ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Intrusion Detection in Heterogeneous Wireless Sensor Networks with Liveliness Proficient Node Localization Algorithm

Chinnabbaiah R[1], Manjunatha C[2], Poonam G[3]

HOD, Computer Science & Engineering, KJTET Polytechnic, Mulbagal, India [1]

Lecturer, Computer Science & Engineering, KJTET Polytechnic, Mulbagal, India[2]

Assistant Professor, Computer Science & Engineering, R.V. College of Engineering, Bangalore, India[3]

Abstract: In the recent growth of wireless sensor networks deal with different functional areas, to carry out different functionalities known as catastrophe revitalization, deep search, intrusion detection and number of other functionalities in neat digital world. The functionality with respect to the wireless sensor network, the node localization is mainly used for estimating the liveliness proficient of the network. Node localization requires informing the origin events, assisting group queries, routing a solution to the deployed network system. This proposed research work focus on these issues in heterogeneous Wireless Sensor Networks (WSN) models and also estimating different approaches for node location finding. Detecting intrusion in WSN will focus on practical implementations. In many these implemented applications used for detecting intrusion in smart offices and recent network resources. This paper introduces the Liveliness Proficient Node Localization (LPNL) algorithm for network connectivity and broadcast reach-ability, which are essential conditions to make certain corresponding detection possibilities in WSN. Simulation results verify and validate the analytical values for heterogeneous WSN.

Keywords: Intrusion Detection, Node Localization, Wireless Sensor Networks (WSN), Smart offices.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a collection of spatially deployed wireless sensors to monitor various changes of ecological condition in a shared manner without relying on any underlying infrastructure support [*1*]. Many network parameters such as sensing range, transmission range, and node density range are carefully considered at the network design phase, according to specific applications. To realize this, it is critical to capture the impacts of network parameters on network performance with respect to application specifications. In view of the fact that most developments depends on a winning localization, i.e. to approximate their positions in various predetermined coordinate structure, which considers designing efficient localization algorithms.

The sensor nodes are tiny and restricted in power. Sensor types differ according to the application of WSNs. Whatever be the application, the resources such like power, memory and band width are limited. Moreover, most of the sensors nodes are throwing away in natural world, so it is essential to consider energy efficiency to maximize the life time of the WSN. Great efforts devoted to minimizing the energy consumption and extending the lifetime of the network. One of common technique is to place some sensor nodes in sleep mode to save energy and wake up them under various strategies. Work towards maximize the existence of WSN is active area of research. In recent times there is a need of heterogeneous WSN deployment. Lee et al. [*2*] analyze heterogeneous deployments both mathematically and through simulations in different deployment environments and network operation models. In [*3*], Hu et al. investigate some fundamental questions for hybrid deployment of sensor network, and propose a cost model and integer linear programming problem formulation for minimizing energy usage and maximizing lifetime in a hybrid sensor network. Their studies show that network existence can be increased dramatically with the addition of extra micro-servers, and the lifetime of network significantly affected by the location of micro-servers.

Smart environments will represent the next evolutionary improvement stage in, constructing, usefulness, manufacturing, residence, shipboard and other means of transportation system. Similar responsive mortal, the elegant atmosphere relies first and foremost on sensory data from the existent world. Sensory information obtains from numerous sensors of different modalities in distributed locations. The challenges in the hierarchy are detecting the significant quantum, monitor and observing the information, assess and validate the data, formulate significant user display and performing administrative and configuration functions are vast. The data required as a result of neat environment is provided by distributed heterogeneous wireless sensor networks are conscientious for sensing while the first stages of the processing hierarchy. Sensor applications have multi-objective performance requirements. A sensor network is desired to be low-cost and yet capable of meeting stringent performance and robustness requirements of real time applications. These can be met by deployment of a heterogeneous sensor network comprising of a large number of low cost, less powerful sensors and fewer numbers of more powerful cluster heads or sink.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

