ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Secure & Energy-Efficient Intrusion Detection in WSN

B. Kalidass[1], V. Ramasamy[2]

PG Student, Park College of Engineering and Technology, Coimbatore, Tamilnadu, India[1]

Assistant Professor, Park college of Engineering and Technology, Coimbatore, Tamilnadu, India[2]

Abstract: One of the most important goal in wireless sensor networks is to transmit the information to sink as soon as possible in a secure and energy efficient manner .The important factor that would make it possible to reach this goal is the design of efficient set selection algorithm in which only required number of sensors will be working such that the entire detection area is covered. In a particular area, all sensor nodes that are required to cover the entire region will only be in on state and rest of the sensor nodes will be in sleep or off state. In this paper, an efficient set selection algorithm specified for intruder monitoring applications is presented. In our proposed model, we are aiming to extend the traditional intrusion detection approach with the addition of a secure and energy efficient set selection algorithm, which reduces the computational power and saves the network capacity.

I. INTRODUCTION

Wireless sensor network (WSN) is rapidly emerging as an important research area. There are variety and number of applications that are growing on wireless sensor networks. The application ranges from general engineering, environment science, health service, military, etc.

Wireless sensor networks are constituted from clusters of devices using sensor technologies deployed over a specific area, wirelessly communicating to a central system. Using viable and emerging communication infrastructures sensor networks continually monitor physical properties, processes, chemical or magnetic properties. Wireless sensor networks rely on emerging technologies such as communication technologies (RF communication, ad hoc networking routing), semiconductor technologies (MEMS CMOS microprocessor), embedded systems and micro sensor technologies. Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements.

These networks will consist of hundreds or thousands of self-organizing, low-power, low cost wireless nodes deployed in large number to monitor and affect the environment. Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The main idea of our scheme is to find the set of nodes which coordinative cover every node in networks. The rest of paper is organized as follow. Section II describes the related work. Section III gives a detailed design with the proposed algorithms. Section IV concludes with its future enhancement. Finally section V shows the bibliography.

II. RELATED WORKS

WSNs have several inherent restrictions compared to IP networks. The main restrictions are: limited bandwidth of the wireless links connecting sensor nodes, limited computing power, and limited energy supply, especially in case of battery-operated networks.

In [2] the main design challenge considered is about energy consumption. In routing-based networks, the total number of operating nodes at any moment (when the network is transmitting) is always lower than in flooding-based networks; thus, routing consumes less energy. On the other hand, flooding-based messages are much more efficient, as they do not need the overhead associated with transmitting routing tables and commands, which increases with the number of nodes and hops. In modern flooding-based systems, the energy of the signals received from adjacent nodes adds up, so less power can be used for achieving the same range.

Range and coverage are among the most important WSN design challenges which is considered in [4]. In networks with simple topology, the range of the network is directly related to the range between two adjacent nodes and thus is affected by the quality of the physical layer circuitry and software. In routing-based networks using mesh topology, the network range also depends on the routing quality of each single path between each two elements of the network. In flooding-
based networks using mesh topology, the nodes sum up the energy from all the received nodes, creating a much better range of the whole network compared to the most sophisticated routing network. In addition, multiple propagation paths improve network coverage to a "no dead spots" quality.

Latency importance in WSN design depends heavily on the specific type of application. For example, in an irrigation application where the time resolution for water pump switching is tens of minutes, latency is of no consequence. On the contrary, in a utility application where customers call the utility staff about current meter reading, latency determines the quality of the staff service. In some industrial control applications, a delayed feedback to an emergency situation can be very costly or even perilous.

Deployment is another factor which has great importance in WSN. Issues in Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks are handled in [1]. The two types of networks handle network deployment and maintenance differently. Routing-based networks employ special techniques to self-organize by discovering the network nodes, finding the optimal routing table, propagating it through the network, and continuously changing it according to changeable propagation conditions and physical network changes. These techniques, some of which are sophisticated, operate well when the networks are small and simple. However, when the networks are larger with large numbers of nodes and hops, then expert human intervention and dedicated management software are usually needed for both initializing the network and coping with major changes. Furthermore, until the network reorganizes, parts of it or the whole thing can be down for various periods of time.

