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. 4, Issue 11, November 2016

Detection and Avoidance of Denial of Service Attack in WSNs

Muthukumar. S[1], Dr.Rubasoundar. K[2], Manikandamoorthi.K[3]

Associate Professor Dept. of Computer Science and Engineering, Sree Sowdambika College of Engineering, Tamilnadu, India[1]

Professor Dept. of Computer Science and Engineering, PSR Engineering College, Tamilnadu, India[2]

Dept. of Computer Science and Engineering, Sree Sowdambika College of Engineering, Tamilnadu, India[3]

Abstract: The Wireless Sensor Networks (WSNs) are emerging as one of the most reliable technologies for implementing ubiquitous computing ultimately leading to an all-pervasive paradigm of computing infrastructure that can be utilized for several interesting applications. Denial of Service (DoS) is an attack where a number of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. DoS attacks disrupt the entire or a part of WSN network. Detection and avoidance of DoS attacks is necessary. For that we design message observation and common key authentication mechanisms by which cluster head (CH) as well as any other sensor nodes in network can able to identify the communicating node is an attacker node or not and isolate that attacker node. This approach is efficiently, detects and avoids Dos attack completely.

KEYWORDS: Wireless Sensor Networks, Denial of service attacks, Security.

I. INTRODUCTION

Presently wireless sensor networks have gained universal attention and mainly spread in Micro-Mechanical System (MEMS) technology which has facilitated the growth of advanced sensors. These sensors are tiny, with narrow dealing out and computing resources and they are of low cost compared to conventional sensors. These sensor nodes can intellect, evaluate and congregate information from the surroundings and based on some local conclusion methods. WSNs have immense possibilities for applications in scenarios such as armed intention tracking and scrutiny, natural disaster relief, biomedical health monitoring, dangerous surroundings investigation and seismic sensing and in military target tracking and surveillance. WSN can also support in invasion finding and credentials. Natural disasters, sensor nodes can intellect and distinguish the environment to predict disasters before they arise. In biomedical applications, surgical implants of sensors can help to screen a patient's health. Sensors along the volcanic area can perceive the maturity of earthquakes and eruptions. The applications of WSNs include environmental control, habitat monitoring, object tracking, nuclear reactor control, fire detection and traffic monitoring. There exists various security attacks in wireless sensor networks such as: (i) Denial of Service attack (ii) Sink hole attack (iii) Black hole attack (iv) Worm hole attack (v) Selective forwarding attack (vi) Sybil attack (vii) Node replication attack.

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. 4, Issue 11, November 2016

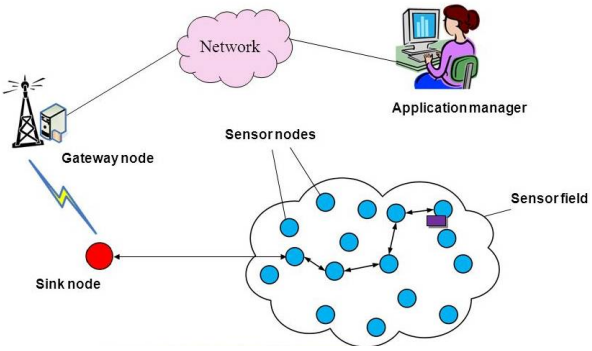

Fig 1: Architecture of WSN

The types of WSNs are structured WSN and unstructured WSN. Sensor nodes may be deployed in an ad hoc method into the field. WSN offer a bridge between the real physical and virtual worlds and posses the capability to monitor the wide range of possible applications to industry, science, transportation, civil infrastructure, and security. Wireless sensor networks present the capability for applications to scrutinize and respond to actions, but their isolation introduce challenges and vulnerabilities for network manage and energy consumption. Wireless networks are deployed in open RF communication link, and communication happens in the same frequency band. So radio snooping or spying is very easy. The sensor nodes are low-cost and use minimal resources like power, bandwidth, and storage. It is difficult to add strong security algorithms as those are complex to implement. As a result, sensor networks adopt low-cost modest security protocols. WSN is deployed in extreme climatic conditions and terrains. It is difficult to continuously to monitor these networks for potential attacks.
The rest of the paper

