ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Cluster based Detection of Denial of Service Attacks in Wireless Sensor Networks

Muthukumar. S [1], Dr.Rubasoundar [2] . K , 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: Denial of Service attack, from the name itself demonstrates is essentially an endeavor by an attacker to debilitate the assets accessible to a network such as application or administration. Therefore authorized clients can't get any access. DoS attacks induce severe effect on the network. Accordingly, viable recognition of DoS attacks is basic to the security of network resources. In this paper, we presented a new strategy for distinguishing Denial of Service (DoS) attacks in cluster based wireless sensor networks. Our technique depends on the decision of manager nodes called mNodes which discover and report the activities of DoS attack. Each cluster comprises of mNodes and typical sensor nodes. The part of a mNode is to examine the traffic and to send a warning message to the cluster head if any anomalous traffic is recognized. The election process of mNodes is dynamic and conducted occasionally based on node's remaining energy. The proposed technique can enhance the lifetime of the network by limiting the energy utilization for every sensor node and can enhance security by avoiding attacks.

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

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of a sufficient number of small size sensors which communicate wirelessly with each other. These sensors are tiny devices with limited computing capability, and memory and operated with limited battery energy. They sense, process and store information. They produce a measurable response the deployed environment. They can be used in medical, environmental and military sectors. They monitor physical phenomena such as temperature in order to detect and prevent chemical, biological or nuclear threats [1, 2]. Different topologies are possible such as hierarchical. In this type of deployment, sensor nodes are organized or subdivided into clusters. In each cluster, a common node called cluster head (CH) is elected by the other nodes using one clustering algorithm such as LEACH [3, 4] or HEED [5].

The CH is chosen among ordinary sensor nodes that have sufficient resources such as residual energy, memory and computing capacity. In this type of network, each sensor node sends data to its CH and the CH performs locally aggregation on the received data. The CH is the only node that can relay aggregated results to another CH or a base station (BS). This transmission can be achieved directly from the CH to BS via long range radio transmission or by multi-hopping through CHs of other clusters. Due to the limited energy, the MAC layer is an important topic in WSN [6-8]. Another important issue is the security related to WSN deployment which is an important and frequent requirement that is being investigated extensively.

Sensitive information produced by the network should be protected from unauthorized discovery. Data integrity and authenticity must be guaranteed. Availability is another important issue that must be taken into consideration. If the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

delivered services by the WSN are not available to authorized users when they ask the BS, then the network is unavailable and does not fulfill its functions. Sensor networks have limited resources and are sometimes unstable, thus they are more vulnerable to Denial of Service (DoS) attacks. A DoS attack is any event which may have serious impacts. It reduces or eradicates the network ability to achieve its ordinary tasks or prevents a legitimate user from using a service [9, 10]. In this paper, we present a novel technique for detecting DoS attacks in sensor networks. In each cluster we have three types of nodes, sensing nodes, mNodes (manager nodes) and a cluster head. Some mNodes are used in [11], but in their work, the authors have not taken into consideration the concept of energy.

The mNodes are fixed and do not change during the network lifetime. They are deployed to perform only detection tasks. They do not sense and send data. The contribution of our work is to use these specific, elected periodically nodes to verify traffic in the sensor network and to provide a dynamic solution that can allow DoS attack prevention and can increase the sensor lifetime by minimizing and equilibrating the energy consumption. The mNodes are elected periodically by choosing sensors which have most remaining energy. So each node in the network may be elected as mNode in order to fulfill an analyzing function or may sense data as a normal sensor.

The remainder of this paper is organized as follows. Related works are discussed in section 2 and in section 3 proposed techniques is discussed in detail. The simulation results are discussed in section 4. The section 5 concludes the paper.

II. RELATED WORKS

To deal with DoS attacks in wireless sensor networks, many research studies have been conducted. A cluster-based intrusion detection system is proposed in [11]. It prevents sensor networks from DoS attacks. This solution deploys a set of special nodes called ”guarding nodes” (gNodes) which observe, analyze the network traffic and report DoS attacks to their cluster head if an abnormal event happens. In each cluster there are three types of nodes, gNode, cluster head and sensor node. Any kind of nodes may be compromised. In this study, the detection technique for diverse attack types and the actions taken after detection are explored for the different node types.

Perrig et al. [12] proposed SPINS (Security Protocols for Sensor Networks) which include two efficient symmetric key based security building blocks: SNEP and µTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness, with low overhead. It uses MAC and a shared counter between the sender and the receiver for the cipher block in counter mode which is incremented after each block to achieve two-party authentication and data integrity. µTESLA provides authenticated broadcast using one-way key chains constructed with secure hash functions. It divides a time into time intervals and the sender associates each key of the one-way key chain with one time interval to do cryptographic operations.

Hierarchical sensor networks where clusters are formed dynamically and periodically using the LEACH algorithm, allow distributing the energy load among sensor nodes. The problem of adding security to this type of network is raised by Oliveira et al [13] who propose SecLEACH which is a revised version of LEACH. It applies random key pre-distribution and µTESLA. They can be used both to secure communications in a hierarchical network with dynamic cluster establishment.

