Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering
Volume 15 Issue 7 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Model and Techniques Analysis of Border Intrusion Detection Systems

By Mosad Alkhathami, Lubna Alazzawi & Ali Elkateeb
Wayne State University, United States

Abstract- This research paper sets out to explore various border intrusion detection systems but with emphasis on wireless sensor detection method. The system described in this paper relates to the detection of human beings in particular but also offers ways of detecting non-human intruders such as objects and animals. Thus, the study aims at ascertaining the intruder crossing a specified border or perimeter under surveillance before raising an alarm. It also looks forward to provide intrusion detection mechanisms for other forms of objects that are considered to be intruding to a specified perimeter. The application is being developed for border intrusion detection problems that are mainly focused on human and any other intruder. As such, the system will focus on all forms of intrusion including objects. There is also need for an intrusion detection system to ascertain the identity of the intruder.

Keywords: intrusion detection techniques, wireless sensor network, detection models, dma, neural network, border security, network deployment.

GJRE-F Classification : FOR Code 290901p

Models and Techniques Analysis of Border Intrusion Detection Systems

Mosad Alkhathami [α] , Lubna Alazzawi [σ] & Ali Elkateeb [ρ]

Abstract- This research paper sets out to explore various border intrusion detection systems but with emphasis on wireless sensor detection method. The system described in this paper relates to the detection of human beings in particular but also offers ways of detecting non-human intruders such as objects and animals. Thus, the study aims at ascertaining the intruder crossing a specified border or perimeter under surveillance before raising an alarm. It also looks forward to provide intrusion detection mechanisms for other forms of objects that are considered to be intruding to a specified perimeter. The application is being developed for border intrusion detection problems that are mainly focused on human and any other intruder. As such, the system will focus on all forms of intrusion including objects. There is also need for an intrusion detection system to ascertain the identity of the intruder. There is need for the system to distinguish between animal intrusion, human intrusion and any other object that may be used to detect the intruder. Since this paper is meant particularly for human intrusion, it will focus on the human and while also explaining the capability available for detecting animal and object intrusion. Most of the low-cost surveillance systems lack the capability of discerning the intrusion of animals from humans. The study proposed in this paper will make use of shape to train the neural networks. A series of theories that explain the development of the system has been provided in the paper. The discussion has also included recent intrusion detection techniquesand the mathematical derivation of recommended intrusion detection technique.

Keywords: intrusion detection techniques, wireless sensor network, detection models,dma, neural network, border security, network deployment.

I. Introduction

Borders of all nations in this world are at danger and, because of their vast sizes, cannot in any way, shape, be observed in their whole by individuals at extremely inconvenient times of the day. Security is considered to be the primary concern of most of the countries in the world today. The increase in terror and other related crime activities have raised the need to develop and implement intrusion detection system that can raise an alarm whenever there is danger. There are many applications of intrusion detection mechanisms. The primary concern in this paper is the human and object intrusion mechanism. The study will focus on the development of the intrusion detection that will detect the activities of human beings, as well as, other intruders.

Most of the intrusion detection systems have employed wireless sensor networks to facilitate the communication[1]. Wireless sensor networks are considered to provide not only easy implementation procedures but also rapid alternatives for building the network. Depending on the mode of deployment, the coordinates of the sensor devices can follow a given distribution pattern. The mode of distribution of the sensor devices will depend on the nature of the perimeter under surveillance. The analysis of the distribution mode will can be solved using a three dimensional field models and also analysis of non-uniform deployment[2]. Deterministic deployment can also work for plain and easily accessible fields.The system will be deployed in sensitive areas that are expected to have suspicious activities by human beings. The model developed here will make use of wireless sensor networks that will be controlled from a central point. The wireless sensor networks will work to track the detection signals that are obtained from each individual sensor.This paper is organized as follows: Section 2 presents the intrusion detection system architectural design. Section 3 briefly describes different types of sensors that used intrusion detection. Section 4gives the Network Model for WSN. Section 5 presents the intrusion detection systemtechniques. Section 6the recommended technique for Intrusion detection system. Finally, this paper is concluded in Section7.

II. Intrusion Detection System Architectural Design

The design of a successful intrusion system will have to incorporate a given perimeter that will be defined by the monitoring system. Typical intrusion systems are normally developed to monitor a given perimeter which in most cases is defined by an object. The entire security perimeter of the border is coordinated from a central base station [3]. Any detection segment is sent to the central base station. It should be also mentioned the activity of such systems must be supported 24/7. The system should be allowed to run throughout its life. This ensures continuous monitoring of the defined region. Additionally, the deployment of the sensors should be made in such a

Author α σ : Department of Electrical and Computer Engineering, Wayne State University, Detroit, MI. e-mails: fc0233@wayne.edu, drlubna@wayne.edu
Author ρ: Department of Electrical and Computer Engineering, University of Michigan, Dearborn. e-mail: MIelkateeb@umich.edu

way that the perimeter is entirely covered without any unattended spaces in between the nodes. This requires accurate and effective orientation and positioning of the sensor devices [4]. It can also be said that such system require a design where intruders are less likely to notice the location of the sensors. There is also need for the sensor devices to communicate to each other. This can only be accomplished through the use of line topology where the sensor devices are placed in a straight line of a semi-straight. This implies that routing will be very important in deriving the communication protocols for the sensors [5].

