IDS in WSNs-Based On Spy Node and Ballot Scheme

Shabnam Sangwan¹, Jyoti² & Reema Sachdeva³

¹,³A.P in CSE, ²M.Tech Scholar in CSE

¹,²Sat Kabir Institute of Technology & Management, Bhadurgarh, Jhajjar, Haryana (132103), India

Abstract: Due to the distributed nature, multi-hop communications and their deployment in remote areas, WSNs are susceptible to numerous security attacks that can adversely affect performance. Therefore, to ensure the proper functionality of WSNs, security is the foremost and important concern in almost all wireless sensor networking scenarios. WSN mechanisms cannot presently ensure that an intrusion will not occur. For example, using a compromised node, an adversary could do an attack acting as a correct node of the network to acquire all the information. Such attacks are called as internal attacks. Therefore, it is necessary to protect the wireless sensor network from internal attacks, which is the purpose of this paper. Algorithm for transport layer attack has been developed in this paper which also focuses on minimum energy consumption. We have tested the algorithm for sink hole attack mainly using voting scheme but it can also works for other attacks like worm hole attack, black hole attack.

Keywords: WSN, Clustering, K-means algorithm, sinkhole attack, Spy node.

1. INTRODUCTION

Wireless sensor networks has become a hot space of research in recent years, due to the large potential of sensor networks to enable applications that connect the physical world to the virtual world. By networking massive numbers of tiny sensor nodes, it is possible to get knowledge concerning physical phenomena that was troublesome or impossible to get in more conventional ways. In the coming years, as advances in micro-fabrication technology enable the value of producing sensor nodes to still drop, increasing deployments of wireless sensor networks are expected, with the networks eventually growing to massive numbers of nodes. Potential applications for such large-scale wireless sensor networks exist in a large number of fields, including medical monitoring, environmental monitoring, surveillance, home security, military operations, and industrial machine monitoring. Once coming up with network protocols for wireless sensor networks, several factors should be considered. The foremost necessary factor, because of the scarce energy resources, routing decisions should be guided by some awareness of the energy resources within the network. If a sensor network is well connected, topology management services ought to be employed in conjunction with the normal routing protocols. Protocol scalability is an important design criterion. Clustering has been proposed by researchers to group a number of sensors, usually within a geographic neighborhood, to form a cluster that is managed by a cluster head. Simple sensor nodes are usually not well physically protected because they are cheap and are invariably deployed in open or may be in hostile environments wherever they will be easily captured and compromised. That is why it has become a difficult task to secure WSN. As WSN suffers from varied attacks by anomaly nodes. So it is necessary to notice these anomaly nodes. For this several problems are faced some of them which are considered in our work, when literature survey are listed –WSN is a resource constrained and energy constrained network. Thus there’s invariably scariness of resources and battery in sensor nodes so conventional IDS can’t be used for WSN. Several IDS presented by researchers are restricted to solely network layer due to which many types of attacks by intruders might go unidentified. Thus detection scheme ought to be such that it will analyze the anomaly node at each OSI layer so that attacking probability decreases or in other words cross layer detection scheme should be tried. Crossover detection has a problem of using different IDS at every layer that consumes additional energy and resources too. Thus a generalize algorithm for nearly all type of attacks should be proposed. Keeping issues discussed in mind very first objective will be the establishment of WSN network. It can be done by three methods, out of that we are going to choose unsupervised learning for WSN nodes distribution because it don’t require prior training.
Since sensor nodes are resource constrained so we are going to place a mobile spy in WSN which can take data from every sensor node. Neighboring Ballot mechanism are going to be followed for intruder detection in spy node and results are going to be shown in form of false alarms just in case of different attacks in network. Keeping problems discussed in mind following will be key objectives which will be tried to achieve in our work:

- The very first objective will be the establishment of WSN network. It can be done by three methods, out of which we will select unsupervised learning for WSN nodes distribution as it don’t require prior training.
- Since sensor nodes are resource constrained so we will put a mobile spy in WSN which will take data from every sensor node.
- Detection mechanism has to be deployed on each node which consumes battery of node, rather than we will deploy this only on spy node as it will have the information of every sensor node.
- Neighboring Voting mechanism will be followed for intruder detection in spy node and results will be shown in form of false alarms in case of different attacks in network.

2. LITERATURE REVIEW

Intrusion detection is a very important aspect within the massive domain of computer network security. Main specialize in Intrusion Detection System [4] providing a new game theoretic-approach and focus solely on the anomaly primarily based intrusion detection system [6]. New intrusion detection system supported cross layer interaction between the network, Mac and physical layers[10]. Also an efficient MAC address based intruder tracking system[8], So we have addressed the matter of intrusion detection in a totally different approach in which the idea of cross layer is widely used resulting in the birth of a new style of IDS. By experimentation, we have evaluated our system using the NS simulator to demonstrate its effectiveness in detecting different kinds of attacks at multiple layers of the OSI model. Some intrusion system is anomaly primarily based several authors worked on such system. In Intrusion detection system to avoid wasting energy several clustering algorithms used like K-means algorithm. An both centralized and distributed k-means clustering algorithm approach employed in network simulator [9][31].