The running of a detection mechanism on every node in the network allows achieving a perfect detection against DoS attacks but it is not a feasible solution in a constrained network. In [14], an optimized placement of detection nodes in a network for distributed detection of DoS attacks is proposed. In addition to placing detection nodes at critical points in a network, this proposition minimizes the number of these required nodes and therefore reduces the cost and processing overheads.

An adaptive security design (SecCBSN) to secure clusterbased communication in sensor networks, is proposed in [15]. It consists of three modules, which can detect malicious nodes by providing secure communication and authentication protocols between nodes. In each cluster, a CH schedules transmission and monitors periods for its sensor nodes. The primary security module uses the TESLA certificate (TCert) to enable existing nodes to authenticate new incoming nodes, triggering the establishment of secure links and broadcast authentication between neighboring nodes. In SecCBSN, the intrusion detection module prevents against compromised nodes. It uses alarm return protocols, trust value evaluation, and the propagation of black and white lists of nodes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Data aggregation is the process of summarizing and combining sensor data in order to reduce the size of data transmission in the network. In a cluster-based sensor network, a cluster head is elected by the other nodes in order to aggregate data locally and to transmit the aggregation result to the base station. This process needs security mechanisms to ensure data confidentiality and authentication. Ozdemir and Xiao [4] explore the relationship between security and data aggregation process in wireless sensor networks. They present an extensive literature survey by summarizing the state-of the- art data aggregation protocols and based on this literature survey, open research areas and future research ways are specified.

III. PROPOSED TECHNIQUE

A. Architecture

We consider a cluster-based sensor network, where the sensor is a tiny device that collects information from a target region and reports this information to the base station. In each cluster we have three types of nodes, a cluster head, sensor nodes, and manager nodes called mNodes. Only a cluster head can aggregate and send data to the sink. The proposed cluster based technique that can detect DoS attacks in sensor networks is shown in Figure 1.

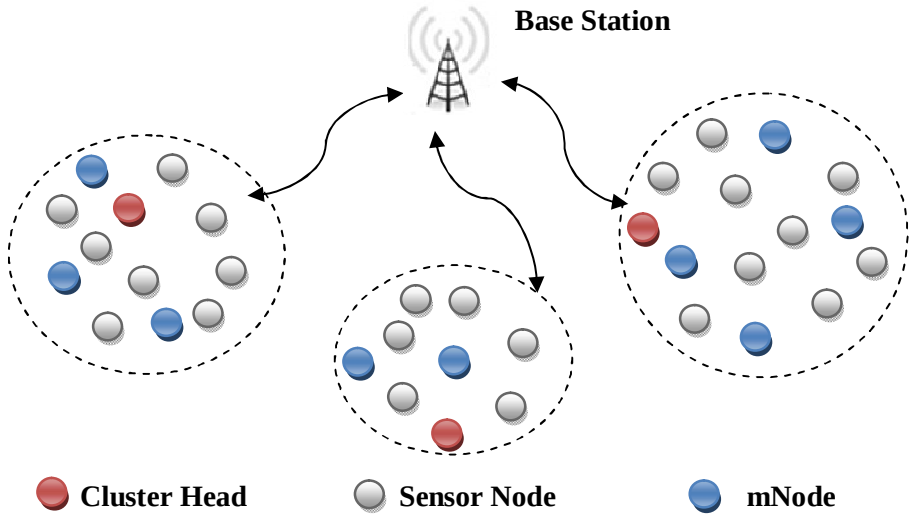

Figure 1: Architecture of proposed cluster

The construction of clusters in the sensor network can be performed by any method proposed in previous researches such as LEACH [16, 4]. In each cluster, a set of special nodes are deployed to analyze the network traffic and to detect abnormal behaviors. At time t, a set of mNodes is designated among all the nodes in the cluster having the most remaining energy. They are deployed to analyze the traffic and they do not do sensing tasks. At a particular time, another set of mNodes is elected to replace the old mNodes and the latter become sensor nodes which perform the sensing task, and so on. This can improve the life time of the network by minimizing the energy consumption of each sensor node and can improve security by preventing the attackers to compromise mNodes and others nodes.

B. Operation Principle

To form clusters in our network and to elect the CH in each cluster, we choose to use LEACH which is the first clustering algorithm proposed to form clusters of sensors and which provides equilibrium of energy consumption through a random rotation of CHs, allowing the energy requirements of the system to be distributed among all the sensors.