The sensor nodes in WSNs are usually static once they deploy and communicate mainly through broadcast instead of point-to-point communication. Sensors nodes are deployed in a various situations and applications should be secure from all types of intruders. A group of safety protocols or mechanisms have been designed for sensor networks. For example, SPINS (Sensor Protocol for Information via Negotiation), a set of protocols, provides secure information privacy, two-way information verification and information innovation and legitimate broadcast for sensor network [*6*]. LEAP (Localized Encryption and Authentication Protocol), is designed to support in-network processing basis on the different security requirements for different types of messages exchange [*7*]. In general, security solutions in the network can be divided into two categories: prevention solution and detection solution. Prevention techniques such as encryption, authentication, firewalls, physical isolation, as the first line of defense, are usually to prevent attacks from outside. 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 hierarchy of this paper is as follows: section II gives the different parameters used in localization, section III explains the different localization techniques in WSN, section IV gives the related work, section V explains the Architecture model, section VI gives the problem statement, Section VII gives the Assumption, Section VIII gives the Heterogeneous WSN, section IX gives the Performance Evaluation and Section X explains the Conclusion and Future work.

II. PARAMETERS of LOCALIZATION

For the various ways of estimating location information, the naming of parameters was distinguished the similarities and differences between different approaches. Such as high accuracy, need for military installation. For intrusion detection power plays a major role in wireless sensor network, as each sensor device has limited power, computational ability and the ability to communicate. And also considers the initial battery powers of the nodes, identical at deployment runtime and also not to change significantly within the reception of four beacon messages by a particular static node.

III. LOCALIZATION TECHNIQUES in WSN

Currently many types of localization approaches and accuracy requirements are available. Localization techniques will be categorized into two types. Range-based and Range-free. Range-based approach mainly uses the absolute distance estimation or angle estimation, significance that a node in a network can measure the distances from itself to the beacons. [*13, 14, 15, 16, 17, 18*] are some examples of range-based localization techniques. In contrast, range-free approach [*19, 20*] means that it is unfeasible for a node to determine the straight distances from itself to beacons. Only through connectivity and proximity, a node can approximate its regions or areas where it stays. Range-based approach is particular while range-free method is often inaccurate. Range-based techniques can also divide into two categories. One is distance estimation by one-hop node and multi-hop node, meaning that a node in the network can not directly communicate with beacons. Localization in WSN is a multi-hop approach because a node may not communicate directly with beacons. Only through multi-hop routing, can send or receive messages to or from beacons. Existing location discovery approaches [*21*] basically consists of two basic phases: (1) Distance or angle estimation and (2) Distance and angle merging. The majority accepted methods for estimating the distance between two nodes are described below: Received Signal Strength Indicator (RSSI), Time based methods (ToA, TDoA), Angle-of-Arrival (AoA, DoA), Triangulation and Maximum Likelihood (ML) estimation.

IV. RELATED WORK

The deployment of large number of cheap homogeneous and heterogeneous sensor devices with different capabilities is presented [*2*]. Intrusion detection is one of the critical applications in WSNs, and recently, several approaches for intrusion detection in homogeneous WSNs has been presented [*3*], [*4*]. A detection based security scheme for sensor nodes have low computation and communication capacity. They have exact properties such as their stable neighborhood information that allows for detection of anomalies in networking and transceiver behaviors of the neighboring nodes has been presented [*5*]. As sensor networks edge closer towards the deployment of sensor nodes, a security issues become a central concern for making sensor networks feasible and useful has been presented [*6*]. LEAP (Localized Encryption and Authentication Protocols), a key management protocol for sensor networks that is designed to support network system processing, at the same time violating the security impact of a node compromise to the immediate network neighborhood of the compromised node has been presented [*7*]. Security in sensor networks is important in smart world monitoring and home security applications to prevent intruders from eavesdropping, tampering with sensor data, and from launching denial-of-service (DOS) attacks against the entire network has been presented [*8*]. To track the movement of an intruder detection problem has considered for resource constraints are discussed [*9*]. Theoretical analysis on the intrusion detection in both homogeneous and heterogeneous WSNs and compared of same either for the single sensing detection or the multiple-sensing detection scenarios has presented [*10*]. A tracking method called Scalable Tracking Using Networked Sensors (STUN) that scales well to large numbers of sensors and moving objects by using hierarchy has been studied [*11*] [*12*].

V. ARCHITECTURE MODEL

This part describes the overall system architecture of intrusion detection in heterogeneous wireless sensor networks.