III. Intrusion Detection Sensors

The decision on the location and distribution of the sensors is considered to largely contribute tothe success of the system. Human intrusion can be detected using many sensor modalities that do not emit a signal and sense how targets modify it. Magnetic sensors accept that the trespasser, for instance a person carrying weapons, has material that is magnetically sensitive [6]. Ferromagnetic material generates a particular magnetic signature, which can be sensed by means of a magnetometer. Footsteps of humans and animals, birds flapping their wings, etc., correspondingly make sound over and above the entity's voiced sound. Sensors designed to take measurements of sound are fundamentally hydrophones and microphones. Conversely, vibration-based motion sensors sense displacement, velocity, and acceleration using ismometers/geophones, velometers, and accelerometers, respectively. Additionally, in the case of heavy vehicles there might be coupling between the acoustic noise and ground vibrations [7]. The acoustic waves travel at different speeds and their amplitudes decrease at different rates with distance or get absorbed at different rates. This helps in distinguishing the type of intruding vehicle or other noise source. Table below shows a comparison between different types of sensors when used in detecting intrusions such as human beings, animals, or objects.

Table 1 : Comparison of the existing intrusion detection sensors [12]

Sensor	Low Power	Reliability	Cost
Infrared(Thermal)	Yes	Medium	Low
Ultrasound	No	High	High
Accelerometer(Seismic)	Yes	Low	High

Table above shows a comparison between different types of sensors used in detecting intrusion such ashuman beings, animals, or objects. Infrared, ultrasound and accelerometer are most common intrusion detection sensors. Comparing the infrared and accelerometer sensors, the infrared sensor has better movement detection properties [8]. In addition, an infrared sensor requires low energy and has an analogue output signal that gives the direction of an object's movement. Ultrasound sensors are used to locate objects such as human beings using the high frequency acoustic waves reflected from an object. The delay between transmission of the ultrasound pulse and the echo return helps determine the distance of the object. Accelerometer is a low power dynamic sensor used to determine the position and velocity, orientation or tilt and impact or vibration and shock.

IV. Intrusion Detection Sensor Models

An intrusion detection sensor model is a model of a real time intrusion detection system that is capable of detecting penetrations, break-ins and other forms of abuse. An intrusion detection sensor model helps discover distinct pattern that describes an abnormal or intrusion activity. The discovered distinct pattern is used to train the detection model to recognize abnormalities and intrusion. The models are built using low cost sensors that send sound and light data to help the model make an automated decision and report an abnormality or intrusion activity. Each model of the network can monitor the local region and then communicate through the wireless channels with the other nodes for the collaborative production of a high-level representing on the state of the environment [9].There are many different types of sensor models that can be employed in intrusion detection systems. Depending on the area to be covered and the type of space, different kinds of WSN can be deployed. Most of the outdoor applications are known to make use of microwaves, infrared, ultrasonic and radar sensor systems. The effectiveness of these models will depend on the target to sensor distance, environment, propagation characteristics, size and motion pattern of the target, amount of energy emitted, capability of the sensor etc[6].Below are the detailed descriptions about the most common detection sensor models.

a) *Probabilistic Model*

Probabilistic sensing model is an accurate sensing model adopted in the analysis of the quality of coverage of WSN. A probabilistic sensing model takes into account the detection probabilities of the sending device, which decay with factors such as distance, hardware configuration and environmental conditions [10]. The probabilistic sensing model helps develop intrusion detection systems whose sensors are deployed and distributed in a manner that meets the system requirements and minimizes cost. Probabilistic sensor model relies on the threshold distance within which an intruder can be detected wirelessly. This implies that the threshold distance is governed by the perimeter of the space within which the detection should occur. In relation to Elfes' model the detection probability can be described by such physical parameters of the sensors that are accommodated by the generic model parameters. If the target sensor distance is abbreviated d, the detection probability is an exponentially decaying function of *d*. The rate of decay is determined by two parameters; *y* and *B* which reflect the sensor characteristics [11]. In general the probability that a sensor will detect a target can be found using the following relation.

$$P_d = \begin{cases} 1 \\ e^{-\lambda}(d - d_t^1)^{\beta} \\ 0 \end{cases}$$

According to the formula above, the probabilistic sensing model sensor detects a target object with a probability of 1 if the distance between the target and the sensor *d* is below the threshold distance d_t. This is a simplified formula using *d* alone that can be deployed indoors where the light of sight is ensured. According to the following, the following conditions holds:

If $d<d^1_t$thenP$_d$= 0. However, the detection probability used if target object lies in a range of $d^1_t<d<d^2_t$, then an exponentially decaying function is deployed, using the parameters β and λ. The parameters β, λ, d^1_t *and* d^2_t are adjusted based on the physical characteristics of a sensor. Different detection models can be illustrated using the following figure. The figure shows three common detection models that are governed by different technical parameters.