Hostile Environment: Sensor networks can be deployed in remote or hostile environment such as battle fields. In these cases, the nodes cannot be protected from physical attacks, since anyone could have access to the location where they are deployed. An adversary could capture a sensor node or even introduce his own malicious nodes inside the networks. If the latter is the case, the adversaries aim is to trick the network into accepting his nodes as legitimates.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Location of nodes: One challenge is how to accurately find the location of each sensor node the location of each sensor node, at a low cost. The node localization problem has received tremendous attention from the research community, thus emphasizing that it is an important problem and that it is a difficult problem. It is an important problem because the quality of the data obtained from the WSN and the operation of the network can both be significantly impacted by inaccurate node locations.

The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. Intrusion detection (i.e., object tracking) in a WSN can be regarded as a monitoring system for detecting the intruder that is invading the network domain. The intrusion detection application concerns how fast the intruder can be detected by the WSN. IDSs in ad hoc networks or WSNs have been proposed to suite the characteristics of wireless environment. IDSs in ad hoc networks and they classified IDS into two types: stand-alone and cooperative. In stand-alone IDS, local IDS agent is run on each node independently to detect intrusion. So far, every decision is made itself based only on information received

in each node; this architecture has not been chosen for WSNs. The nature of wireless network is distributed and requires cooperation of neighbor nodes thus cooperative schemes are best IDS schemes suite to the characteristics of WSNs

In our proposed model, we are aiming to extend the traditional intrusion detection approach with the addition of a secure and energy efficient set selection algorithm, which reduces the computational power and saves the network capacity.

III. PROTOCOL DESIGN

Set selection for efficiency

The main requirement regarding the deployment of a WSN is the set of sensors. There are mainly three constraints for this set selection.

1. Maximum coverage
2. Maximum connectivity
3. Minimum number of sensors

We are proposing a method, which will meet all of the above mentioned constraints. If there is one or more link between two sensors which are having the maximum number of neighboring sensors, then we could obtain maximum coverage within the network. Since we have to deal with the number of neighbors, first of all we have to maintain a list indicating the number of neighbors of each and every node in the deployed area. Here we are not using the parameters such as transmission range and communication range in order to minimize the computation overhead. The main assumption is that the coverage of each node depends on the number of its neighbors. Now, we can come to our proposed algorithm.

Variables used are:

No. of Neighbors of a node MaxNbr – Maximum Neighbor to keep the nodes with max NbrCnt

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

NbrLst – Neighbor List to keep the neighbors of each node with MaxNbr

CmnNbr – Common Neighbors to keep the Common neighbors from NbrLst[i] ∩NbrLst[j]

SelSet – To keep the final selected set of nodes

Algorithm: Set Selection Algorithm

1. Count all the One-hop neighbours of all nodes and record it in NbrCnt[]

2. Set nodes with maximum neighbours to MaxNbr[]

3. Find One-hop neighbours of each node in MaxNbr[] and feed in NbrLst[]

4. Repeat steps for each NbrLst[i]

4.1.1 Repeat steps for each NbrLst[j] (where j=i+1)

4.1a Find NbrLst[i] ∩NbrLst[j] and feed it in CmnNbr[]

4.1.2 Select nodes with minimum CmnNbr[] (≥1) and current CmnNbr[], keep them in SelSet[]

4.1.3 Remove values of nodes in SelSet[] from NbrLst[]

5. Repeat steps 3 and 4 with next element in MaxNbr[]

6. Return SelSet[]

SelSet is the final set of nodes. The main component in this algorithm is NbrCnt, the number of neighbors of each node. The two nodes with maximum number of neighbors are chosen and the numbers of neighbors which are common to both nodes are computed. This comparison is worked out inside a loop in order to reach all nodes. Once, a node is found in such a way that it has exactly one common node, and then the node with maximum number of neighbors, the currently executing node and the intermediate node are feed into the final set. This process is repeated with all the selected nodes. The algorithm terminates with the maximum coverage of the deployed area. The proposed algorithm gives coverage more than 90%. Hence we can consider it as one of most powerful and efficient algorithm in the field of network deployment.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