K-means is mainly a prototype based algorithm rule that alternates between two major steps, assignment observations to clusters and computing cluster centers till a stopping criterion is satisfied. An Intrusion Detection System (IDS) mechanism to observe the intruder within the network that uses Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for its routing operation [30]. An adaptive secure routing protocol that relies on bio inspired Mechanism of many economical routing protocols are projected for specific scenarios to attain specific objectives in WSN [13]. However, such networks have several limitations like low data rates and security threats. It uses distributed ant-based methodology to pick out two optimum ways keeping in sight route security. Simulation results show that our routing protocol will perform higher in several situations. An efficient MAC address primarily based intruder tracking system has been developed for early intruder detection and it’s bar [8]. Wireless sensor network (WSN) is a rising technology that shows great promise for varied applications each for mass public and military. A Voronoi diagram based network specification, that deploys mobile data collectors (MDCs), ensures the compatibility of the anomaly detection model for the resource constrained WSNs, and warrants data integrity between the MDCs [25] and also the LNs. A parameter and trust issue primarily based secure communication framework and style a trust management system for wireless sensor networks[28].Wireless network system liable to many attacks out of this sink hole attack[15][16] is that the most dangerous because it often give path for alternative attacks too. A theme to defend against sink hole attacks[1][2] using mobile agents and Leader that are Based on Intrusion Detection System (LBIDS) so as to provide a whole solution to observe and avoid [14][12] sinkhole attack. The Adaptive Trust Management Protocol (ATMP), that adjusts trust and reputation based on the behavior of sensor nodes [29] [11]. Some thought about multidimensional trust attributes derived from communication and social networks to judge the overall trust of a sensor node [17]. The weighted vote Based Trust Management scheme to enhance the performance of intrusion tolerance in HWSN [18] [24]. As in depth literature review of machine learning strategies that were used to address common problems in wireless sensor networks [20] (WSNs), Some cooperative [7] and advanced [26] strategies of Intrusion detection was additionally projected. Swarm Intelligence (SI), a comparatively new bio inspired family of strategies, seeks inspiration within the behavior of swarms of insects or alternative animals. When applied in alternative fields successfully SI began to gather the interest of researchers operating within the field of intrusion detection [5].

3. PROPOSED WORK

In WSN network security and energy consumption are perpetually concern. Security improvement and
reducing the energy consumption algorithm continues to be in developing stage. The necessity of the algorithm is that there ought to be exchange between these two considerations. In our work we have place a leap forward for such kind of work. The matter in WSN is categorized in three classes in our work:

i) Clustering of WSN nodes with cluster head therefore that minimum energy consumption takes place in data transmission, ii) incessantly running a security algorithm and iii) reduction of energy usage.

**Step 1:** In WSN every node will communicate with different freely, however if let it happen then no specific routing algorithm are going to be effective and since each node needs to transmit data to base station that is placed at a really far distance from several of nodes and nodes are perpetually equipped with power constraint battery sources, therefore in transmitting messages to a very far distance can drain out their battery in no time. To avoid this several nodes together select a head amongst them that is as regards to several of nodes and have enough power to communicate with base station, unsuitable to distance. That node head choice is called cluster. This clustering are often supervised and unsupervised. Since nodes placement could be a stochastic process, therefore unsupervised clustering move. These clustering are done on the idea that nodes are at a minimal distance to cluster head that is chosen on the similar criteria in order that nodes have to be compelled to pay minimum energy in transmitting data to base station via cluster head. It’s a sort of hierarchy, that lets nodes to live more. Our work used unsupervised learning methodology. In clustering algorithm nodes doesn’t communicate directly with sink node. They need to pass the collected knowledge to the cluster head. Cluster head can aggregate the data, received from cluster nodes and transmits it to the base station. Therefore minimizes the energy consumption and range of messages communicated to base station. Additionally number of active nodes in communication is reduced. In our work k-means clustering algorithm is employed as unsupervised learning for of clustering of nodes. Steps for implementing the k means that cluster are:

- Arbitrarily generate k points (cluster centers), k being the amount of clusters desired.
- Calculate the distance between every of the data points to every of the centers, and assign each point to the nearest center.
- Calculate the new cluster center by calculating the average value of all data points within the respective cluster.
- With the new centers, repeat step 2. If the assignment of cluster for the data points changes, repeat step 3 else stop the method.

The distance between the data points is calculated using Euclidean distance.

**Step 2:** Once establishing the WSN nodes in a very pattern, security enhancement is the matter for enhancement. Varied attacks on WSN are known until currently like Sybil attack, black hole attack. Amongst all, sink hole attack is additional dangerous because it will change the data and opens a path to different attacks too. For detection of sink hole attack varied ways are prompt antecedently however none of them is full proof and if anyone is then that forgets the energy consumption. However in our work we have a tendency to unbroken a win to win scenario in between them. In several detection algorithms, nodes are accountable to run algorithm on their part that consumes energy. However if this detection technique is not the responsibility of nodes then battery power of nodes are often saved up-to an extent. To stay this in mind we have the tendency to use the conception of a spy node which is able to keep running through whole network, connecting with base station. Since it will begin from base station and finish at base station therefore battery demand will not be constraint for it. Within the geographical region several polling points are selected that spy node can gather the information from nearby cluster head and detection algorithm can be run on the spy node, not within the node. It therefore saves energy of node. For this purpose all geographical region is split by voronoi diagram and polling point are placed on the idea of that.