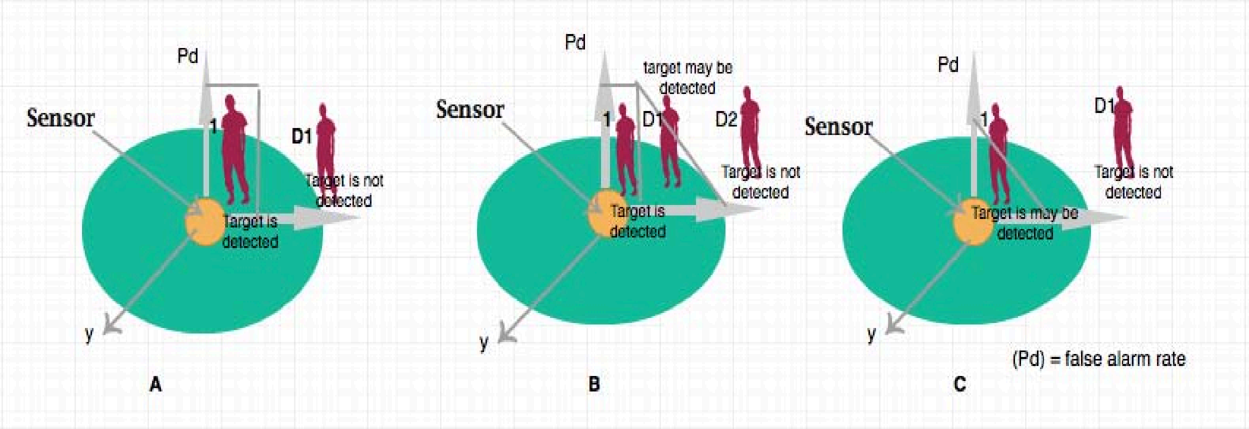

Figure 1 : *a) Binary Detector b) Elfes's Detector, c) Neyman-Pearson detector*

The probabilistic model is founded on the concept that the sensors will operate in the presence of additive white Gaussian noise. It is also assumed that the signal will undergo path loss. There are two hypotheses that represent the presence and absence of a target setup. The NP detector serves to compute the likelihood ratio which is used to compare the detection results against a threshold false alarm constraint [12]. The formulation of NP is provided below where Gaussian noise and path loss are assumed.

$$\text{pd}=1\text{-}\Phi(\Phi - 1(1-\alpha) - \sqrt{\gamma 9d)}$$

The above relation incorporates both target distance and the cumulative distribution function of zero mean unit variance Gaussian random variable at the point x. If the standard bounds are introduced into the system, then the probability can be computed as below. In the above formulation, *γ(d)* is a signal to noise ratio at the sensor, when a target is at a distance *d*. *Φ(x)* represents the cumulative function of the zero mean and unit variance Gaussian variable at a point *x*. The equation uses the proportionality $\gamma(d) \sim d^{-\eta}$. The formula below is derived using the standard bounds on *Φ(x)*.

$$pd \approx A(\gamma(d).\eta.\alpha)exp\{\Phi - 1(1-\alpha) - \sqrt{\gamma(d)}$$

Where A(ϒ(d)) is the signal to noise ratio level. It can be emphasized that the above model has demonstrated an exponentially decaying factors that is governed by the sensor-target distance [13].

b) *Exposure-Based Sensor Model*

The second model that is commonly used in the intrusion detection systems is the exposure-based sensor models. This model is based on the fact that the received energy level provides a clue on the observability. The expected level of observability within the monitored space is referred to as exposure. The total amount of energy that is received by the sensors at different points on the breath path is normally defined as the path of exposure[14]. The level of detection energy can be expressed as shown below.

$$Si(d) = \frac{k}{dk}$$

From the above formulation, *Si(d)* represents the signal energy of the target. The signal energy for the target is a measure from an *i*th sensor, and the distance between the target and the sensor is *d*. Where k is barrier coverage or the decay factor of the energy and dk is detection energy. *k* is a nonnegative constant that satisfies the condition 2<*k*<5 [15]. A multiplicative factor can be included in the system to cater for the effects of obstacles and other sources of errors. The most essential designing factor is the fusion of exposure levels where different types of sensor devices are deployed [16]. Using the preceding sensing and exposure model and knowing the threshold energy, can detect any kind of target. Finally the advantage of exposure-based coverage assessment is the inclusion of a practical object detection probability that is based on signal processing, signal distortion, as applicable to specific sensor types.

