Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

Mobile Host Intrusion Detection in Surveillance Wireless Sensor Networks with Fusion of Sensor Data

J. Josephin Jinisha*

*Corresponding Author, Department of Computer Application, Noorul Islam Centre for Higher Education, Tamilnadu, India. E-mail: jinishamelbin@gmail.com

S. Jerine

Department of Software Engineering, Noorul Islam Centre for Higher Education, Tamilnadu, India. E-mail: ssjerine@gmail.com

Abstract

In intrusion detection applications, wireless sensor networks are commonly used. Many research literature papers are aimed at generating and evaluating the information on intruder detection in terms of probability of detection and false alarm rates. In two modalities, the model for acoustic signal and the sensor probability model, and in this research paper, the problems of passive motive intrusion detections have been solved. The aim is to establish a three-stage hierarchy to determine if mobile intruders are present. The sensor nodes at the fundamental level have a k-mean clustering grouping. For binary hypothesis testing, the strengths or probabilities in the cluster head are employed. Cluster leaders send their judgments to the Fusion Centre (FC) after completing a Likelihood Ratio Test (LRT) to ensure invaders are correctly inferred. A numerical analysis of the signals received determines the optimal value for probability computation. The resulting fusion rule maximizes detection likelihood regarding the allowed falsifying rates. The number of absolute sensor nodes determines the exact fusion rule. Compared to earlier fusion rules, simulation results show that the new fusion rule has a better ability to follow mobile invaders and enhanced accuracy and detection speed.

Keywords: False alarm rate; Binary hypothesis; Probability detection; Wireless sensor network; Mobile intruder detection.

Journal of Information Technology Management, 2023, Vol. 15, Special Issue, pp. 67-77
Published by University of Tehran, Faculty of Management
doi: https://doi.org/ 10.22059/jitm.2023.91568
Article Type: Research Paper

Received: December 22, 2022
Received in revised form: January 15, 2023
Accepted: February 20, 2023
Published online: March 15, 2023

Introduction

Sensor fusion is of utmost importance when it is necessary to reliably and accurately detect and monitor intricate in the Surveillance Wireless Sensor Network (SWSN). Multiple heterogeneous sensor nodes are used to create a network. Those sensor nodes offer a tremendous amount of information about the presence/absence of surveillance intruders, which is incompatible and unknown (Ciuonzo et al., 2017). Various sensing methods, like seismic, acoustic, radiographic, thermal, optical, and photo sensing, are used to detect intruders. The possibility of seeing false alarm rates is used to assess detection quality. Various models, such as Received Signal Strength (RSS), Time Difference of Arrival (TDoA), and Direction of Arrival DOA, are used to determine these probabilities. Different procedures are needed in the fusion centre to process the data obtained to find them. This data treatment is much more relevant, accurate, and informative than the original information. Each sensor node collects the initial data from the single-bit data collection (Lou et al., 2019).

Literature Review

The use of fusion technology is used when intruders are detected to deduce noisy observations of students. Many researchers have suggested several novel solutions to achieve this objective. For intruder detection, different types of sensor nodes are used. The pyro-infrared detector (PIR) was employed to detect human intrusts (Ciuonzo et al., 2017). A fusion rule is developed (camera and microphone) for wireless multimedia surveillance applications (Li & Hu, 2003). Many wireless network fusion approaches, including military, healthcare, and robotics, are discussed by (Li et al., 2015). The diverse sensor types employed for these applications were also discussed.

Niu et al., (2006) proposed a rule that considers the number of total detections as statistics on the decision. First, each node separately selects an intruder based on noise signals received and decides on the results of its nearby node detection (Katenka et al., 2007). The signal power must exceed the limit. The Central Limit Theorem (CLT) is estimated when it is used for the previously sensed values. It has been concluded that the local voting fusion technology best uses this algorithm at a fixed false alarm rate than the optimal fusion. The model's ability to attenuate the signal is not entirely reliant on it. An OR-Rule is proposed for threshold merging for successful sensors based on a bright sign at each sensor node (Yazici et al., 2019). Chebyshev's OR-Rule Inequality determines the threshold value based on statistical measurements of the sensors. This rule estimates the intrusions and rate of effect using the threshold distance between the interferers and the sensor nodes (Xiong et al., 2015).

The Gaussian distribution calculates the incursion probability and compares the findings to standard distributions. For Gaussian distribution performance evaluation, different network properties, such as single and multiple sensing models and an intrusion distance, are used

(Nardelli et al., 2016). A two-level algorithm is proposed for non-cooperative intrusion detection (Zhu et al., 2010). Noise values of each node of sensors are transferred via the binary symmetric channel to the fusion centre (BSC). The FC produces results worldwide. Statistical data for General Rao Test (GRT) is considered for the signal received, and a rule of fusion is made. The simulation showed that this fusion rule has less computational complexity than the GLR. Abrardo et al., (2017) have analyzed all electromagnetic signals that detect intrusions in fusion inputs.