The mNodes are responsible for preventing DoS attacks in sensor networks. In each cluster we have N sensor nodes that elect a cluster head using LEACH protocol. Then we choose k nodes among N that can be elected as mNodes. In

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

each cluster some of the nodes having more residual energy since they do not often participating in packet transmission. This kind of nodes is chosen by the cluster head because the information of all nodes in a cluster is gathered by the cluster head and also all processes within the cluster is done without the knowledge of cluster head. After a particular time another set of k nodes i.e. mNodes are chosen and replace it for old mNodes. These k nodes are those with the most residual energy that can perform the task of analyzing network traffic. Once these nodes are chosen they begin to monitor traffic using a statistical technique that is discussed in this section. The purpose of this solution is to provide a mean to elect periodically these manager nodes in order to avoid energy depletion and to reduce the likelihood of detection of these nodes by the attackers. At each period we have in a cluster a different set of mNodes, a cluster head and sensing nodes.

IV. SIMULATION RESULTS

Figure 2 represents the detection rate for different numbers of mNode groups and for groups of different sizes. The same node is considered compromised in all the graphs. Based on the size of the clusters number of mNodes are elected. Here the whole network is split into three clusters in which 5 mNodes, 12 mNodes and 20 mNodes are elected depending on cluster size. Detection performance of these mNodes on the corresponding clusters is plotted in Figure 2.

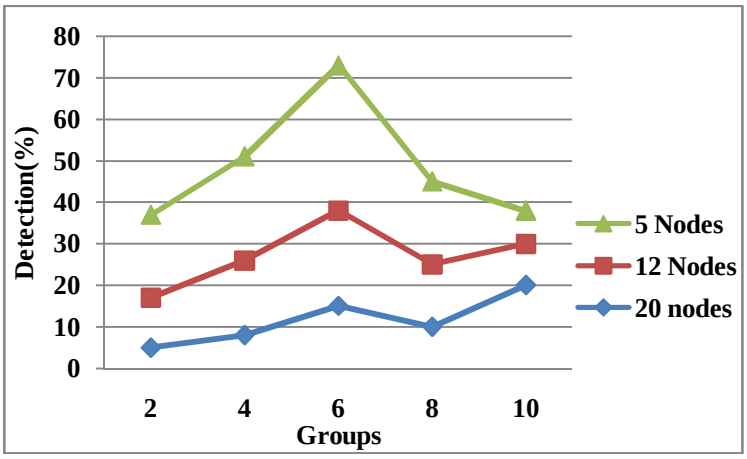

Figure 2: Detection Vs Group

The figure 3 represents the detection rate by the number of mNodes used. We show two results, the first is for a five cooperation node and the second for an average of 15 cooperation nodes. Notice that the detection rate increases as the number of mNodes increases and that for 12 mNodes, we already have a sufficiently large percentage of attack detections.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

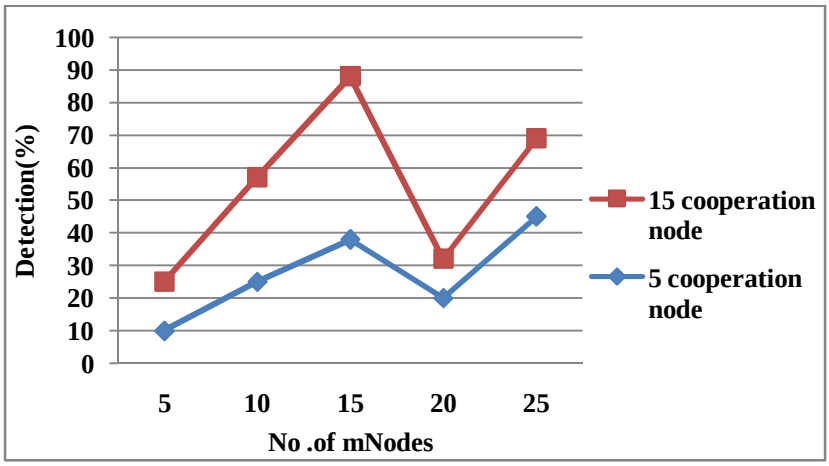

Figure 3: No. of mNodes Vs Detection (%)

V. CONCLUSION

Because of the restricted ability of a sensor, it is extremely hard to keep a sensor from a DoS attack. Detection of DoS mechanisms, utilized as a part of the wired or remote network environments which can't be utilized for sensor network because of the constrained capacity of sensors and the absence of centralized monitoring and administration in sensor networks. Considering DoS attack and creating discovery methods are essential as they can have severe impacts. In this paper, we presented a dynamic technique for cluster based detection network. Some unique nodes called mNodes, are selected to monitor and to report activities of DoS attack to the cluster head. The chosen mNodes change progressively with a specific end goal to keep away from consumption of energy and to decrease the probability of recognition of these nodes by the attackers. Our proposed technique offers a few benefits over the static strategy. It identifies several attacks. It preserves the network energy by varying the mNodes in the cluster. It performs load balancing and enhances the lifetime of the network. Besides it increases the security of the network by evading the prediction of mNode by an attecker.

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] Afrand Agah and Sajal K. Das:"Preventing DoS 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] Gu Hsin Lai and Chia-Mei Chen:"Detecting Denial of Service Attacks in Sensor Networks". Journal of Computers Vol.18, No.4, January 2008.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

[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.