A. System Architecture Model

The System Architecture model consists of the user or programs, network configuration, network deployment, Liveliness Estimation. The figure 1 describes the System architecture.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

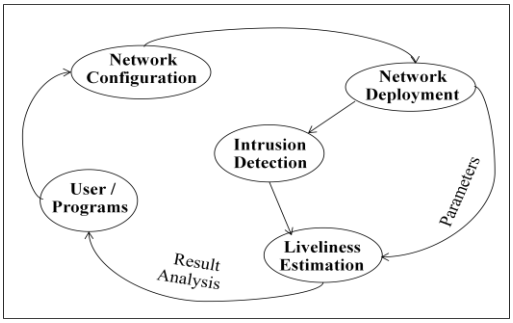

Figure 1 System Architecture

The user or programs are the main activity for configuring the network with specified manner, it includes user activities such setting of network size, node size, sensor radius, transmission period, transmission radius, transmission cost, and receiver cost etc. Network deployment will mainly perform the node deployment based on the user configuration or automated programs. Intrusion Detection will detect the intruders in deployed wireless sensor networks and inform to the sink or intelligent sensor nodes dynamically as soon it is detected. Liveliness Estimation will estimate the power efficiency based on the network deployment parameters and detection performance. Finally estimated results will be monitor by the user and take actions accordingly.

B. Network Model

The network model considers as wireless sensor network in a two-dimensional (2D) plane with N sensors, denoted by a set $N = (d1, d2, d3, \dots dn)$ where $d1$ is the ith sensor. These sensors are uniformly and independently deployed in a square area$A1 = (N * N)$. Such a random deployment of nodes $d1, d2, \dots, dn$ which results in a 2D Poisson point distribution of sensors. All sensors are static once the WSN has been deployed.

Consider here two types WSN: homogeneous and heterogeneous. In a homogeneous WSN, each sensor has the same sensing radius of $rad(s)$, and the transmission range of $rad(x)$. A sensor will sense the intruder within its sensing coverage area that is a disk with radius $rad(s)$ centered at the sensor. Denote the node density of the heterogeneous WSN as shown in figure 2.

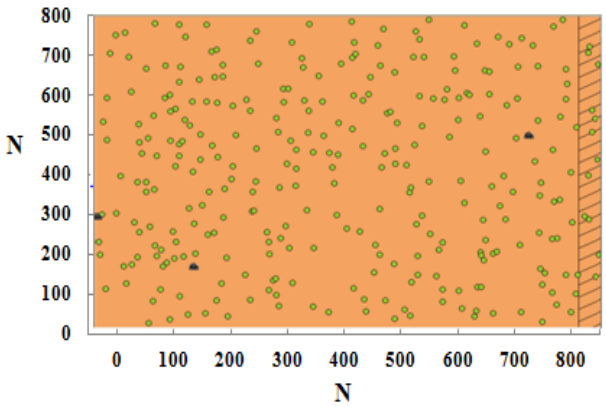

Figure 2. Heterogeneous WSN Deployment

In heterogeneous WSN with two types of sensors, as shown in figure 2. They are, Type I sensor that has a larger sensing range $rad(s1)$, as well a longer transmission range $rad(x1)$, and Type II sensor that has a smaller sensing range $rad(s2)$, as well a shorter transmission range $rad(x2)$.

Hence in our network model, the intruder does not know the sensing coverage map of the WSN.

C. Detection Model

There are two detection models, in terms of how many sensors are required to recognize an intruder: single sensing detection model and multiple-sensing detection model. In single-sensing detection model the intruder will be identified by using only one single sensor with their intelligent behavior.

In the multiple-sensing detection model, the intruder will only be identified by using cooperative knowledge from at least m sensors (m is defined by specific application requirements). For simplicity of expression, multiple sensing and m-sensing are interchangeable, will be discussed in this paper.

VI. PROBLEM STATEMENT

This research work proposes intrusion detection in heterogeneous wireless sensor networks. The main intention is to detect several types of malicious behaviors that can compromise the security and trust of a computer system. To create a network scenario for locate the nodes through energy efficient localization algorithm. To apply the analytical model for single sensing detection and multiple-sensing detection scenarios for heterogeneous WSNs. To enhance or reduce the energy efficiency using LPNL algorithm.