c) *Shape Based Intrusion Detection Models*

There is need for an intrusion detection system to ascertain the identity of the intruder. There is need for the system to distinguish between animal intrusion, human intrusion and any other object that may be used to intrude any object. Since this paper is meant for human and object intrusion detection mechanism, the algorithm developed will focus on the human and other object detection mechanisms. Most of the low-cost surveillance systems lack the capability of discerning the intrusion of animals from humans. The shape of a human being and the intruding objects are simplified through removal of the redundant points that connect short and straight line segments. The technique can be employed to search for best matched contour within the database in order to distinguish humans from other objects using different viewing angles and distances [17].

This methodology makes use of differential motion analysis which detects the scene change within perimeter of the surveyed region. The object contour is extracted by getting the difference between a reference and the test image. The differential motion analysis method eliminates illumination variations through subtraction. The polygon approximation technique integrated into the system to extract contour in order to remove the noise and as such eliminate redundant data points. This makes the shape to be represented using a fixed number of points. The shapes are described in a way that makes them invariant to rotation, scaling and translation using shape representation techniques such as turn angle and bend angle function. The shape features that are collected are used to measure similarity between the test contour and those contained in the database. The following Figure shows the basic steps that can be used to extract the shape of a human being.

An intrusion detection system under this model has a database composed of different shape features of possible objects through training. The database thus contains shape features of images taken from different times, locations, angles and distances. The new shape features of a target object is calculated from the contour and compared with a reference shape feature in the system database. The target and reference shape are matched based on either a similarity or a dissimilarity measure. A best shape match for a target object is one with a high similarity measure or a minimum dissimilarity measure with a reference shape feature. The matching helps determine the intrusion object.

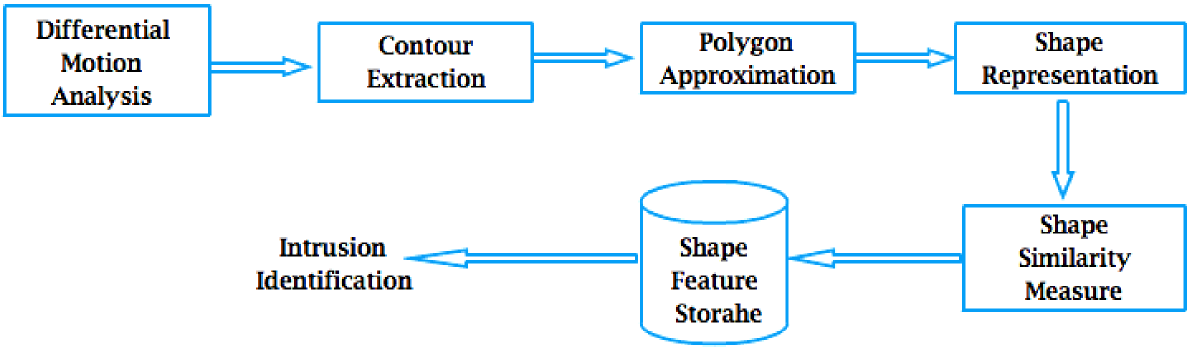

Figure 2 : Basic steps used to extract shape of human being

d) *Barrier Coverage Intrusion Detection Models*

Any kind of movement or crossing could be detected by the barrier coverage model. The purpose of barrier coverage is to detect intruders who attempt to cross from one side to the other side of the border area that you want to detect. Barrier coverage model is a technique whose goal is to minimize the probability of an undetected intrusion through a sensor network or a barrier. S But sometimes in some situations, it is not necessary for detecting both direction of crossing the belt. Therefore, barrier coverage is not suitable model since it may not differentiate the illegal intruders from the legal [18]. The barrier coverage can be considered as the coverage with the goal of minimizing the probability of undetected penetration through the barrier. Figure 3 shows the general of the barrier coverage problem where start and end points of the path are selected from bottom and top of the area. The selection of the path depends on the objective.

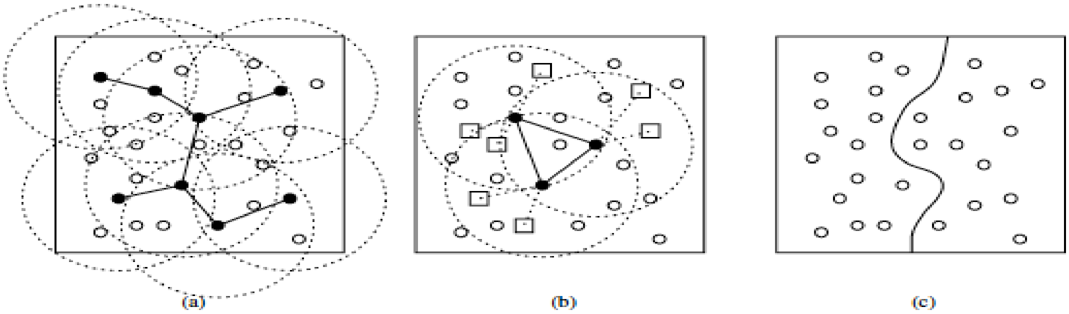

Figure 3 : (a) Random sensor deployment for square-shaped area; (b) random sensor deployment to cover set of points; (c) general barrier coverage problem [18]

Figure 3 represents a sample of random deployment of sensors to cover the perimeter of a square shaped area. The active sensors are represented by the set of connected black nodes through a scheduling mechanism inside the square shaped area.

