Identification of Denial of Service Attacks in WSN using Cluster mechanism

Srinivas Gadari
Assoc. Prof.
Department of ECE
Siddhartha Institute of Technology and Sciences
Narapally, Hyderabad, Telangana, India

Shirisha Munasa D
Assoc. Prof.
Department of ECE
Siddhartha Institute of Technology and Sciences
Narapally, Hyderabad, Telangana, India

Abstract- **A denial of service attack, as the name implies, is an attempt by an attacker to disable network assets such as applications or management. As a result, only authorized clients have access. DoS attacks have a significant impact on the network. As a result, effective detection of DoS attacks is critical to network resource security. We developed a new technique for detecting Denial of Service (DoS) attacks in clustered wireless sensor networks in this research. Our method is based on the decisions of manager nodes known as mNodes, which detect and report DoS attack activity. mNodes and typical sensor nodes make up each cluster. A mNode's job is to examine traffic and deliver a warning message to the cluster head if it detects any unusual traffic. The voting process for mNodes is dynamic and takes place on a regular basis, depending on the node's remaining energy. The proposed technique can extend the network's lifetime by limiting the amount of energy used by each sensor node, as well as improve security by preventing attacks.**

Key Terms: Wireless Sensor Network (WSN),Cluster Head (CH), Monitor Nodes (mNodes) and Denial of Service attack (DoS).

I. INTRODUCTION

A Wireless Sensor Network (WSN) is made up of a large number of tiny sensors that communicate with each other wirelessly. These sensors are small devices with limited computing and memory capabilities, and they run on a little amount of battery power. They detect, process, and store data. They generate a quantifiable response in the deployed environment. They have applications in the medical, environmental, and military fields. They keep an eye on physical phenomena like temperature to detect and prevent chemical, biological, and nuclear dangers [1, 2]. Different topologies, such as hierarchical, are feasible. Sensor nodes are structured or subdivided into clusters in this deployment. The remaining nodes in each cluster elect a common node known as the cluster head (CH) using a clustering method such as LEACH [3, 4] or HEED [5]. The CH is selected from a pool of regular sensor nodes with suitable resources such as residual energy, memory, and processing power. In this type of network, each sensor node provides data to its CH, which aggregates the data locally. The only node that can broadcast aggregated findings to another CH or a base station is the CH (BS). This transfer can be made directly from the CH to the BS using long-range radio transmission or by multi-hopping across other clusters' CHs. The MAC layer is an important topic in WSN [6-8] because of the restricted energy. Another key issue is the security of WSN deployment, which is a common and important necessity that is being thoroughly researched. The network's sensitive information should be safeguarded from unwanted access. Integrity and authenticity of data must be ensured. Another essential factor to consider is the availability of resources. The network is unavailable and does not fulfil its functions if the WSN's supplied services are not available to authorised users when they ask the BS. Sensor networks have limited resources and are occasionally unstable, making them more vulnerable to DoS attacks. A denial-of-service (DoS) assault is any incident that has the potential to cause significant damage. It hinders or eliminates a genuine user's capacity to access a service by reducing or eliminating the network's ability to perform routine activities [9, 10]. We describe a novel technique for detecting DoS attacks in sensor networks in this research. There are three sorts of nodes in each cluster: sensing nodes, mNodes (management nodes), and a cluster head. Although some mNodes are employed in [11], the authors do not examine the concept of energy in their work. The mNodes remain constant during the network's lifespan. They are only sent out to undertake detecting jobs. They don't detect or transmit data. Our contribution is to employ these unique, periodically elected nodes to validate traffic in the sensor network and to provide a dynamic solution that can avoid DoS attacks and extend sensor lifetime by minimizing and balancing energy consumption. The mNodes are

chosen on a regular basis by selecting sensors with the most remaining energy. As a result, each node in the network can be designated as a mNode to perform an analytical function or sense data as a regular sensor.