VII. ASSUMPTIONS

A sensor network deployment can usually be categorized as either a dense deployment or a sparse deployment. A dense deployment has relatively high number of sensor nodes in the given field of interest, while a sparse deployment will be having fewer nodes. The dense deployment model is used in situations, where it is important for every event to be detected or when it is important to have multiple sensors which cover the entire area. The sparse deployment model will be used in situations, where the cost of the sensors make a dense deployment prohibitive or to achieve maximum coverage using minimum number of sensors.

It is assumed that once nodes are deployed they are static in most of the coverage area and they stay in the same place. The newer sensor nodes have the ability to relocate after they deployed, these are known as mobile nodes. Here each sensor node determining the location, it needs to move in order to provide maximum coverage.

VIII. HETEROGENEOUS WSN

A Heterogeneous WSN is more complex as compared to homogeneous WSN and which consists of a number of sensor nodes of different types deployed in a particular area and which are collectively working together to achieve a particular aim. For e.g. the wireless sensor network is mainly used in military applications such as in borders for finding out the infiltrations. Heterogeneous WSN are also used for monitoring and control industrial

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

process, monitoring machine instruments health, monitoring surrounding and habitation, healthcare applications, house automation and traffic control.

Consider two types of sensors: Type I and Type II with the node density of $\rho 1$ and $\rho 2$ respectively. A Type I sensor has the sensing range $rad(s1)$, and the sensing coverage is a disk of area $A1 = \pi {r_{s1}}^2$. A Type II sensor has the sensing coverage area A2 with the sensing range $rad(s2)$ without loss of generality. And assume that $rad(s1) > rad(s2)$ in our network sensor model. In heterogeneous WSN, every point in the network domain is said to be covered or reached. If the reaching or covered point is within the sensing range of any sensor (Type I, Type II, or both).

A. Algorithm

The LPNL algorithm is used for node selection trying to select the high capability nodes compared to other sensor nodes. High capability means that sensor node having large sensing range and transmission range. High sensing range implies the fast recognition of intruder in the high mobility network state of affairs.

The procedure for LPNL algorithm is as follows:

The LPNL Algorithm considering a Heterogeneous WSN in 2D plane deployed in square area A1 = (N*N) with d number of intelligent nodes. And also the WSN is heterogeneous so Type I and Type II sensing range and transmission range rad(s) and rad(x) respectively. In the Step 2 initializes all the above mentioned parameters. In Step3 before choosing the intelligent sensor node d out of deployed (N*N) sensor nodes. Then to check whether they are properly initialized, based on the configuration setting and proceed to step 4. For choosing sink d with min N (d), to report all intrusion detection to these sink d. In Step 5 again choosing d because the liveliness of previously chosen d will goes down automatically, and estimating new d, the distance between N (d) and d depends on the sensing range rad(s), and transmission range rad(x). In step 6 the chosen d have more than one node. This LPNL Algorithm is proved that to handle the entire intrusion detection problem without need for additional deployment of sensor nodes, select a certain set of sensor nodes that covers the complete area depends on type of node, its transmission range and sensing range.

The LPNL algorithm as shown below:

Liveliness Proficient Node Localization (LPNL) Algorithm:
Input: In the WSN, Deployed intelligent sensor nodes configuration, Detection Performance measurements.
Output: To Estimate the Liveliness of the intelligent Sensor nodes.
Step 1: Begin
Step 2: Initialize $N, N(d), A1, rad(s), rad(x)$
Step 3: Check if $N, N(d), A1, rad(s), rad(x)$ are null then proceed
Step 4: Repeat for each N
$d \leftarrow min\ N(d)$
if $N(d)$ is not null
Choose d
Step 5: In $A1$ for each $N(d)$ and $rad(s), rad(x)$
$d \leftarrow$ *distance between* d *and* $N(d) < ((rad(s) + rad(x))/2)$
Step 6: if $d > 1$
$N \leftarrow N - N(d)$
Else
$N \leftarrow N - d$
Repeat until N is null
Step 7: End

Figure 3. LPNL Algorithm

B. Theorem

For calculating the probability $P(D)$ that an intruder can be immediately detected once it enters a heterogeneous WSN will be given by:

$$P(D \leftarrow 0) = 1 - \bigcup_{i=1}^{N} e - n(d)$$

Where (d) , is the number of type d nodes activated in the area$A1 = (rad(s) + rad(x)/2)$.