V. Intrusion Detection Systemtechniques

Intrusion involves an activity that violates the security policy of a protected area or system, while intrusion detection is the process of identifying an intrusion. Monitoring illegal movement across a border is a challenging task. WSN is an emerging technology that is expected to provide new ways of energy and cost efficient border intrusion detection. An intrusion detection system technique is usually deployed as a line of defense to protect a border. Intrusion detection system techniques include the cost effective techniques deployed for monitoring critical applications ranging from border monitoring to industrial control. Intrusion detection techniques provide accurate detection and tracking of intrusion with minimal human intervention [19, 20]. Some of the existing intrusion detection techniques include dynamic mechanical analysis, infrared intrusion, neural network, and image processing detection systemare described below.

a) Dynamic Mechanical Analysis Detection System

Dynamic Mechanical Analysis (DMA)system considered to be a powerful technique that can be used to process the shape of a human being. The processing helps to distinguish the human beings from animals. It also helps the system to differentiate humans from other objects. The following Figure illustrates the working mechanism of DMA.

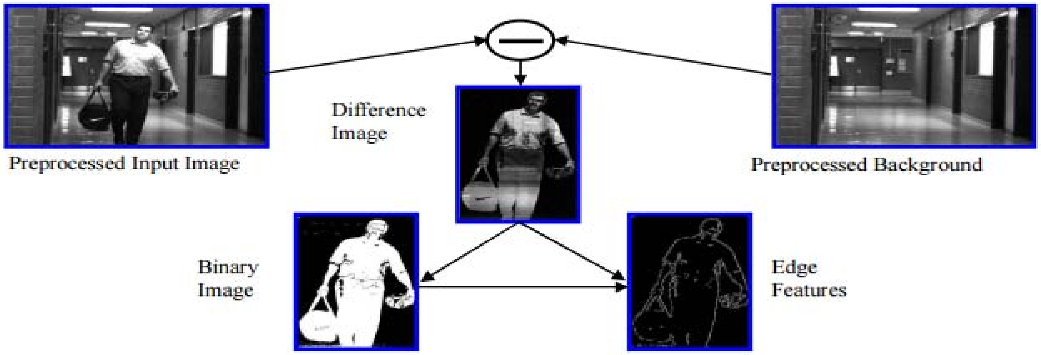

Figure 4 : Differential motion analysis using a reference background [2]

In Figure 4 the selected reference image was subtracted from the input image to provide the difference image. Also a linear threshold can be selected to binarize the difference image.It should be noted that shape descriptors and classification algorithms ought to be invariant to rotation, translation, scaling since the objects can be viewed from different angles, locations at different sizes. The following expression can be used to compute the data point reduction[17].

$$K(S1, S2) = \frac{|\beta(S1, S2) - 180|(S1)(S2)}{|(S1) + |S2)}$$

The formula above is a curve evolution technique that compares the relevance measures of the vertices on the contours. K is the relevance measure for the curve evolution method. K is modified to eliminate the redundant points while maintaining the significance of the contours. In the formula above, β is the turn angle on the vertex between the line segments s_1 and s_2. $l(s_1)$ and $l(s_2)$ represents the normalized lengths from a vertex to the two adjacent vertices. Applying the formula of the modified curve evolution reduces the short and straight line segments that provide little information about an overall shape of an object. This method easily measures shape similarity as it preserves a fixed number of data points and preserves detail shape information unlike other techniques that may lose data points containing critical shape information. This can be illustrated in the following series of figures which outline the distinguishing feature of animals against those of a human being.