II. DENIAL OF SERVICE (DoS) ATTACKS

Any type of intentional activity that can disrupt, subvert or even destroy the network is known as a Denial of Service (DoS) attack. Basically, DoS attacks can be categorized into three types:
1. Consumption of scarce, limited or non-renewable resources.
2. Destruction or alteration of configuration information.
3. Physical destruction or alteration of network resources.
DoS attack target the network resources. The hardware of sensor nodes is typically constrained and attackers can try to overload them. The DoS attack is one of the major energy consumption attacks in a WSN. DoS attacks are dependent on the vulnerabilities of each layer in the layered architecture of wireless networks. The physical layer is being the lowest layer and the first to be attacked by jammers. This physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. As an outcome of DoS attack, the sensor node fails to function when the energy is exhausted. Sensor nodes are vulnerable against this type of physical attack. DoS attacks are very critical such as jamming attack and tampering attack. Jamming is the deliberated interference of the wireless communication channel. Tampering is another type of physical attack, which targets the actual hardware of the sensor nodes. In this attack, it is difficult to know whether any particular DoS situation is caused intentionally or unintentionally. [1] The WSN's denial of sleep attack is a subset of the Denial of Service class of network attacks. Stajano and Anderson first mention denial of sleep attacks in 1999 as "sleep deprivation torture". Energy –limited system designers often incorporate power management mechanisms to monitor active processes and power down non-essential subsystems when feasible. A denial of sleep attack penetrates a device‟s power management system to reduce the opportunities to transition into lower power states.

III. RELATED WORK

Several researchers have worked with different techniques to detect DoS attack and to identify the malicious nodes that source Denial of Service attack in wireless sensor networks.

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. 4, Issue 11, November 2016

Manju V.c and Sasi Kumar M [2] has proposed a technique for identifying jamming attack in the wireless sensor networks. Based on residual energy of nodes some of the existing nodes are marked as monitor nodes. These nodes collect the Receiver Signal Strength Indicator and packet delivery ratio from all the other nodes. Based on this metric, they compute a weight value of each node. The computed weight value is compared against the threshold value. When the estimated weight value goes beyond the threshold value, the corresponding node is marked as jammer and it is isolated from data transmission. This technique significantly improves system performance.

Michael Brownfield, et al., [1] has described the energy resource vulnerabilities of Wireless Sensor Networks. They also proposed a new MAC protocol which mitigates many of the effects of denial of sleep attacks. G-MAC has several energy-saving features. It shows guarantee in extending the network existence and also the centralized architecture makes the network more resistant to denial of sleep attacks.

Wenyuan Xu, et al., [4] has proposed two different but complementary approaches. First approach is to simply retreat from the interferer, which may be accomplished by either spectral evasion (channel surfing) or spatial evasion (spatial retreats). The second approach aims to compete more actively with the interferer by adjusting resources, such as power levels and communication coding, for achieve communication in the presence of the jammer. These techniques are important areas for studying and classifying the scenarios where one defense strategy is advantageous over another.

Mingyan Li, et al., [3] have derived solutions to the optimization problems, optimal attack and network defense strategies. They also found alternatives for modeling lack of knowledge for the attacker and the network. Hung-Min Sun, et al., [5] have multi dataflow topologies scheme to reduce the affected area caused by the mobile jamming attack. Mobile jamming attack not only causes the energy consumption but also breaks the routing on WSN and also shows that the existing defense mechanism is unable to withstand this attack.

Jan Blumenthal, et al., [6] has introduced Weighted Centroid Localization technique to make it fast and easy for the algorithm to locate devices in wireless sensor networks.WCL algorithm is derived from a centroid determination which calculates the position of devices by averaging the coordinates of known reference points. They summarized the basic theoretical and practical facts concerning the analysis of RSSI measurements.

David R. Raymond and Randy C [7] have classified the Lightweight Medium Access Control (LMAC) technique. Initially, it classified denial-of-sleep attacks on WSN medium access control protocols based on attacker's knowledge of the MAC protocol and ability to penetrate the network. Next, it explored potential attacks from each attack classification. The impact on sensor networks running for leading WSN MAC protocols and analyzing the efficiency of implementations of these attacks. Finally, it proposed a framework to defend against denial of- sleep attacks and provides specific techniques that can be used against the vulnerability of each denial-of-sleep.

IV. SYSTEM ARCHITECTURE

In WSN, the authenticated servers create and circulate special keys for every node. It likewise keeps up the details of attacker node. Subsequent to getting the key from server every nodes produce the hash code. At whatever point a node needs to make communication with some other node in a network for first time it needs to demonstrate its character in addition to the verification data to their separate cluster head in order to access service.