2.RELATED WORKS

Many research efforts have been undertaken to deal with DoSattacks in wireless sensor networks. [11] proposes a cluster-based intrusion detection system. It protects sensor networks from denial-of-service (DoS) attacks. This approach deploys a collection of special nodes known as "guarding nodes" (gNodes) that monitor, analyse, and report DoS attacks to their cluster head whenever something unusual occurs. There are three sorts of nodes in each cluster: gNode, cluster head, and sensor node. Any type of node could be hacked. The detection technique for various attack kinds, as well as the measures followed after detection, are investigated in this study for various node types. SPINS (Security Protocols for Sensor Networks) was proposed by Perrig et al. [12], and it includes two efficient symmetric key based security building blocks: SNEP and μTESLA. With low overhead, SNEP enables data confidentiality, two-party data authentication, and data freshness. It achieves two-party authentication and data integrity by using MAC and a shared counter between the sender and receiver for the cypher block in counter mode, which is incremented after each block. μTESLAuses one-way key chains with secure hash algorithms to deliver authenticated broadcast. To perform cryptographic operations, it divides time into time intervals, with the sender associating each key in the one-way key chain with one-time period. The LEACH method allows dividing the energy load among sensor nodes in hierarchical sensor networks where clusters are generated dynamically and frequently. Oliveira et al [13] propose SecLEACH, an improved version of LEACH, to address the difficulty of providing security to this type of network. It uses μTESLA and random key pre-distribution. They can be used to encrypt communications in a hierarchical network as well as to create dynamic clusters. Running a detection mechanism on each node in the network provides for perfect detection of DoSattacks, but this is not a practical solution in a restricted network. [14] proposes an efficient network arrangement of detection nodes for widespread detection of DoS attacks. This proposal not only places detection nodes at crucial points in a network, but it also reduces the number of these required nodes, lowering the cost and processing overheads. In the work [15], proposes an adaptive security design (SecCBSN) to protect clusterbased communication in sensor networks. It comprises of three modules that provide secure communication and authentication protocols between nodes in order to detect rogue nodes. A CH sets transmission and checks periods for its sensor nodes in each cluster. The core security module makes use of the TESLA certificate (TCert) to allow current nodes to authenticate new incoming nodes, allowing secure links and broadcast authentication between neighbors to be established. The intrusion detection module in SecCBSN guards against compromised nodes. It makes use of alarm return protocols, trust value evaluation, and node black and white lists propagation. The process of summarizing and integrating sensor data for minimizing the size of data transmission in the network is known as data aggregation. A cluster head is elected by the other nodes in a cluster-based sensor network to aggregate data locally and communicate the aggregation result to the base station. To maintain data confidentiality and authenticity, this procedure requires security methods. In wireless sensor networks, Ozdemir and Xiao [4] investigate the relationship between security and the data aggregation process. They give a comprehensive literature review by summarizing state-of-the-art data aggregation procedures, and they identify open research topics and future research directions based on this review.

3.PROPOSED TECHNIQUE

A. Architecture

A cluster-based sensor network contains sensor and it is a small device that collects data from a specified location and reports it to the base station. There are three types of nodes in each cluster: a cluster head, sensor nodes, and mNodes (management nodes). Only the cluster head has the ability to aggregate data and transmit it to the sink. Figure 1 depicts the suggested cluster-based technique for detecting DoS attacks in sensor networks.