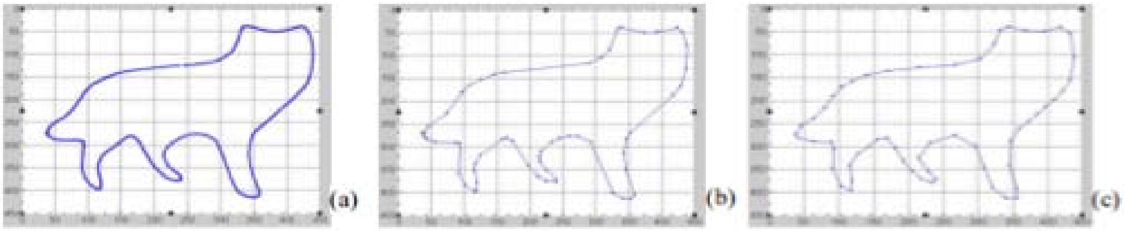

Figure 5 : (a) Original data set, (b) reduced to 60 points using Equation 5, (c) equal space sampling

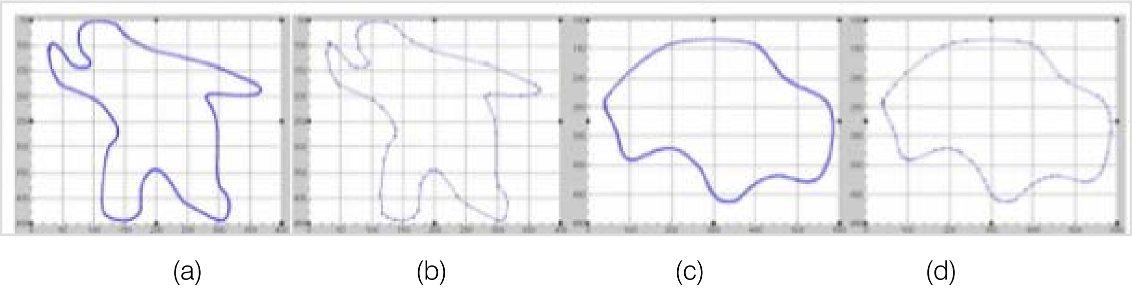

Figure 6 : Distinguishing features of animals against those of human beings [1]

In the above figure, 5(a) and 6(a) represents the original data set of a dog and human respectively. The data set is obtained through the use of contour extraction algorithm. Applying the equation above helps reduce the data set to obtain figure (b). The 60 data points contribute to the shape, and figure (c) is produced by equal space sampling of the data points. As we can see from the figure above, the bend angle have been reduced using the Fourier descriptors [21]. The any given bend angle function; the similarity of the two shapes can be established through Fourier expansion as shown below.

$$\Theta(1) = \mu 0 + \sum_{n=1}^{\infty} (an \;\; cos\, nl + bn \; \sin nl)$$

The Fourier descriptors derived above is used to measure the similarity between two shapes [22]. *An* and*Bn* are the coefficients for each frequency component. The below formulation shows how the coefficients can be derived considering that ϴ*(l)* is a step function.

$$\mu 0 = -\pi - \frac{1}{l} \sum_{k-1}^{\infty} \lambda k \; \theta k$$

$$An = -\frac{1}{n\pi} \sum_{k=1}^{m} \theta k \; sin \frac{2m\lambda}{L} \quad Bn = \frac{1}{n\pi} \sum_{k=1}^{m} \theta k \; cos \frac{2m\lambda}{L}$$

$$Where \; \lambda k \sum_{i=1}^{k} |, \; AND \; L = \sum_{i=1}^{\infty} | , = the \; total \; lenght$$

b) Infrared Intrusion Detection System

Infrared is one of thetechniques that can be employed to detect presence of intruders. In this system valuable information can be obtained from the human such as the location and the other necessary signal that will confirm presence of a human being. The system is known to make use of the rate of the heartbeat to detect human beings. The system makes use of infrared sensor that comprises of a light emitting diode which is adjacent to a phototransistor. The infrared sensor is used to measure the distance between the detector and the intruder. The infrared sensor consists of infrared LED and a pair of silicon phototransistors. The high intensity and long range infrared distance sensors can be used to determine the presence of an intruder accurately and precisely [23].

This technology makes use of infrared light that is absorbed well in blood and weakly in human tissue.

As such, if light that is reflected back from the skin of an intruder on account of blood passages is captured by the detector. The reflected light consists of intensity variations that occur as a result of variations in the blood volume in the tissue which give rise to variations in output voltages of the detector. The voltage variations are used to detect the heart rate. When the voltage variations are found to match those of the heart rate, positive results of the detection are assumed.

c) Neural Network Intrusion Detection System

A neural network is essentially a network of computational units that jointly implement complex mapping functions.Also it is a systems mainly focus on the face to detect the presence of an intruder. There are two main stages that are involved in the detection process; application of a set of neural network-based filters to the image and arbitration of the filter outputs. Cameras of high resolution are used to take live images which are processed by the system. The images taken are first introduced to a set of filters which look for the location that might contain the face. Once the face has been located, the arbitrator is used to merge the detections from the individual filters and hence eliminate the overlapping detections.

The first component of the system involves receiving the image at a specified pixel by the filter. The filter processes the image to given an output that signifies the presence or absence of the face. The following figure can be used to illustrate the algorithm of the underlying process.