Many research studies examine magnetic signals for vehicle detection and provide unreliable findings. To tackle this problem, Varshney (2012) suggested a vehicle recognition method based on GPS, SNR, and magnet signaling parking. When the sampling rate was set to 1 Hz, 99.83% of the samples were correctly identified. The probability of detection mistakes is a crucial performance indicator for fusion-based intrusion techniques. By determining the exact likelihood of an error, we may obtain information regarding the existence of mobile invaders.

The findings are derived utilizing the information above methods and a basic signal decay model. The received signal is sent into the binary generating hypothesis (H0/H1) as an input. H0's null, and H1's distinct. The H1 is zero and zero. In most algorithms, the intrusion characteristics and categories are not adequately defined. The type of application must be correctly defined because WSNs are application-specific networks.

Contextuality of the Work

Sensor fusion may be classified into three main modes: a merging of decision-making data fusion. A fusion centre (FC) test input specifies the total number of detection node outcomes in data fusion. The FC then makes the detection judgment. Data fusion is a central fusion technology (Jusoh & Almajali, 2020). The results of this fusion process are pretty precise. However, many detection data transfers are required, increasing total communication and energy usage. Fusion decision, on the other hand, is a distributed fusion strategy. Based on data from every node, each sensor node determines whether or not an intruder is present. This technique has the advantage of reducing overall communication and improving network processing.

The energy consumption issue, therefore, remains the same. The essential functional fusion characteristics are indicated and extracted from the signal of the sensor node. Each node's features are passed on to the FC. The data transferred to the FC is less due to the extraction function. Due to the reduced data size compared with data fusion and decision fusion, the results generated by this technique are less accurate (Niculescu & Nath, 2001). This article uses the fusion decision to conclude mobile passive intrusion detection with the advantages and demerits of three fusion techniques being considered. Integrating data from various radars, lidars, and cameras to provide a comprehensive view of the surroundings is called sensor fusion. Because it accounts for the strengths of the many sensors, the resultant model is more accurate.

Importance and Role

This work looks at intrusion detection in challenging and sensitive environments. Only static sensor nodes can be employed randomly in these areas for efficient and accurate identification of intruders because the base station cannot entirely rely on the single node's sensing results in real time. The results from using several sensor nodes are combined to demonstrate that the mobile intruder is present and intercepted. This problem statement presents other challenges: computation accuracy and completeness. In this paper, the main contributions are:

1. When a sensory intrusion area is intercepted, static sensor nodes perceive the presence of the passive mobile intruder within each cluster. Measuring the intruders is based on the acoustic $E_n(t)$ and probabilistic models Sn(t).

2. A three-tier hierarchy for decision fusion is presented to increase the accuracy of detection findings.

3. To minimize the wrong alert rate and maximize the probability of detection.

4. To compare the number of sensors, mobile intrusion speeds, probability of detection, false alarms, and the accuracy of the model results.

Mobile Intruder Detection: Design Concept

The passive mobile intrusion detection problem has now been resolved with decision-making fusion. Passive intruders are data that are not known as positioning and signal properties for the sensory nodes used. An intruder must be detected when a sensor node sensing area is intercepted. Malicious vehicles are considered to be passive intruders in sensitive areas in this document. When the car roams randomly, it is deemed harmful to a sensitive region. They know precisely how to go from one side to another as approved cars. The basis for successfully detecting the intrusion is a 3-stage hierarchy illustrated in Figure 1. This hierarchy contains multiple baseline sensors. The sensor nodes are sound-receiving nodes for acoustic sensors that detect the intrusion result. With the long distance between sensor nodes and moving intruders, the strength of the acoustic signal decreases. Clusters with mean k-clusters are classified as sensor nodes. Each sensor node is known as the cluster head of each cluster for the vital energy, ribbon width, communication, and sensing power nodes. It was also regarded as a cluster head for middleware. The cluster leaders send the joint decision to the fusion centre in a high-quality format. The discussion concludes with two types of communication links: 1) communication between sensor nodes and cluster heads and 2) communication between cluster heads and the fusion centre. The passive intrusion instrument is constantly challenged by noise and interference in the signal caused by environmental elements such as regional obstructions, wind, and external noise. The primary purpose of this paper is to find the most likely intruders to detect Pdet while limiting the false alarm rate of Pfp.