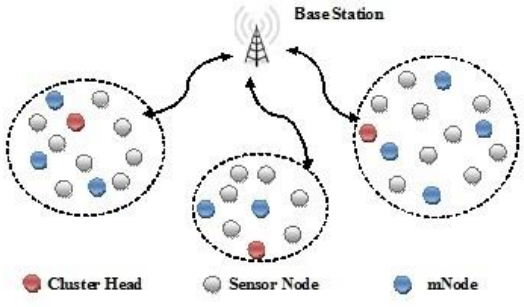

Figure 1: Architecture of proposed cluster

The cluster formation is done using any method such as LEACH [16, 4], in the sensor network.A set of special nodes is deployed in each cluster to examine

network traffic and detect odd behaviors. At time t, from all the nodes in the cluster with the maximum remaining energy, a set of mNodes is chosen. They are just used to analyses traffic and are not used for sensing. Another set of mNodes is chosen to replace the old mNodes at a specific period, and the latter become sensor nodes that do the sensing task, and so on. This can extend the network's life by reducing the amount of energy consumed by each sensor node, as well as increase security by preventing attackers from compromising mNodes and other nodes.

B. Operation Principle

We chose LEACH to form clusters in our network and elect the CH in each cluster. LEACH is the first clustering algorithm proposed to form sensor clusters and provides energy consumption equilibrium through a random rotation of CHs, allowing the system's energy requirements to be distributed among all sensors. In sensor networks, the mNodes are in charge of preventing DoSattacks. We have N sensor nodes in each cluster that use the LEACH protocol to elect a cluster head. Then, from among N nodes, we select k nodes that can be elected as mNodes. Because they are not frequently involved in packet transmission, some nodes in each cluster have higher residual energy. The cluster head selects this type of node because the cluster head collects information from all nodes in the cluster and all cluster processes are performed without the cluster head's knowledge. After a certain amount of time, a new set of k nodes, referred to as mNodes, is chosen to replace the old mNodes. These k nodes are the ones with the largest leftover energy and can do network traffic analysis. Once these nodes have been selected, they begin monitoring traffic using a statistical technique described later in this section. The goal of this approach is to provide a way to elect these manager nodes on a regular basis in order to avoid energy depletion and limit the risk of attackers discovering these nodes. We have a different set of mNodes, a cluster head, and sensing nodes in each cluster at each period.

4. SIMULATION RESULTS

Figure 2 shows the detection rate for various numbers of Node groups and varied group sizes. In all of the graphs, the same node is compromised. The number of Nodes is determined by the cluster size. The entire network is divided into three clusters, with 5 Nodes in green color, 12 Nodes in red color, and 20 Nodes in blue color. chosen for each cluster size. Figure 2 shows the detection performance of these Nodes on the relevant clusters.

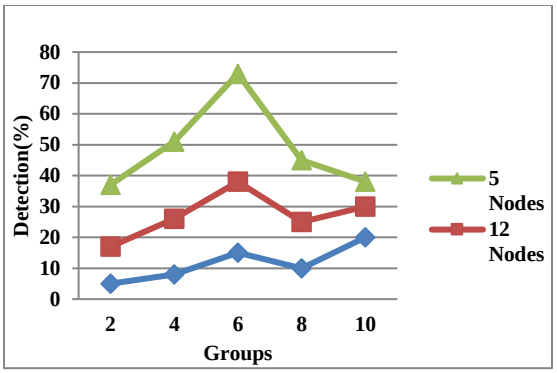

Figure 2: Detection Vs Group

Figure 3 shows the detection rate as a function of the number of Nodes employed. We provide two outcomes, one for a five-cooperation-node system and the other for a 15-cooperation-node system. It's worth noting that the detection rate rises with the number of Nodes, and that with 12 Nodes, we already have a significant enough percentage of attack detections.

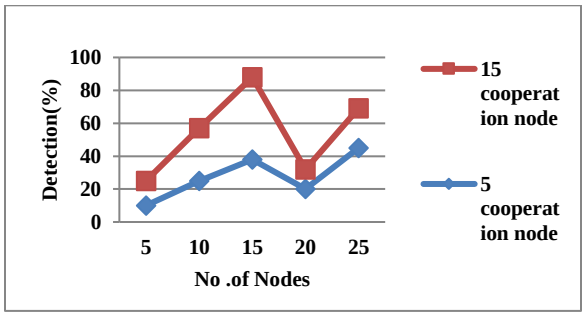

Figure 3: No.of Nodes Vs Detection (%)