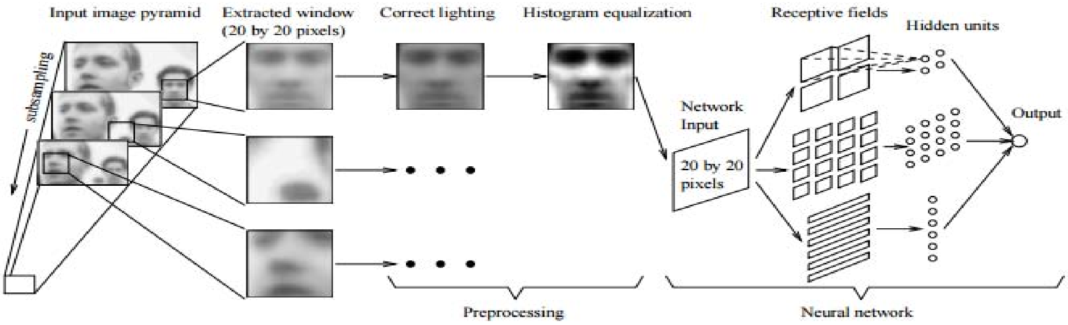

Figure 7 : Basic algorithm that is used to detect the presence of an intruder

The filter is normally applied at every location of the image in order to detect the face. Faces that may be larger than the window size are normally subsampled by a factor of 1.2 and the filter applied to each scale. The processed window is passed through a system of neural networks which determine the presence of the face. The neural network is normally trained prior to the detection on the general features of a face. This implies that neural networks are relied upon in confirming the presence of a face and therefore the presence of an intruder. It should also be noted that a minimum threshold on the number of detections is set in order to eliminate false detections [23]. The idea of using neural network is to discover patterns that describe an intrusion activity and train the neural network to discover them. The neural network system uses a set of 32 MicaZ sensor nodes. The nodes distributed along a perimeter to detect single and group intrusion.

d) Image Processing Detection System

The forthtechnique of intruder observation framework is image processing-based human intruder identification framework. It is by method for utilizing image to follow out whether there is a presence of trespasser/human intruder or not. Image processing-based human intruder location framework is broadly supported by numerous professionals when contrasted with robber alert frameworks and radar-based human intruder recognition, principally because of these four reasons: [24]

a. It helps catch pictures. The connected security camera is an extraordinary device to catch a photo of the robber/terrorist when they are attempting to break into a precluded domain.
b. More probability of the robbers/terrorists being caught. Control rooms have the capacity to view the photos from the cameras to distinguish intruders for easier arrests.
c. Security cameras are extraordinary aversion instruments. Robbers/terrorists are known for dodging region that has great security, particularly those fitted with security cameras.
d. Security cameras can secure defenseless ranges. At the point when control is inside the foundation's edge and needs to see what is going on outside of the adjacent building for security, security cameras are the most ideal approach for this objective securely.

In general, the image processing-based trespasser detection system could be a divided to two main categories: first is night vision/IR spectrum image processing-based human intruder detection system which can divide to digital video surveillance and analog video surveillance. The second one is vision spectrum image processing-based human intruder detection system which can known as type of video recording system applying digital technology.

VI. Recommended Technique for Intrusion Detection System

There are many techniques that are associated with intrusion detection systems. The DMA is considered to be the most powerful technique that can be used to process the shape of a human being. This process helps to distinguish the human beings from animals. It also helps the system to differentiate humans from other objects.Using DMA on the fact that is has capability of discerning human beings from animals and vehicles. The use of DMA is considered to be cost effective. It does not involve a lot of costs and time of installation. DMA is also known to consume less amount of energy as compared to other methods that were considered in the paper. Its processing time is also considered to be the least in considerations to other techniques mentioned in this paper.

VII. Conclusion

Wireless sensor networks have attracted lots of attention in recent years due to their potential in many applications such as border intrusion detection systems. The field of intrusion detection has been, and will continue to, develop rapidly. A number of models and techniques found in current systems are outlined in this paper. The paper relates the detection of human beings and other intrusion objects. Detection of intrusion for threat assessment and intruder identification requires the capability of distinguishing whether the intrusion object is a human, animal or other object. The techniques discussed in this paper uses simple electronic motion detection sensors that monitor the motion, or location of an object within a secured perimeter. This paper found out some Techniquesuch as DMA is the most suitable for various reasons. First, it can detect humans and non-human intruders. Second, it is not as expensive as other conventional methods. Third, it is easily scalable. Using, DMA the contours of an intruding object can be extracted for shape feature analysis. The paper highlighted how contour points are simplified by removing the redundant points that connect short and straight line segments. The intrusion detection techniques have been developed to best match contour feature in a database and that of a target to distinguish a human from an animal or other objects. The matching process of a target and database shape feature can be done from different angles and distances. The paper covers barrier and sensor coverage which is an important element in WSN. Future research can study communication issues and breach path problems.