**Step 2.1** Voronoi diagram divides the region in such a way that every points on the lines within the diagram are equidistant to the closest two (or more) source points. It is a diagram that is created by taking pairs of points that are approximate and drawing a line that’s equidistant between them and perpendicular to the line connecting them.

**Step 2.2:** Voronoi vertices can locate the position of polling point wherever spy node can collect the data and run the detection algorithm. Base station has all data concerning the position of cluster head in geographical region and it’d be quite easier to setup the polling location near to cluster head that is in range of spy node. Since spy node is additionally having a range to communicate so the voronoi vertex closest to cluster head that comes in the vary of spy node from which vertex can be awarded information collecting work position and referred to as polling point. In our work we have assigned every polling location for every cluster. These polling points can create a travel path for spy node as shown in figure 1 below, designed in MATLAB throughout our work. Blue color lines show the voronoi edges and red dots shows polling
point location wherever spy node can collect data form cluster head. Dotted lines show the path of spy node.

**Step 2.3:** In clustering nodes in cluster can’t talk to different cluster nodes directly. They need to follow a hierarchy that starts from their cluster head to base station and so to respective cluster head of sink node.

![Voroni cell plotting](image1)

*Figure 1: Voroni edges and polling point location along with spy node path*

Each source node transmits its information to cluster head and so cluster head add source node’s ID and own ID with the information and send it to base station. Base station has all data concerning tall nodes and cluster head to that they’re associated, therefore it’ll route the message along with the sink node ID to respective cluster head. However if any node is affected by intruder then the information transferred to base station either altered or lost in between. In a sinkhole attack an intruder compromises an existing node or introduces a counterfeit node within the network and uses it to launch an attack. The attacker node tries to draw in all the traffic from neighboring nodes supported the routing metric employed in the routing protocol. Sinkhole attacks are a kind of network layer attack wherever the compromised node sends fake routing information to its neighbors to attract network traffic to itself. Based on the communication flow within the WSN the sinkhole doesn’t got to target all the nodes within the network however solely has to target nodes close to the base station or cluster head if it happens within a cluster. It reflects the identity of a node that is simply next to cluster head or base station to different nodes. In consequence of which nodes treat it single hope aroof from cluster head and transfers the information to sink hole node that is altered by that and more sent to cluster head and then sink hole followed by hierarchy. In our work sink hole is chosen indiscriminately in any cluster and it create illusion of one hope away identity to different and alter their information as shown in figure 2.

![Sink Hole](image2)

*Figure 2: Sink hole affecting other nodes in range*

We have thought of the energy of sink hole same as different nodes. Number of nodes affected by sink hole depends upon the density of nodes. More will be the nodes in a cluster more other nodes will be affected.

**Step 2.4:** because of serious attacks by sink hole the detection and removal from the network is important. Base station has the authority to permit access to any node within the network or will take away any node too. Thus once malicious node is
detected, base station can take away that. Our study used the voting based algorithm to detect the intruder. Several algorithms are thought of to notice this network layer attack however several of them run detection engine supported knowledge of single node which may result in erroneous result. If neighboring nodes help is additionally included within the detection engine then more confidence on detection mechanism are often designed. For this purpose we tend to used voting based algorithm, if majority of nodes voted against any node then that node are thought of as malicious node. This process executes in two steps:

- When any node communicates with malicious node then a doubt can be raised regarding the malicious node.
- If major number of communicating nodes raised doubt regarding the particular node then that may be confirmed as intruder and an alarm can be raised to base station regarding the identity of that node and base station remove that node kind the network. In our work we’ve got taken as two nodes’ doubts as threshold to select the particular node as malicious node.

**Step 3:** energy is consumed in transmission and reception of sensor node. If intruder detection mechanism is run on sensor node then that conjointly consumes energy and since node is actually energy constrained, therefore it might be better if detection mechanism is executed on another node that doesn’t contribute in creating network. Therefore to avoid running detection mechanism on nodes, a spy node is employed which is able to keep acquiring the network and collect information from cluster heads at pre allocated polling points. The detection mechanism is going to be run on spy node. It collects knowledge from cluster head and check whether or not any doubt is raised or not, if raised then it’ll follow voting mechanism and raises alarm to base station. The travel path for spy node is already designed in previous step. In WSN once any node transmits knowledge then it conjointly adds its ID together with destination ID and data. Once sink hole gets the knowledge and transmits it to head after altering it, it has to add its ID also. This all table of data sent from nodes to head is passed to spy node which may simply check the last hop node ID. If multiple nodes send information through compromised node to cluster head then in their routing table malicious node ID are going to be in last hop node ID to cluster head .If the prevalence of this same ID is more than two times, then that node is confirmed as malicious node as in figure 3 and base station removes that from network.

![figure 3](image)

**Figure 3:** Malicious node detection by spy node

**References**