5. CONCLUSION

It is extremely difficult to protect a sensor from a DoS attack due to its limited capabilities. Detection of DoS techniques, which can be used in wired or remote network environments but can't be used in sensor networks due to sensor capacity limitations and the lack of centralized monitoring and management. It is critical to consider DoS attacks and develop detection mechanisms since they can have devastating consequences. We presented a dynamic approach for cluster-based detection networks in this paper. Some special nodes, known as mNodes, are chosen to monitor and report DoS attack activity to the cluster head. The chosen mNodes change over time in order to avoid energy usage and reduce the likelihood of attackers recognising these nodes. In comparison to the static strategy, our proposed method has a few advantages. It detects a number of attacks. It maintains network energy by adjusting the cluster's mNodes. It performs load balancing and extends the network's

lifespan. Furthermore, it improves network security by avoiding an attacker's prediction of mNode.

REFERENCES

[1] Bai Li and Lynn Batten:"Using mobile agents to recover from node and database compromise in path-based DoS attacks in wireless sensor networks". Journal of Network and Computer Applications 32 (2009), pp. 377- 387.
[2] WR. Claycomb and D. Shin:"A novel node level security policy framework for wireless sensor networks". Journal of Network and Computer Applications 34 (2011), pages 418-428.
[3] Heinzelman WR et al:"Energy-Efficient Communication Protocol for Wireless Microsensor Networks". Proceedings of the IEEE Hawaii international conference on system sciences, 2000.
[4] S. Ozdemir and Y. Xiao:"Secure data aggregation in wireless sensor networks: A comprehensive overview". Computer Networks 53, pages 2022- 2037, 2009.
[5] O. Younis, S. Fahmy:"HEED: a hybrid, energy-efficient distributed clustering technique for ad hoc sensor networks". IEEE Trans. Mobile Comput. 3 (4), pages 366-379, 2004.
[6] J. Ben-Othman and B. Yahya:" Energy Efficient and QoS based Routing Protocol for Wireless Sensor Networks". Elseiver Journal of Parallel and Distributed Computing (JPDC), Volume 70, Number 8, pp. 849-857, August 2010
[7] B. Yahya and J. Ben-Othman"Energy Efficient and QoS Aware Medium Access Control for Wireless Sensor Networks". Wiley (Concurrency and Computation : Practice and Experience), Volume 22, Number 10, pp. 1252-1266 July 2010.
[8] B. Yahya and J. Ben-Othman:"Towards a Classification of Energy- Aware MAC protocols for Wireless Sensor Networks". Wiley Wireless Communications and Mobile Computing (WCMC), Volume 9, Issue 12, Feb. 2009, Pages 1572-1607.
[9] F. Hu and N. Sharma:"Security considerations in ad hoc sensor networks". Ad Hoc Networks 3 (2005)
[10] AfrandAgah and Sajal K. Das:"PreventingDoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Technique". International Journal of Network Security, Vol.5, No.2, pages 145-153, Sept. 2007.
[11] GuHsin Lai and Chia-Mei Chen:"Detecting Denial of Service Attacks in Sensor Networks". Journal of Computers Vol.18, No.4, January 2008.
[12] Adrian Perrig et al:"SPINS: Security Protocols for Sensor Networks". Mobile Computing and Networking 2001 Rome, Italy.
[13] Leonardo B. Oliveira et al:"SecLEACH, On the security of clustered sensor networks". Signal Processing 87 (2007), pp. 2882-2895.
[14] M.H. Islam et al:"Optimal Sensor Placement for Detection against Distributed Denial of Service Attacks". Pakistan Journal of Engineering and Applied Sciences, vol4, Jan 2009, pp. 80-92.
[15] Heinzelman WR et al:"Energy-Efficient Communication Protocol for Wireless Microsensor Networks". Proceedings of the IEEE Hawaii international conference on system sciences, 2000.