References Références Referencias

1. Kim, D., Lee, S., Kim, T., & Park, J. (2012). Quantitative Intrusion Intensity Assessment for Intrusion Detection Systems. Security Comm. Networks, 5(10), 1199-1208.
2. Said Omar, and AlaaElnashar. "Scaling of wireless sensor network intrusion detection probability: 3D sensors, 3D intruders, and 3D environments" EURASIP Journal on Wireless Communications and Networking (2015): 1-12.
3. Liu, G. (2014). Intrusion Detection Systems. AMM, 596, 852-855. Doi:10.4028/ www.Scientific.Net/Amm.596.852
4. Vokorokos, L., Ennert, M., Dudláková, Z., &Fortotira, O. (2014). A Control Node for Intrusion Detection Systems Management. Aei, 14(3), 28-31.
5. Shamshirband, S., Anuar, N., Kiah, M., & Patel, A. (2013). An Appraisal and Design Of A Multi-Agent System Based Cooperative Wireless Intrusion Detection Computational Intelligence Technique.Engineering Applications Of Artificial Intelligence, 26(9), 2105-2127.
6. Sheltami, T., Basabaa, A., &Shakshuki, E. (2014). A3acks: Adaptive Three Acknowledg ments Intrusion Detection System For Manets. J Ambient Intell Human Comput, 5(4), 611-620.
7. The SmartDetect Project Team. (2010). Wireless sensor networks for human intruder detection. Journal of the Indian Institute of Science, 90 (3), 347-380
8. Absar-ul-Hasan, Ghalib A. Shah, and Ather Ali. “Intrusion Detection System Using Wireless Sensor Networks'. EJSE Special Issue: Wireless Sensor Networks and Practical Applications”, (2010): 90-99. Web. 17 Sept. 2015.
9. Mosad HAlkhathami, Lubna Alazzawi.(March-2015). "Border Security Control via Distributed WSN Technolog.",International Journal of Scientific & Engineering Research, Volume 6, Issue 3.
10. Hasan, Osman, and SofièneTahar. (2015) Formalized Probability Theory and Applications Using Theorem Proving. Internet resource.
11. Fuchsberger, A. (2005). Intrusion Detection Systems and Intrusion Prevention Systems. Information Security Technical Report, 10(3), 134-139.
12. Aldosari, Saeed, and José MF Moura.(2007). "Detection in sensor networks: The saddlepoint approximation." Signal Processing, IEEE Transactions on 55.1 327-340.
13. Barry, B., & Chan, H. (2010). Architecture And Performance Evaluation Of A Hybrid Intrusion Detection System For IP Telephony. Security Comm. Networks, 6(12), 1539-1555.
14. Boob, S., &Jadhav, P. (2010). Wireless Intrusion Detection System. International Journal of Computer Applications, 5(8), 9-13.

15. Smolinski, Tomasz G, Mariofanna G. Milanova, and Aboul E. Hassanien. Applications of Computational Intelligence in Biology: Current Trends and Open Problems. Berlin: Springer, 2008. Print.
16. Cai, C., & Yuan, L. (2013). Intrusion Detection System Based On Ant Colony System. Journal of Networks, 8(4).
17. Farah, N., Avishek, M., Muhammad, F., Rahman, A., Rafni, M., & Md., D. (2015). Application Of Machine Learning Approaches In Intrusion Detection System: A Survey. Ijarai, 4(3).
18. Sindhuja, L. S., and G. Padmavath, (2015). "Clone Detection Using Enhanced EDD (EEDD) with Danger Theory in Mobile Wireless Sensor Network." International Journal of Security & Its Applications
19. Mosad Alkhathami, Lubna Alazzawi, and Ali Elkateeb,(Apr 2015)"Border Surveillance And Intrusion Detection Using Wireless Sensor Networks", IJAET,Vol. 8, Issue 2, pp. 17-29.
20. B. Sun, L. Osborne, Y. Xiao, and S. Guizani, (Oct 2007) "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," *IEEE Wireless Comm. Magazine,* vol. 14, no. 5, pp. 56-63
21. Janakiraman, S. (2009).An Intelligent Distributed Intrusion Detection System Using Genetic Algorithm.JCIT.
22. Zhang, Dengsheng, and Guojun Lu.(2009). 'A Comparative Study On Shape Retrieval Using Fourier Descriptors With Different Shape Signatures'. n. page. Web.
23. Korcak, M., Lamer, J., &Jakab, F. (2014). Intrusion Prevention/Intrusion Detection System (IPS/IDS) For Wifi Networks. IJCNC, 6(4), 77-89.
24. Wong, Wai Kit, Chu Kiong Loo, and Way Soong Lim. (2013)."Omnidirectional Human Intrusion Detection System Using Computer Vision Techniques." Effective Surveillance for Homeland Security: Balancing Technology and Social Issues 411.

This page is intentionally left blank