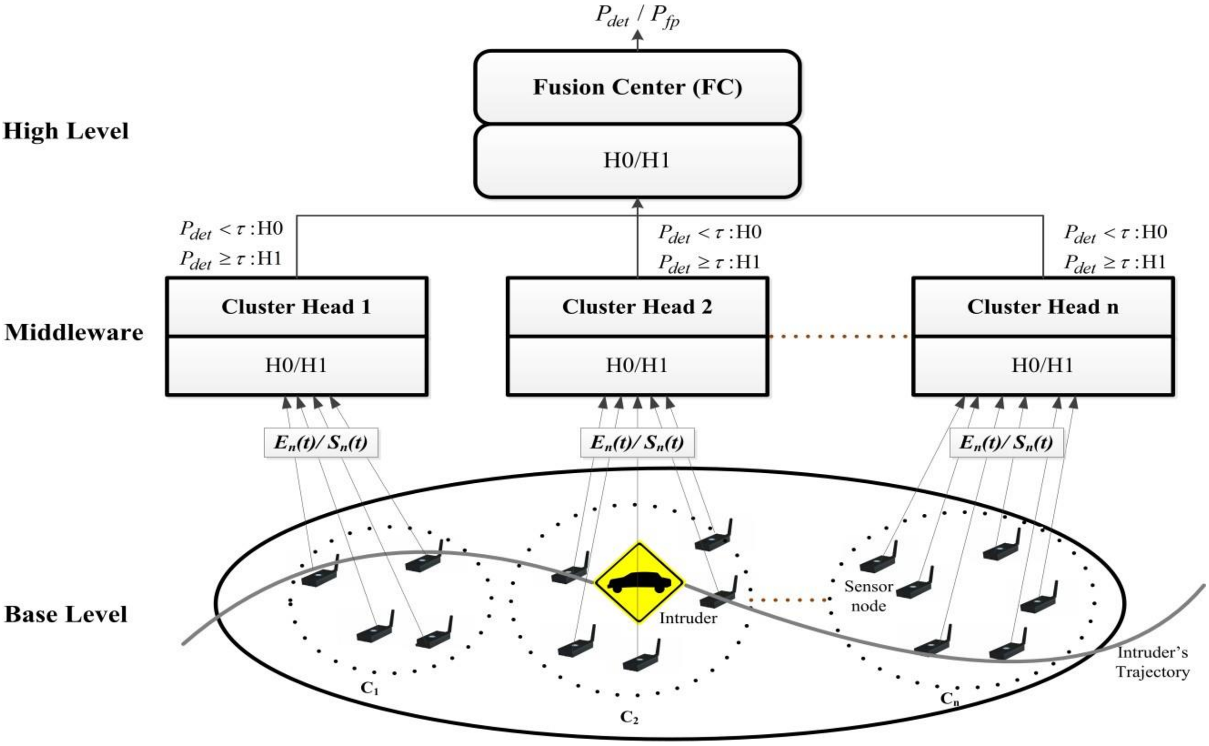

Figure 1. Architecture of intrusion detector

The intruder's presence in the literature is based on the probability of detection of different signal characteristics. The study calculated the likelihood of detection by Pdet and concluded that the intruders contain both the acoustic signal model and the probabilistic sensor model (Onur et al., 2007). When sensor nodes in open areas are used, the son emitted by a car detects the insect and locates it. Signal Strength En(t) and Sn at 'T' time intervals are the outputs of these models (t). As input to each sensor node, these findings are given in the binary hypothesis test H0/H1. Neyman Pearson Lemma presents the binary hypothesis. The NP test is used to detect an intruder on the cluster head. The FC provides a final indicator of an incursion into the sensitive region after a Likelihood Ratio Test (LRT) with probabilities and false alarm rates. The cluster managers' decisions determine the outcomes.

Network Model and Sensor Fusion Algorithm

The sensitive area Ar shall be equipped with a random distribution of an active series of N nodes, Si I = 1, 2, 3, ..., N). For each sensor node Rs standard and Rc where Rc < 2Rs are used. The sensitive region is deemed optimally covered to prevent intruder detection. There are also impediments in the exposed region that decay or disrupt, as well as the sensor node's probability. Every sensor node was assumed to be a well-known location algorithm after deployment (Zhu et al., 2010). The difference between the present and estimated sensor node placements is considered random.

As seen in Figure 1, sensor node sub-sets are clustered together and referred to as clusters. A series of MI clusters exist. Sensor fusion supplies the CHi sensor findings to each MI cluster sensor node as a cluster head. The results are provided as a binary test entry for the CHi assumption. The Cluster CHi head decides if an intruder is in the sensitive area and informs the FC about the choices that have been made. When the received signal force en(t) is higher or equal to the value Sn(t), an intruder is detected. Each sensor node contains the actual sensor results of gaussian additive noise. A central probability limit theorem and false pre-survey alarm rates will determine the threshold value. The main aim is to maximize the possibility of Pdet detection at any fake alarm rate. The process is discussed step by step below.

