THE TECHNIQUE TO DETECT AND AVOID THE DENIAL OF SERVICE ATTACKS IN WIRELESS SENSOR NETWORKS

Nagarathna C.R[1], Chinnaswamy C.N[2]

[1]*Dept of CSE, NIE, Mysore, India*
[2]*Dept of CSE, NIE, Mysore India*

Abstract

Wireless Sensor Networks (WSNs) have being used in many fields like ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, military applications and health related applications. The harsh and unattended deployment of these networks along with that in wireless sensor networks each node has limited energy, computation and storage space makes they are more vulnerable to attacks than wired networks. . It is a critical challenge to present the effective and lightweight security protocol to prevent various attacks for WSN, especially for the denial of service (DOS) attack. However, the adversaries can compromise some sensors and launch the DoS attack by replaying redundant messages or making overdose of fake messages. Under this situation, DoS attack breaks off the wireless communication channel and causes either unintentionally in the form of interference, noise or collision between the block the communication bandwidth, which makes the network not work well even fail down. In this paper 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, detect and avoids Dos attack completely.

Keywords-*Wireless Sensor Networks, Denial of service attacks, Security*

----------***----------

1. INTRODUCTION

Wireless Sensor Networks (WSNs) often considered as a self-organized network of low cost, power and complex sensor nodes have been typically designed to monitor the environment for physical and chemical changes, disaster regions and climatic conditions. The sensor nodes are light and portable, with sensing abilities, communication and processing board, and are used for sensing in critical applications. The figure1 shows the example of wireless sensor networks.

- The Sensor nodes that form the sensor network. Their main objectives are making discrete, local measurement about phenomenon surrounding these sensors, forming a wireless network by communicating over a wireless medium, and collect data and rout data back to the user via sink (Base Station).
- The sink (Base Station) communicates with the user via internet or satellite communication. It is located near the sensor field or well-equipped nodes of the sensor network. Collected data from the sensor field routed back to the sink by a multi-hop infrastructure less architecture through the sink.
- The user who is interested in obtaining information about specific phenomenon to measure/monitor its behaviour.

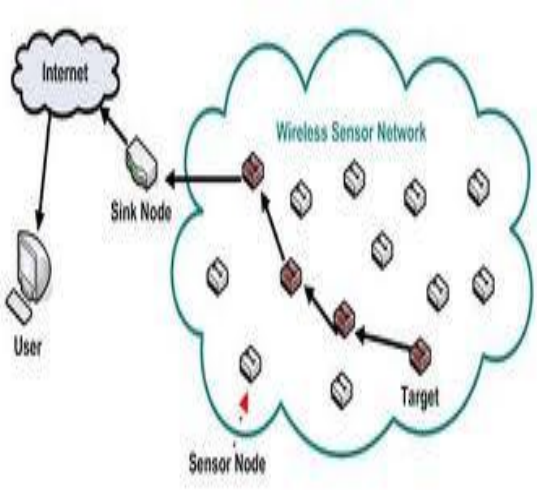

Fig 1 Wireless sensor network

The harsh and unattended deployment of these networks along with that in wireless sensor networks each node has limited energy, computation and storage space makes, Wireless networks are easily subjected to intentional or unintentional attacks than the wired based networks. The simplest form of such attacks is denial of service attack which can block any current legitimate communication. However, the adversaries can compromise some sensors and launch the DoS attack by replaying redundant messages or making overdose of fake messages . The **denial-of-service (DoS)** is an attempt to make a machine or network resource unavailable to its intended users. Due to the severe security attacks in the wireless media,

the network faces various difficulties. Prevention of DOS attack has become a very serious problem in network security.

In this paper we design secure cluster head at each cluster. Cluster head maintains the normal and abnormal messages list. And fix the threshold values for each messages. And this system also uses a common key authentication isolate the malicious node. This system is efficient and avoids Dos attack completely. 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.

Whenever a node has to communicate with another node in a network for first time it has to show its identity plus the authentication information to get service. The authentication information is formed by using hashing technique on certificate credential. After receiving the message it distinguishes whether it is normal or abnormal messages and also check the threshold value. It simply drop the abnormal message and increment the count compare it with threshold value, if it crosses then sender node is consider as attacker node. Once a node s1 trying to communicate with CH1 (cluster head) ,s1 has to produce its authentication (Hash Code) .In case CH1 identifies s1 is an attacker node then it will inform to authentication server. Once authentication server got information about attacker node it has to send a new key to all other nodes except attacker node. Consider now s1 node has moved from cluster1 to cluster2 and trying to communicate with CH2 , at that time it has to produce the hashing code for authentication. CH2 has to generate hash code with new key and compare with hash code with s1 node which will not match. So, that CH2 easily identifies s1 is an attacked node.