C. m-Sensing in a Heterogeneous WSN

In m-sensing detection model of the heterogeneous WSN with two types of sensors, at least m sensors are required to detect an intruder. These m sensors can be any combination of Type I and Type II sensors. For instance, if five sensors are required to detect an intruder, for a specific application, the intruder can be detected by any of the following sensor combinations:

- Five Type I sensors,
- Five Type II sensors,
- Two Type I sensor and three Type II sensors, and
- Three Type I sensors and two Type II sensors.

IX. PERFORMANCE EVALUATION

This section describes the simulation and result analysis.

A. Simulation Background

First, for deploying network the user to set required parameters should as shown in Figure 4. For this configuration setting, the user need to set the network size, sensor radius, transmission radius, transmitter period, transmission cost, and receiver cost.

Second, the user need to set power, initial power up to 1000 units and residual power will set up to 1000 units. Also shows the sensor activity for the actual sensing of intrusion detection in WSN. The grid shows the deployment of sink in WSN as shown in Figure 4. The simulation control will shows the network deployment, start simulation, replay simulation, and the simulation status shows performance measurements, all these activities will be observed in Figure 4. The simulation control, first button is deployment network used for deploying the sensors in 2D plane. The second button used for starting the simulation, if button as pressed it will shows the simulation of analytical model. Next button is replay simulation, used for replying the previous simulation once more. Next button is exit button if user presses this, it will exit from the analytical model. The performance measurements or status, test all the performance measurements used to analyze the results.

B. Heterogeneous Intrusion Detection

The proposed simulation consider two types of nodes, in order to obtain the results of varying the parameters such as sensing radius, transmission radius, number of sensors nodes etc. The snap shot of simulator before deploying network as shown in figure 4, for varying above mentioned parameters. The sensors are uniformly distributed in a two dimensional space of 1000*1000 meters. The sensing radius is varied from 0 to 100 meters and maximal allowable intrusion distance is 100 meters. The snap shot of simulator after deploying network as mentioned earlier it requires five sensors for

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Heterogeneous WSN, the five deployed sensor nodes will be observed in the grid lines, the same will be shown in Figure 5. The snap shot of simulator results shown in Figure 6. From Figure 6 the user will observe the intrusion detection reported immediately to the sink present in the grid lines, the detection reporting will be indicated in red line from figure 6.

In addition to this simulation status panel also shown in figure 6. The status indicates status of the developed analytical model. Whether it is ready state, running state, and aborted. The sensors indicate the total number deployed sensor nodes. The time indicates the total time of simulation. The power indicates the total liveliness of deployed intelligent nodes or sinks. The Intrusion Detection Count indicates the total number of malicious nodes to be detected in our simulation.

Figure 4. Simulation Configuration of Network

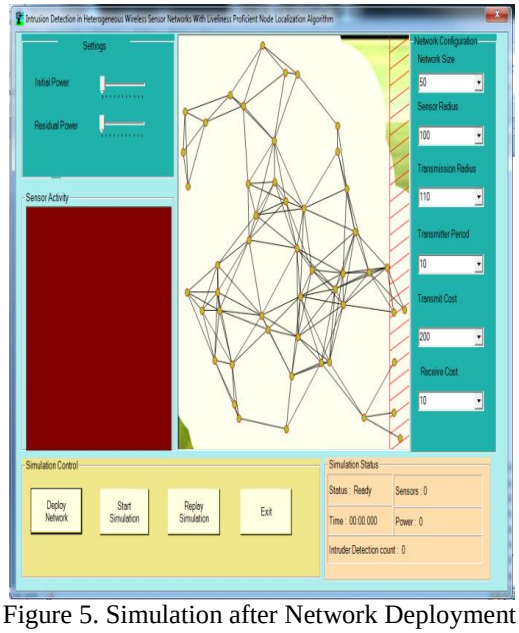

Figure 5. Simulation after Network Deployment

The snap shot below shows the Simulation result along with detection indication path from infected sensor nodes to intelligent nodes.

