac conventions are helpless to a full mastery strike, which decreases the system lifetime to the base conceivable by amplifying the force utilization of the hubs' radio subsystem. Indeed without the capability to infiltrate encryption, inconspicuous strike might be started, which lessen the system lifetime by requests of size. Assuming that sensor systems are to meet current desires, they must be hearty notwithstanding system assaults to incorporate disavowal of-slumber. This approach likewise increments the system overhead.

C. Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks

Raymond D. R. Et al. [6] Describes the host based lightweight interruption identification system, Clustered Adaptive Rate Limiting (Carl) dependent upon the rate restricting approach at Mac layer is proposed to thrashing foreswearing of slumber ambushes. The essential inadequacy of the above strategy is that the period throughout which hubs are alert is not synchronized, so if a hub has a parcel to send, there is no certification that different hubs will survey at the correct opportunity to catch a share of the prelude and remain wakeful for the information bundle. The procedure utilized within B-Mac builds inertness in multi bounce systems and if blasts of system movement are produced at a higher rate than is upheld by rate-restricting approach, system activity is lost. So in adjustable rate constraining, system activity is limited just when malignant parcels have been sensed at a rate sufficient to suspect the strike. . It could be utilized to administer arrange lifetimes and better throughput at once even in face of slumber need strike.

D. An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks.

Chen C. et al. [7] describe a scheme is proposed utilizing fake schedule switch with Rssi measurement aid. Here we focus on previous attack and introduce fake schedule. The sensor nodes can reduce and debilitate the harm from fatigue attack and on the contrary make the attackers lose their energy quickly in order to die. Recreation results indicate that at a spot price of energy and delay, network health can be guaranteed and packets drop ratio has been decreased compare with original scenario without our scheme. Here in this paper we consider just S-Mac protocol with duty cycle 10%. In

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 1, January 2014**

the event that packet misfortune is not caused by the attack, then fake schedule switch is harmful. Due to which Rssi is used as a quality assigned to each node and node having attacker one bounce away has larger Rssi worth.

E. Sleep deprivation Attack Detection in Wireless Sensor network

TapalinaBhattasali et al. [8] proposed a hierarchical framework based on distributed collaborative mechanism for detecting sleep deprivation torture in wireless sensor network efficiently.In heterogeneous sensor field, sensor nodes are categorized into various roles such as sink gateway (SG), sector monitor(SM), Sector-in –charge (SIC) and leaf node (LN) depending on their battery capacity. Here leaf node is used to sense the data, SIC is used to collect the data and SM detect the data as valid data and invalid data. Sink Gateway is used to access other networks.Here if leaf nodes are directly affected by intruder, node cannot detect it. As a result battery of affected node may be low or exhausted completely. This can affect data transmission for network due to which it is done in authenticated way.

F. Optimal Dynamic Sleep Time Control in wireless Sensor Networks

Ning et al. [9] Proposed the dynamic sleep time rather than fixed sleep time which minimizes the energy wasted in idle channel i.e. energy to transmit and receive the message. This paper has used the dynamic programming (Dp) algorithm rather than differential mathematical statements (Ode) to find the comprehensively optimal result. The problem with this approach is that there are a few cases where it is not conceivable to find a worldwide optimal result utilizing Dp, therefore Ode must be used which is difficult to execute and is complex.

G. Distributed Wake-Up scheduling for Data collection in tree-based wireless sensor networks

Fang-Jing wu et al. [10] expressed a plan reputed to be conveyed get up planning plan for information gathering in a sensor networks that accomplishes both vigor protection and low reporting dormancy, i.e. in a multihop wireless network, a basic and productive method for characterizing impedance neighbors is to deny a hub from utilizing the same slot0code as those of its 1-jump and 2-bounce neighbors. Force sparing and inactivity are enhanced to drag out network lifetime and freshness of information.

## V. COMPARISON OF EXISTING SOLUTIONS

From the description of each of the results presented in Section Iv, we can effectively notice that no result offers an achievable answer for the Denial of sleep attacks.

Out of the all proposed answers for tackle the problem of Denial of sleep attacks, the results based on Mac protocol[4] have caused a few serious performance punishment, the single purpose of failure is conceivable. Proposed by David R. Raymond, et al. [5] is used to investigation each Mac protocol with various sorts of denial of sleep attacks by forming a framework yet this result increases the network overhead. The Carl technique proposed by Raymond D. R. et al. [6] comes up short when network traffic is generated at higher rate than is the rate –limiting policy. The fake schedule switch result proposed by Chen C. et al. [7] is the most yearning ones, however either they require complex establishments. Then again, proposed by TapalineBhattasali et al. [8] is comparatively more effective yet leaf nodes are directly attacked by the intruder. The result proposed by Ning et al. [9] is used to find the dynamic sleep time yet result becomes complex in a few cases. Other result proposed by Fang-Jing wu, is not equipped to handle various errands at a same time.

## VI. CONCLUSION

This paper portrayed Wsn, a few conceivable Denials of sleep ambushes, a percentage of the sorts of denial of sleep strike. We dissected some as of now accessible results; recognize their qualities and confinements and give correlation around them. So we can say that this paper may be utilized as a source of perspective via scientists when choosing how to secure the sensor nodes. We are likewise taking on advancing an answer of securing the sensor nodes in the groups, with the goal that we can determine sensor nodes has the ability to adapt up to assaults

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 1, January 2014**

## REFERENCES.

1. Zheng, Jun, and Abbas Jamalipour. Wireless sensor networks: a networking perspective. Wiley. com, 2009.
2. Raymond, David R., and Scott F. Midkiff. "Denial-of-service in wireless sensor networks: Attacks and defenses." Pervasive Computing, IEEE 7.1 (2008): 74-81.
3. Brownfield, Michael, Yatharth Gupta, and Nathaniel Davis. "Wireless sensor network denial of sleep attack." Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC. IEEE, 2005.
4. Raymond, David R., and Scott F. Midkiff. "Clustered adaptive rate limiting: Defeating denial-of-sleep attacks in wireless sensor networks." Military Communications Conference, 2007. MILCOM 2007. IEEE. IEEE, 2007.*Security* (IJCSIS), Vol. 2, 2009.
5. Bhattasali, Tapalina, RituparnaChaki, and SugataSanyal. "Sleep Deprivation Attack Detection in Wireless Sensor Network." arXiv preprint arXiv:1203.0231(2012).
6. Walters, John Paul, et al. "Wireless sensor network security: A survey."Security in distributed, grid, mobile, and pervasive computing 1 (2007): 367.Vol.2, Issue 4, pp. 450-455, 2012.
7. Kaur, Simerpreet, MdAtaullah, and Monika Garg. "Security from Denial of Sleep Attack in Wireless Sensor Network." INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY 4.2 (2013): 419-425.
8. Wu, Fang-Jing, and Yu-Chee Tseng. "Distributed wake-up scheduling for data collection in tree-based wireless sensor networks." Communications Letters, IEEE 13.11 (2009): 850-852.

## BIOGRAPHY

**RamandeepKaur**is aMtech student in the Computer Science Department, Guru kashi University. Her research interests are Computer Networks (wireless Networks).