2. RELATED WORKS

WSNs are vulnerable to the DoS attacks since they are energy-constrained devices without a central powerful monitoring point [1]. Meanwhile, there are deferent types of DoS attack in the layers protocol of sensor network . According to Chaudhari H.C. and KadamL.U[2].Based On the Capability of the Attacker attacks can be characterised as **Outsider versus insider (node compromise) attacks**: Outside attacks are defined as attacks from nodes, which do not belong to a WSN; insider attacks occur when legitimate nodes of a WSN behave in un intended or unauthorized ways. **Passive versus active attacks:** Passive attacks include eavesdropping on or monitoring packets exchanged within a WSN; active attacks involve some modifications of the data steam or the creation of a false stream Many solutions of different sensor network routing protocols are designed to enhance the security of sensor network . Some examples areCAD algorithm[3] is used to detect the selective forwarding attack.Code Guard[4] uses digital signature to identify pollution attack&Honey node algorithm[5] for jamming attack.

In Ref. [6], the authors designed a one-way hash chain (OHC) to protect end-to-end communications in WSNs from path-based DoS attacks. The OHC deploys an OHC in each intermediate node of path to detect a PDoSattack. OHC put a new OHC number for every message from source. Therefore, the messages, which can be authenticated correctly in the chain, can only be transferred. However, OHC did not provide any protection for the data transmission between the member nodes and the CH, which is threatened by the attacks. Therefore , it not provide any protection for the head of the network , the attacker node may attack head and disrupt overall functions of the network.

3. SYSTEM ARCHITECHTURE

The authenticated server generate and distribute unique keys for each nodes in the network. It also maintain the attacker node details. After receiving the key from server each nodes generate the hash code. Whenever a node has to communicate with another node in a network for first time it has to show its identity plus the authentication information to their respective cluster head for access service . Cluster heads receive and verify the authentication. If it authenticated then start communication with that sensor node. After start communication the system at the cluster head identify whether it receive normal or abnormal messages and drop the abnormal messages. One node randomly sends the abnormal messages, consider that node as attacker node. After detecting the attacker node, notify to the server. Then server update the attacker node details, generate and distribute the new keys to all the nodes in the cluster region except the attacker node. When the attacker node try to re-communicate, cluster head verify the authentication, it not authenticated so drop the communication.

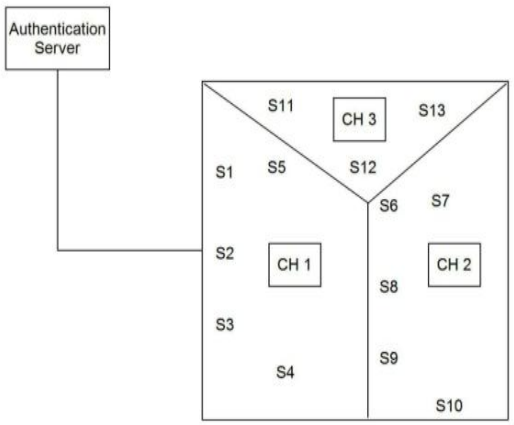

Fig 2 System architecture

4. SYSTEM MODULES

4.1 Normal Case

Consider the network with many sensor nodes . Divide the network into many clusters as shown in figure2. In each cluster, there is a node named CH(cluster head) which manages member nodes, such as collecting information or release requirements etc. Meanwhile, the member nodes gather and submit information to the CH, and then the CH aggregate and forward the information to the base station. Once the cluster formed, all member sensors' identities (IDs) register in CH. Authenticated server generate and distribute the unique

keys to each nodes. After receive the keys sensor nodes and cluster head generate the hash code using hashing functions. After initial phase, the new node will be authenticated by CH and neighbour nodes.

4.2 Attack Case

In Attack module we create one node as attacker (malicious) node. Malicious node tries to inject large numbers of bogus messages or replayed messages to the cluster head in order to interrupt communication as shown in following figure 3. Finally our overall network has been Infected.

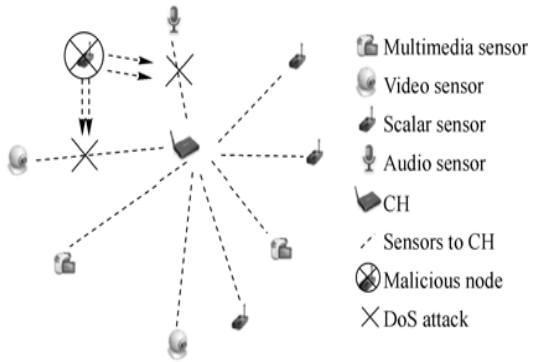

Fig 3 Attack model

4.3 Detection and Avoidance Protocol Case

To communicate with any nodes in the network first it should send the request with hash code to their respective cluster head. Then cluster head verify and authenticate the sender node, if it authenticate then only receive the message otherwise discard the communication with that node. And herewe design a Message observation mechanism to detect the DoSattack, and then give the corresponding countermeasure, a avoidance protocol in detail.

4.3.1 Message Observation Mechanism

We design the message observation mechanism at each cluster head. This mechanism keeps the normal and abnormal message list. Given Φ is Normal, 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 abnormal message, timestampindicates the last time when the msg has been considered as abnormal message.