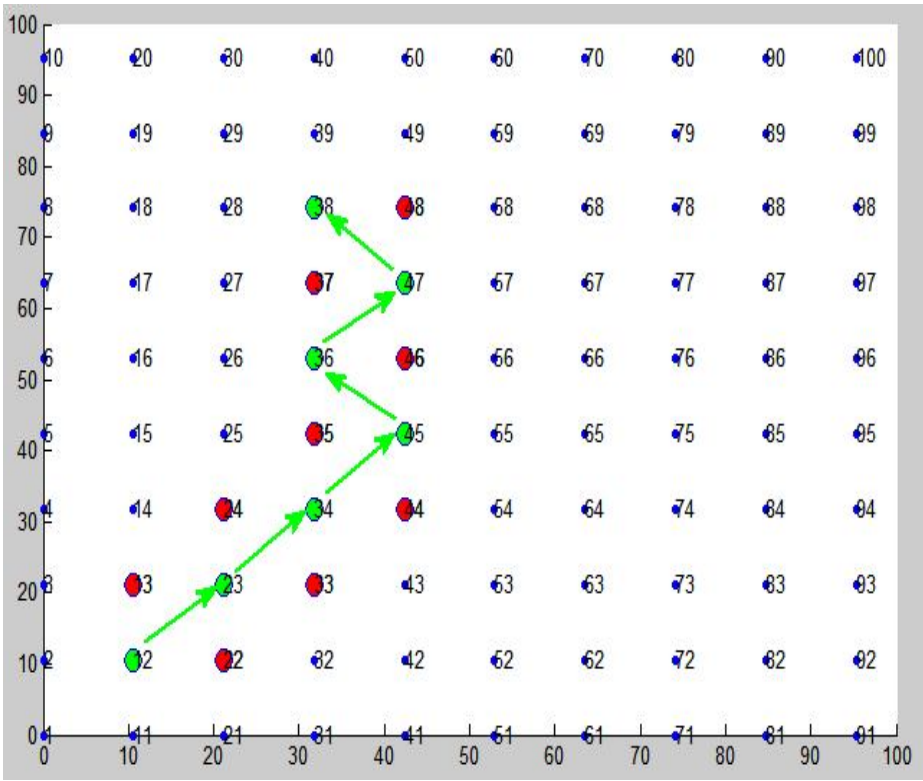

Fig 3. Guard nodes for security

Then, our next step is to find the distance of these selected nodes from the sink node and these nodes will get a unique rank according to the computed distance. The node which is near to the sink node will get top rank (low number).

The main purpose of this module is to find a shortest path between the sink node and the detected node. This is computed according to the ranks assigned for the nodes by the sink node. Once such a path is obtained, we are up to find the guard nodes for monitoring the transmission through this path. These guard nodes are obtained by the intersection of neighboring nodes of the two adjacent nodes in the selected path.

Guard nodes are obtained not only for the secure transmission, but also they can replace any failed node in the selected path.

This further extends the durability and extendibility of our proposed scheme.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. CONCLUSIONS AND FUTURE SCOPE

In wireless sensor networks, finding an optimal node deployment strategy that would minimize cost, reduce computation and communication overhead, be resilient to node failures, and provide a high degree of coverage with network connectivity is extremely challenging. Here, we are proposed a secure and energy efficient algorithm. The security constraint of our scheme has explained in the security module. How our method becomes energy efficient, which can be viewed by the analysis we have done. We have deployed in a 100*100 square meters area for both homogeneous and hetero generous networks.