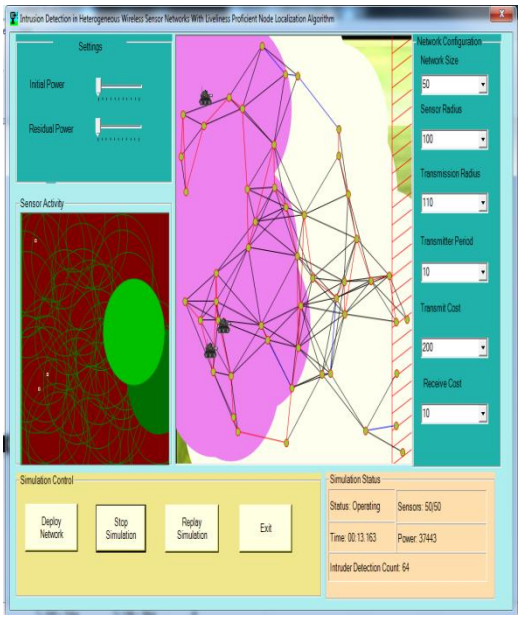

Figure 6. Simulation Results

The graph in figure 7 shows the detection probability over sensing range of the node. The probability will be calculated using the probability calculation theorem discussed in section VIII. The proof shows correctness of estimating analytical model. It is apparent that the single sensing detection probability is higher than that of multi sensing detection probability .This is because the multi-sensing detection imposes a stricter requirement on detecting the intruder for example in our case we need at least five intelligent sensors nodes are required.

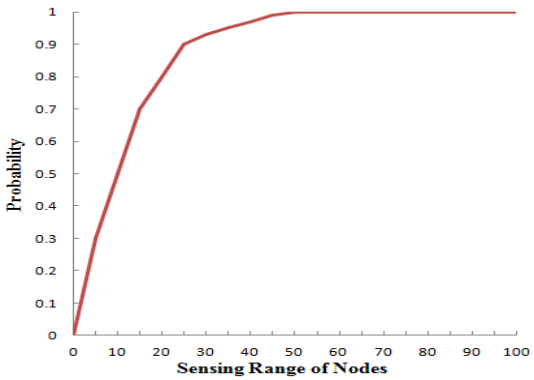

Figure 7. Probability Estimation

The Liveliness estimated by LPNL algorithm is analyzed in the figure 8 given below. Here we compared our results with the universal case. We understood that the node liveliness depends on the energy used by one node for a unit time is one unit. The graph clearly shows the liveliness proficient. The Intrusion detection performed using the LPNL algorithm will be highly energy efficient in case of heterogeneous wireless sensor networks with both Type I and Type II sensor nodes. The numbers of sensors nodes are varied in each execution and find out how it will affect the selection process.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

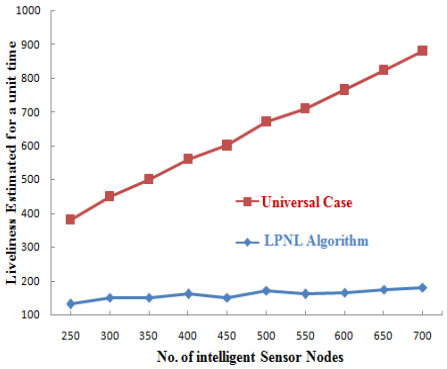

Figure 8. Liveliness Estimation

X. CONCLUSION and FUTURE WORK

This paper examines intrusion detection in heterogeneous wireless sensor networks by characterizing the intrusion detection probability among different network parameters such as sensing range, transmission range, and node density range and also node distance. The main trade-offs identified in WSN is deploying high-cost devices or intelligent sensor nodes under total cost constraints. The intelligent sensor devices can function as a cluster-head or sink to collect and process the data from low-cost sensors, which can enhance the duration of network sensing operation. The LPNL algorithm minimizes the deployment of intelligent sensor nodes in efficient way under total cost constraints. And increase the intrusion detection in a liveliness proficient manner. The developed analytical model results verify the correctness of the proposed analytical model is proved by simulation. Further the research work can be continued for investigating the number of challenges such as architecture issues, the anomaly detection model, and the multilayer integration approach. For architecture study is refining its design and plan to implement and study its performance implications. For anomaly detection model study is effectiveness and scalability of our approach for building anomaly detection models for WSN routing protocols and for other layers of wireless networking.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam , E. Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, vol.40, no. 8, pp. 102-14, Aug. 2011.

