Prevention of Dos Attacks in Wireless Sensor Networks

M.Annapoorani#1, D.Kiruthika#2, V.Geethamani#3
[#]*Department of Computer Science and Engineering, Tejaa Shakthi Institute of Technology for Women, (Affiliated to Anna University, Chennai), Karumathampatti, Coimbatore.*
[1]m.annapoorani2@gmail.com
[2]mails4kiruthi@gmail.com
[3]vgeethamanismr@gmail.com

Abstract-- **In wireless sensor networks attackers can inject unwanted messages through the nodes which are already being captured by attackers and they inject DOS attacks against reports. The attackers try to launch the false reports also. A number of filtering schemes to avoid these attacks have been introduced which cannot filter strongly. In our scheme each node consists of its own authentication key. Before sending the reports the key is forwarded to the the next node through which it has to send the message. The key generates a code .The message also generates a code. Both the codes are checked for similarity. If both codes are similar then the message is valid. The message is then forwarded to its destination. make use of Hill climbing approach to find the shortest path in which the reports can reach its destination. our scheme can provide strong filtering capacity and memory requirement is low. Our scheme can also remove the false reports ealier.In existing scheme only one path is available for the reports .In our scheme multipath is applicable.**

Keywords-- **DOS Attacks, DDOS Attacks, MAC, Filtering scheme**

I. INTRODUCTION

In wireless sensor networks large number of nodes is present. These sensor networks have less memory space and suffer more attacks. The following are the attacks. Injecting unwanted message attacks, Selecting and forwarding attacks, Message distribution attacks. In injecting unwanted message attack the attackers try to inject the false reports into the sensor networks .The false reports contain faked information's and events which do not exist. Thus the DOS attacks are launched.

A. SEF (Statistical enroute filtering)

In selective forwarding attacks the reports are selectively attacked and removed. SEF is independent of network topology, but it has limited filtering capacity and cannot prevent impersonating attacks on legitimate nodes.

In SEF [3], a global key pool is divided into n partitions, each containing m keys. Every node randomly picks k keys from one partition. When some event occurs, each sensing node (that detects this event) creates a MAC for its report using one of its random keys. The cluster-head aggregates the reports from the sensing nodes and guarantees each aggregated report contains T MACs that are generated using the keys from T different partitions, where T is a predefined security parameter.

B. IHA (Interleaved hop by hop authentication)

IHA has a drawback [2], that is, it must periodically establish multihop pair wise keys between nodes. Moreover, it asks for a fixed path between the base station and each cluster-head to transmit messages in both directions, which cannot be guaranteed due to the dynamic topology of sensor networks or due to the use of some underlying routing protocol such as GPS

II. METHOD OF ATTACK

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services.[4] Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System servers.

A DoS attack can be perpetrated in a number of ways. The five basic types of attack are:[citation needed] Consumption of computational resources, such as bandwidth, disk space, or processor time. Disruption of configuration information, such as routing information. Disruption of state information, such as unsolicited resetting of TCP sessions. Disruption of physical network components. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

III. OVERCOMING DOS ATTACKS

The technique of IP trace back is used to overcome Denial-of-Service attacks. This paper deals with explaining the two types of IP trace back techniques namely, Packet Marking and Packet Logging which have been proposed earlier

It explains about a hybrid IP trace back technique which uses both packet marking and logging. The hybrid technique claims to have a better performance level in terms of reducing the storage overhead at the routers by half and the access time overhead by the number of neighboring routers. Future enhancements have been proposed in the domain of security for the entire system. The following are some of the methods to overcome DOS attacks.

- Strong filtering capacity
- Key generation
- Multiple paths for the message to travel
- Formation of clusters to make the process easier
- Detecting the active nodes and inactive nodes

A. Packet marking

All marking algorithms have two components: a marking procedure executed by routers in the network and a path reconstruction procedure implemented by the victim. A router "marks" one or more packets by augmenting them with additional information about the path they are traveling. The victim attempts to reconstruct the attack path using only the information in these marked packets. The various marking techniques proposed in this by

1) Sampling and Edge Sampling

Node Append similar to the Record Route option consists of appending each node‘s address to the end of a packet as it traverses through the network from attacker to victim. Node Sampling is used to reduce both the router overhead and the per-packet space requirement, by sampling the path one node at a time instead of recording the entire path. A single static "node" field is reserved in the packet header-large enough to hold a single router address (i.e., 32 bits for IPv4).