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. 4, Issue 11, November 2016

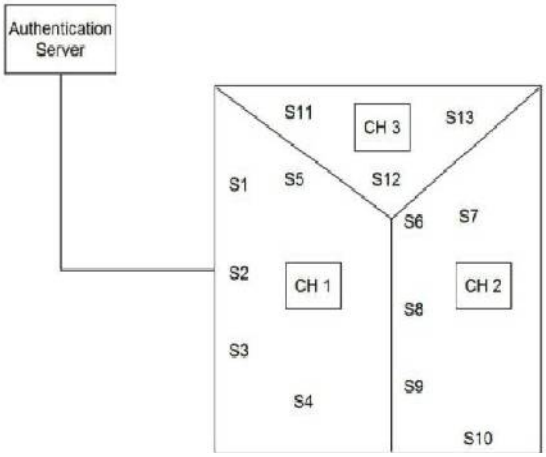

Fig 2: System Architecture

Cluster heads get and check the verification. On the off chance that it verified then begin correspondence with that sensor node. After begin communication the framework at the cluster head recognize whether it get typical or strange messages and drop the anomalous messages. One node haphazardly sends the irregular messages; consider that node as attacker node. In the wake of recognizing the attacker node, report to the server. At that point server overhauls the details of the attacker node, produce and disperses the new keys to every one of the nodes in the area of the cluster with the exception of the attacker node which attempts to re-impart, cluster head confirm the verification, it not verified thus drop the network communication.

V. SYSTEM MODULES

A. REGULAR CASE

A consideration made on the network with numerous sensor nodes and the network is partitioned into many clusters as shown in figure 2. At every cluster, there is a node called Cluster Head (CH) that deals cluster members, for example, gathering data or discharge necessities and so forth. In the mean time, the cluster members accumulate and submit data to the CH, and after that the CH combine and forward the data to the base station. Once the cluster has created, all cluster members' identities (IDs) register in CH. Validated server produce and convey the special keys to every node. After get those special keys of sensor nodes and cluster head produce the hash code utilizing hashing capacities. After beginning stage, the novel node will be confirmed by CH and neighbor nodes.

B. ATTACK CASE

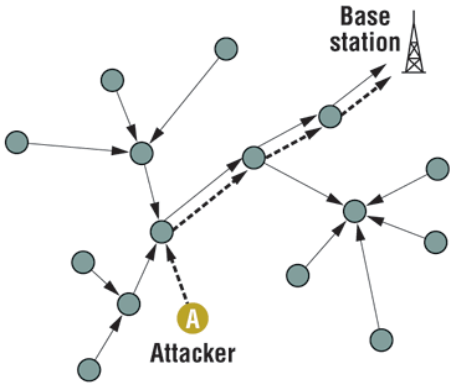

Fig 3: Attack model

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. 4, Issue 11, November 2016

A malicious node is created in the attack module which tries to infuse huge quantities of counterfeit messages or replayed messages to the cluster head to intrude on communication as appeared in figure 3. At last our general network has been contaminated.

C. DETECTION AND AVOIDANCE PROTOCOL CASE

In order to make communication with all nodes in WSN, initially it must send request message with hash code to its particular cluster head. At that point the cluster head check and confirm the source node, on the off chance that it validate then just get the message generally discard the transmission with that particular node. Furthermore, here we outline a Message observation technique to identify the DoS attack, and after that devote the representing countermeasure, an attack avoidance protocol in detail.

a. *Message Observation Mechanism*

We design the message observation mechanism at each cluster head. This mechanism keeps the regular and irregular message list. Given Φ is Regular, and Φ= {nm1|nm2,…,nm|Φ|}, nmi is a representative message which has been submitted successfully. Before deployment, Φ=ϕ. The nmi is a triple as <msg, timestamp, counter>, where msg indicates the content of representative message, timestamp indicates the last time when the msg has been submitted, which can be used to determine whether the expired counter indicates the number of times the message is transmitted. Given Ψ is AML, and Ψ= {am1|am2,...,am|Ψ|}, ami is a representative message which has been considered as bogus messages. Before deployment, Φ=ϕ. The ami is a tuple as <msg, timestamp >, where msgindicates the content of irregular message, time stamp indicates the last time when the meaasge has been considered as irregular message.

b. *Detection Protocol*

In order to recognize the DOS attack, we regularly take two prospects, the quantity of messages and the subject of messages. In the wake of accepting the message it assure whether the received message is regular, irregular or novel message and if that message is regular then contrast the counter measure and the threshold measure if it more prominent then consider that source as an attacker node and if the message is irregular then consider that source node as attacker node, if the received message is a novel one then add that message to the regular message list furthermore check the threshold measure in the event that it crosses then note that node as malevolent node.

Algorithm for Detecting the DOS Attack

Step 1: Obtain the message which is in need to transmit.
Step 2: Assure whether that message belongs to regular or irregular messages.
Step 3: If that message is irregular then take the source node as a malevolent node.
Step 4: If that message is regular then contrast the count and threshold measure, in the event that it crosses the threshold measure then take that source node as attacker node.
Step 5: Go to step 1

c. *Avoidance Protocol*

In the wake of deciding the attacker node, the CH send the warning message to the validated server node, server include that data in its attacker list , create and disseminate the novel keys to every nodes present in that region of with the exception of the attacker node. Additionally CH communicates the attack id to every sensor nodes and notifies that don't get the message from that particular id. Despite the fact that attacker node attempts to make communication with the node it not validated so transmission get discarded. Assume if the attacker node attempt to make communication with other CH, there additionally it not get verified.