[2] Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks (IEEE SECON). (2010).

[3] Hu, W., Chou, C.T., Jha, S., and Bulusu, N.: Deploying Long-Lived and Cost-effective Hybrid Sensor Networks. Elsevier Ad-Hoc Networks, Vol. 4, Issue 6. (2010) 749-767.

[4] A. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks.

[5] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 3, Montreal, Canada, August 2009, pp. 253–259.

[6] A. Perrig, et al., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, 8(5):521- 534, Sep. 2008.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks", Proc. Of the 10th ACM Conference on Computer and Communications Security (CCS '03), Oct. 2004.

[8] J. Deng, R. Han, and S. Mishra, "A Performance Evaluation of Intrusion-tolerant Routing in Wireless Sensor Networks", Proc. of the 2nd Int. IEEE Workshop on Information Processing in Sensor Networks (IPSN'03), Apr. 2003.

[9] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.

[10] O. Dousse, C. Tavoularis, and P. Thiran, "Delay of intrusion detection in wireless sensor networks," in Proceedings of the Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2006.

[11] H. Kung and D. Vlah, "Efficient location tracking using sensor networks," in IEEE Wireless Communications and Networking Conference, ser. 3, vol. 3, March 2005, pp. 1954– 1961.

[12] C.-Y. Lin, W.-C. Peng, and Y.-C. Tseng, "Efficient in-network moving object tracking in wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 5, no. 8, pp. 1044– 1056, 2005.

[13] L. Doherty, K. S. Pister, and L. E. Ghaoui., Convex optimization methods for sensor node position estimation. In Proceedings of IEEE INFOCOM '01, 2001.

[14] A. Savvides, C. Han, and M. Srivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In Proceedings of ACM MobiCom '01, pages 166-179, 2001.

[15] A. Savvides, H. Park, and M. Srivastava., The bits and flops of the n-hop multilateration primitive for node localization problems. In Proceedings of ACM WSNA '02, 2002.

[16] A. Nasipuri and K. Li.,A directionality based location discovery scheme for wireless sensor networks. In Proceedings of ACM WSNA '02, 2002.

[17] N. Patwari, A. O. Hero, M. Perkins, N. S. Correal, and R. J. ODea, Relative Location Estimation in Wireless Sensor Networks. IEEE Transactions on Signal Processing, VOL. 51, NO. 8,2003.

[18] D. Liu, P. Ning, and W. Du., Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks.25th IEEE International Conference on Distributed Computing Systems (ICDCS '05), pp. 609-619, 2005.

[19] T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher, "Range-free localization schemes in large scale sensor networks", In Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking (MobiCom'03), San Diego, CA, USA, pp. 81-95, 2003.

[20] C. Savarese, J. Rabay and K. Langendoen., Robust Positioning Algorithms for Distributed Ad-Hoc Wireless Sensor Networks. USENIX Technical Annual Conference, Monterey, CA, 2002.

[21] G. Mao, B. Fidan and B. D. O. Anderson, "Wireless Sensor Networks Localization Techniques," Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 51, no. 10, pp. 2529-2553, 2007.

BIOGRAPHIES

Chinnabbaiah R has completed Bachelor of Engineering in Information Science and Engineering from Visvesavaraya Technological University, Belgaum. He has 5 years of teaching experience. Presently he is 4th sem, M.Tech Computer Science and Engineering bonafide student of R.V.College of Engineering Bangalore-560059.

Manjunatha C has completed Bachelor of Engineering in Computer Science and Engineering from Visvesavaraya Technological University,Belgaum, He has 4 years of industry experience. Presently he is 4th sem, M.Tech Computer Network Engineering bonafide student of Alpha College of Engineering Bangalore-77

Mrs.Poonam G., has completed M.E(CSE) Pune university & Ph.D(pursuing). She has years of teaching experience and 2 years of industry experience. Presently working as a Assistant Professor, Department of Computer Science & Engineering, R.V.College of Engineering. Mysore Road R.V. Vidyanikethan Post, Bangalore-560059.