Upon receiving a packet, each router chooses to its address in the node field with some probability p. After enough packets have been sent, the victim will have received at least one sample for every router in the attack path. The Edge Sampling technique is used to explicitly encode edges in the attack path rather than simply individual nodes. To do this, reserve two static address sized fields, start and end, in each packet to represent the routers at each end of a link, as well as an additional small field to represent the distance of an edge sample from the victim.

When a router decides to mark a packet, it writes its own address into the start field and writes a zero into the distance field. Otherwise, if the distance field is already zero this indicates that the packet was marked by the previous router. In this case, the router writes its own address into the end field—thereby representing the edge between itself and the previous router—and increments the distance field to one. Finally, if the router does not mark the packet, then it always increments the distance field.

B. Packet logging

Al-Duwairi and G. Manimaran in their paper titled Novel Hybrid Schemes Employing Packet Marking and Logging for IP Trace back [6], explain two techniques namely, Distribute Linked List Trace back and Probabilistic Pipelined Packet Marking.

1. Distributed Linked List Trace back (DLLT)

DLLT is based on the ‗store, mark and forward‘approach with a fixed size marking field for each packet. Any router that marks a packet, stores the content of the marking field in a ‗Marking table‘maintained at the router or else it forwards it to the next router. A linked list is used because the marking field servers as a pointer to the last router that did the marking for a given packet and the marking table of that router contains a pointer i.e. an IP address to the previous marking router and so on. When a router receives a packet, it marks the packet with a probability ‗q‘. If it has been marked previously, the router stores this information before remarking it.

Here only a fraction of traffic is logged at each router without putting a heavy burden on the routers. For storage Bloom filters are used. Each router has a Digest Array (Bloom filter) and a Marking Information Table. Each packet has a 32-bit field which contains the IP address of the marking router.

2. Probabilistic Pipelined Packet Marking (PPPM)

Pipelining is used to allow more than one instruction to be in some stage of execution at the same time. A router that marks a packet represents a pipeline stage, the marking process represents the instruction, execution and the propagation of marking information from one marking router to another represents the flow of instructions in a pipelined system.

The objective of PPPM is to let the destination know about all routers that were involved in marking a certain packet, P, using a constant space in the IP packet header without incurring long term storage overhead at the intermediate routers. Each marking information field in PPPM at each packet has an IP address of the marking router (MR) and an ID used to link the marking done for a given packet by different routers. The fields required in

each packet for marking are a 32 bit IP address, an 8 bit TTL and a c bit ID.

IV. CONCLUSION

In this paper we have discussed about attacks and their types. Mainly we are handling the DOS attacks and how to overcome it. Already many schemes have been implemented to avoid DOS attacks but each one had its own disadvantages. To overcome these disadvantages we have used dynamic enroute filtering scheme, Hill climbing and Hash chaining algorithm to handle the DOS attacks.

V. REFERENCE

[1] .K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," in *Proc.IEEE INFOCOM*, 2006.

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-Hop authentication scheme for filtering of injected false data in sensor networks," in *Proc. IEEE Symp. Security Privacy*, 2004.

[3].Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route detection and filtering of injected false data in sensor networks," in *Proc. IEEE INFOCOM*, 2004.

[4].Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," in *Proc. IEEE INFOCOM*, 2006.

[5] Kavitha Choudhary, Meenakshi and Shilpa "Smurf Attacks: Attacks using ICMP" in *Proc. IJCST, March 2011*

[6] N.Ugtakhbayar, D.Battulga and SH. Sodbileg "Classification of Artificial Intelligence IDs for Smurf Attack" in *Proc. IJAIA, January 2012.*

[7] Kumar, S "Smurf based distributed Denial of Service(DDoS) attack Amplification in Internet" in *Proc. IEEE ICMP, July 2007.*

[8]www.sans.org/reading-room/whitepapers/detection/denial-of-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysis

[9]cseweb.ucsd.edu/~savage/papers/usenixSec03.pdf