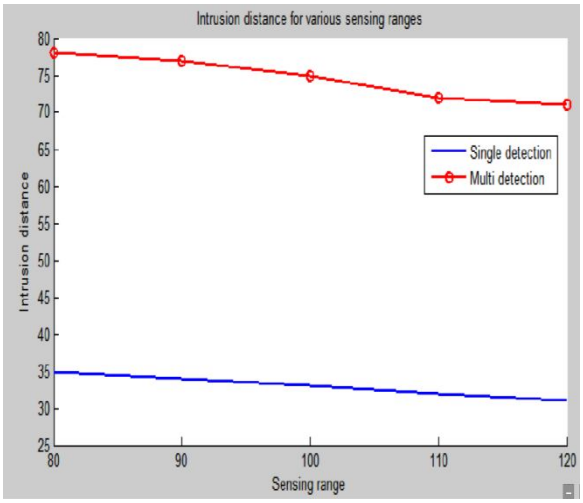

Figure 4: Intrusion distance for various Sensing ranges

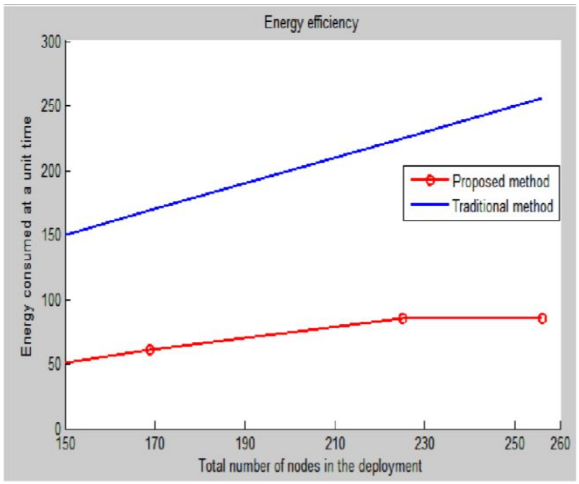

Figure 5: Energy consumption

The above graph shows the change in the distance travelled by the intruder before it gets detected according to various sensing ranges. The graph highlights the fact that as the sensing range increases, the intrusion distance drops for both single detection and multi detection.

We are considering the deployed nodes are having the same power. Each node has power equal to 1 jule. Hence, the power consumed by the total deployment can be calculated from the number of selected nodes in the particular area. Using this data, we can compare the efficiency of the proposed method with that of the traditional methods.

From the figure 5, it's clear that the energy consumed per unit area in the case of traditional method is increasing with the number of nodes in the deployment. In our proposed method, the energy consumption per unit area meets a constant value.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Thus, for a 100*100 square meters deployment: Traditional method consumes a total of 64 unit energy, whereas our algorithm uses only 13 unit energy. That means our scheme is approximately 20% more efficient than the traditional method. From this analysis it is evident that our proposed scheme is energy efficient as we claimed before.

Throughout our project, we mentioned and simulated about a two dimensional wireless sensor network. But our actual point is energy efficient and secure intrusion detection in three dimensional wireless sensor networks. It is difficult to deploy and maintain a three dimensional WSN. However, the two dimensional deployment serves as a key element for three dimensional deployment. With the limited time and infrastructure it was quit impossible to do the above analysis in three dimensional networks. But we are sure that our proposed scheme is well applicable for the three dimensional networks. And three dimensional deployment can be made true as a future enhancement of this project.

REFERENCES

[1] Xiaodong Wang, Student Member, IEEE, Bin Xie, Senior Member, IEEE, Demin Wang, Student Member, IEEE, and Dharma P. Agrawal, Fellow, IEEE. "Intrusion detection in Homogeneous and Heterogeneous Wireless Sensor Networks" Yun Wang, Student Member, IEEE,

[2] Y. Chan and B. H. Soong, "A new lower bound on range-free localization algorithms in wireless sensor networks," IEEE Commun. Lett., vol. 15, no. 1, pp. 16–18, Jan. 2011.

[3] Issa M. Khalil "ELMO: Energy Aware Local Monitoring in Sensor Networks"

[4] O. B. Akan and I. F. Akyildiz, "Event-to-sink reliable transport in wireless sensor networks," IEEE/ACM Trans. Netw., vol. 13, no. 5, pp.1003–1016, Oct. 2005.

[5] Mohamed Mubarak.T, Dr.Syed Abdul Sattar, Dr.Appa Rao, Sajitha M "Energy efficient Intrusion Detection in Three Dimensional Wireless Sensor Networks"

[6] Amitabha Ghosha, Sajal K. Dasb "Coverage and connectivity issues in wireless sensor networks :A survey"

[7] L. Yu, L. Yuan, G. Qu, and A. Ephremides, "Energy-driven detection scheme with guaranteed accuracy," in Proc. IPSN, Nashville, TN, Apr. 2006, pp. 284–291.

[8] L. Yu and A. Ephremides, "Detection performance and energy efficiency of sequential detection in a sensor network," in Proc. HICSS, Jan. 2006,p. 236.