4.3.2 Detection Protocol

To detect DOS attack, we normally consider two aspects, the number of messages and the content of messages. After receiving the message it check whether the received message is normal , abnormal or new message and if the message is if the message is normal then compare the counter value with the threshold value if it greater then consider that sender as a attacker node , if the message is a abnormal then consider that sender node as attacker node,if the message is new one then add that message to the normal message list and also check the threshold value if it crosses then consider that node as malicious node.

Algorithm for Detecting the DOS Attack

Step 1**:** Receive the input message.
Step 2**:** Check whether the message belong to normal or abnormal messages.
Step 3**:** If the message is abnormal then consider the sending node as malicious node.
Step 4**:** If the message is normal then compare the count and threshold value, if it crosses the threshold value then consider that sending node as attacker node.
Step 5: Go to step 1

4.3.3 Avoidance Protocol

After determining the attacker node,cluster head send the notification message to the authenticated server node, server add that information in its attacker list , generate and distribute the new keys to all the nodes in that cluster region except the attacker node. Also cluster head broadcast the attacker id to all its sensor nodes and inform that don't receive the message from that id. Even though attacker node try to communicate with the node it not authenticated so communication get discarded. Suppose if the attacker node try to communicate with other cluster head , there also it not get authenticated.

Algorithm for Avoiding the DOS Attack

Step 1: Cluster head send notification message, consist attacker details to the server.
Step 2: Server store that info in its history record ,generate and distribute the new keys to all the nodes in the cluster region except the attacker node.

The overall process flow is shown in following diagram4. First start the server node and setting the attacker node. The cluster head receive the message from the sensor node and it verify whether its normal or abnormal, if it abnormal or , if the message is normal then compare count with the threshold value , if it crosses then consider that node as attacker node and discard the communication with that node. Cluster head notify to the base station , the base station generate and distribute the new key to all other nodes in cluster region then consider that node as attacker node and inform to the base station else pass the communication with that node.

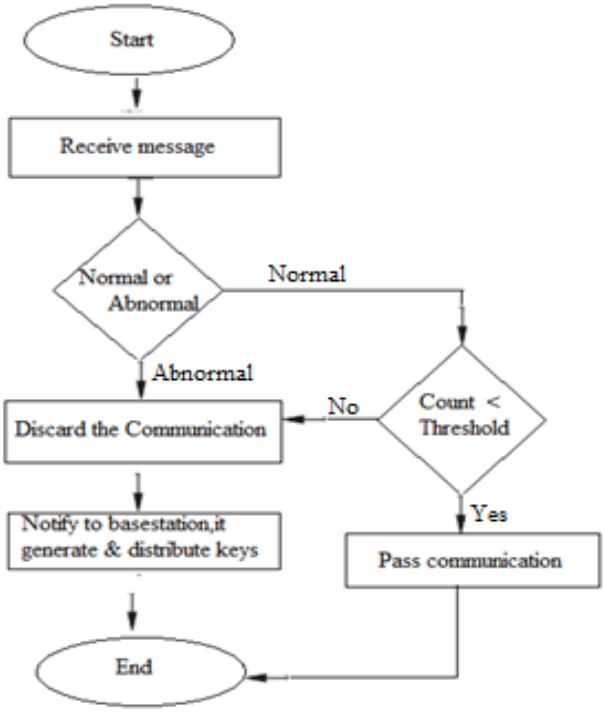

Fig 4 Process flow

5. CONCLUSIONS

It is a critical challenge to present the effective and lightweight security protocol to prevent various attacks for WSN, especially for the denial of service (DOS) attack. In this paper we design secure cluster head at each cluster. This maintains the normal and abnormal 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.

REFERENCES

[1]. "Denial of service attacks in wireless sensor networks: issues and challenges" Al-Sakib Khan Pathan1 Department of Computer Engineering, Kyung Hee University1 Seocheon, Giheung, Yongin 446-701, South Korea .

[2]. "Chaudhari H.C. and Kadam L.U.S wami Vivekanand Mahavidyalaya "Wireless sensor networks: security attacks and challenges".

[3]. DevuManikantanShila, Yu cheng, and Tricha Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNs",IEEE transactions on wireless communications, vol. 9, no. 5 , may 2010.

[4]. G.Lin and G.Noubir . "On link layer Denial of service in data wireless LANs". Wireless communications and MobileComputing, 5(3):273-284, May 2004.

[5]. SudipMisra, Sanjay K. Dhurandher, AvanishRayankula and DeepanshAgrawal, "Using honey nodes for defense against jamming attacks in wireless infrastructure-based networks", computers and electrical engineering, may 2009.

[6]. Deng J, Han R, Mishra S. "Defending against path-based DoS attacks in wireless sensor networks". SASN'05, ACM New York, NY, USA, 3rd ACM workshop on Security of Ad Hoc and Sensor Networks Table of Contents Alexandria, VA, USA, Nov 7, 2005: 89−96.