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. 4, Issue 11, November 2016

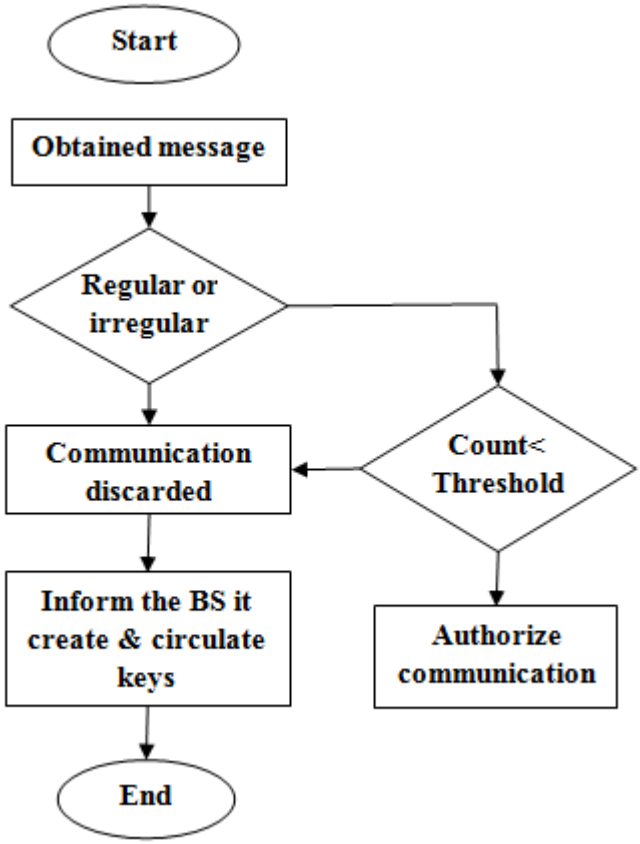

Fig 4: Flow of the proposed work

Algorithm for Avoiding the DOS Attack

Step 1: CH sends warning message, comprise the details of attacker to the.

Step 2: Server keep that data in its history record, produce and circulate the novel keys to every one of the noses in the region of cluster apart from the attacker node.

The figure 4 shows the flow of the overall process. Initially take off the server node and determining the attacker node. The CH get the message from the source node and it check whether its regular or irregular, in the event that it irregular or if the message is regular then contrast number and the threshold measure, on the off chance that it crosses then consider that node as attacker node and discard the transmission with that node. CH inform to the Base Station (BS) , the BS create and disseminate the novel key to every other node in the region of cluster then take that hub as attacker node and notify to the base station else authorize the communication with that node.

VI. CONCLUSION

Wireless sensor network research is transitioning to interesting real-world applications. As the networks become more pervasive and accessible, they will face some of the same problems with which wired Internet and wireless ad hoc networks already struggle. One such problem is denial-of-service. In this paper we design secure cluster head at each cluster. This maintains the regular and irregular messages list. And fix the threshold values for each message. And this system also uses a common key authentication isolate the malicious node. To achieve this there will be an authentication server which has to send a common key for all the sensor node and cluster head whenever need arises. This approach is efficient and avoids Dos attack completely.

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. 4, Issue 11, November 2016

REFERENCES

[1] Michael Brownfield, Yatharth Gupta "Wireless Sensor Network United Denial of Sleep Attack" Proceedings of the 2005 IEEE Workshop on Information Assurance States Military Academy, West Point, NY June 2005
[2] Manju V.c, Sasi Kumar M "Detection of Jamming Style DoS attack in Wireless Sensor Network" IEEE International Conference on Parallel Distributed and Grid Computing 2012
[3] Mingyan Li, Iordanis Koutsopoulos, Radha Poovendran "Optimal Jamming Attacks and Network Defense in Wireless Sensor Networks" IEEE Transactions on Mobile Computing August 2010
[4] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang "Jamming Sensor Networks: Attack and Defense Strategies. IEEE Network. May/June 2006
[5] Hung-Min, Shis-Pu, Chien Ming Chen, "Mobile Jamming Attack and its countermeasure in Wireless Sensor Networking and Applications" Workshops 21 st International conference on Advanced Information Networking and Applications Workshops, 2007.
[6] Jan Blumenthal, Ralf Grossmann, Frank Golatowski and Dirk Timmermann, "Weighted Centroid Localization in Zigbee-based Sensor Networks", IEEE International Symposium on Intelligent Signal Processing, (WISP 2007), pp-I-6, 2007
[7] David R. Raymond, Randy C "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols "IEEE Transactions on Vehicular Technology, Vol 58, hNo.I January 2009.