Algorithm 1: Mobile intrusion detection algorithm

```
Initialize
N -Total number of sensor nodes
M- Number of clusters
$A_r$ - Area of the sensitive region
Uniformly deploy N sensor nodes inside $A_r$
Divide N sensors into M clusters through k-mean clustering
select the sensor at the cluster centroid as cluster head CH; in each cluster C
for each cluster, CHi € M do
    for each sensor node Sj € Ci do
        compute the energy of acoustic signals $E_m(t)$ using (2)
        transmit $E_m(t)$ to CHi
    end for
    compute the intruder detection probability $P_{det}$ at cluster head CH,
    test binary hypothesis H0 and H1 using (3)
    transfer $P_{det}$ to the fusion centre FC if $P_{det} \geq \tau$ and H1 is true.
end for
test maximum likelihood of H1 using (9)
generate intruder detection inference.
```

Performance Evaluation

OMNet++ simulates the fusion sensor protocol proposed and conducts a numeric analysis of Python. Initially, in sensitive zones with an area of Ar = 2500 m2, 50 static 30-meter nodes, as shown in Figure 2. Clusters and cluster heads are used in the K-mean clustering. Figure 2 shows the different colors of each cluster's sub-set of sensory nodes. A mobile intruder intercepts the sensitive area as a red star. Nodes (S34, S40, S47, and S48) are detected to detect the intruder. These sensor nodes convey the energy to the CH8 head. For various -factor decay levels, Figure 3 depicts the power received by sensor nodes inside CH8. The decay factor value increased from 1 to 4 as the acoustic energy increased. As a result, the best deals for calculating acoustic energy are 2 and 3.

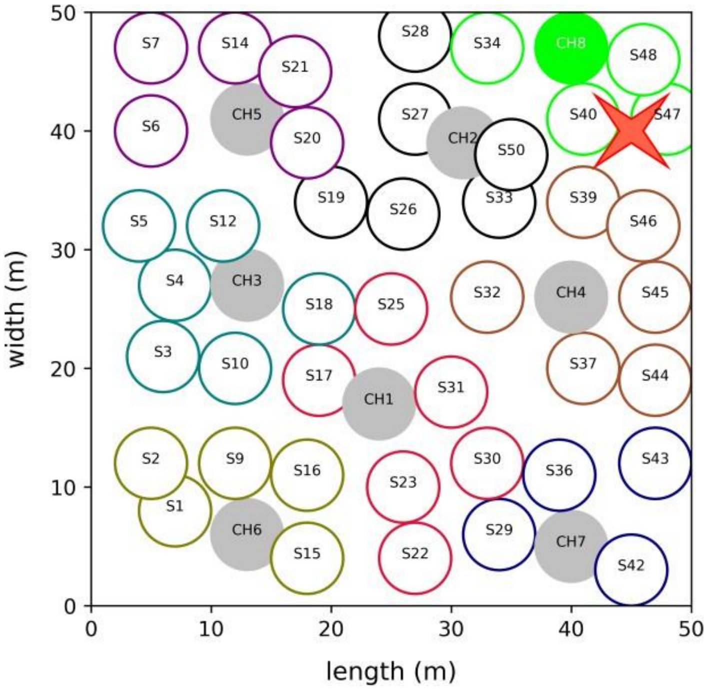

Figure 2. N=50 clustering

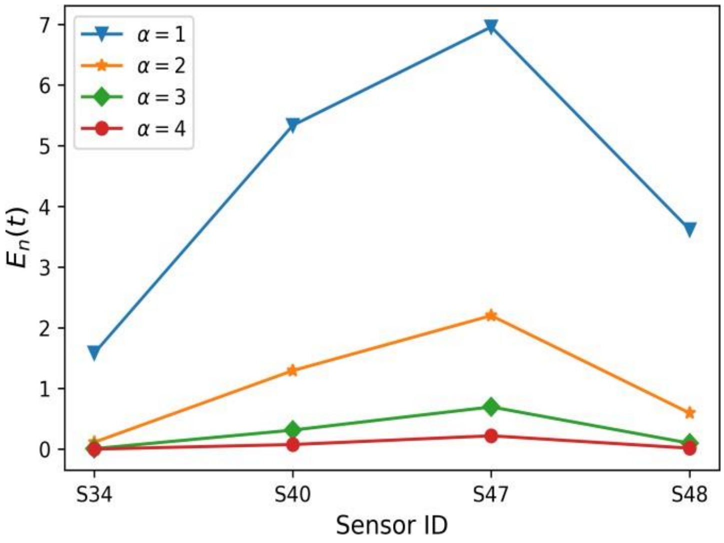

Figure 3. Acoustic energy at each sensor

Figure 4 shows that different cluster heads receive total sound energy when the sensitive area is intercepted randomly by the intruder. The intruders pass through the sensor nodes in these clusters. In three random pathways, the energy accumulated was shown on the heads of the groups. These values are tested for the hypothesis of the presence of intruders. Moreover, the probability of detection and the wrong alarm rates on cluster heads are calculated.

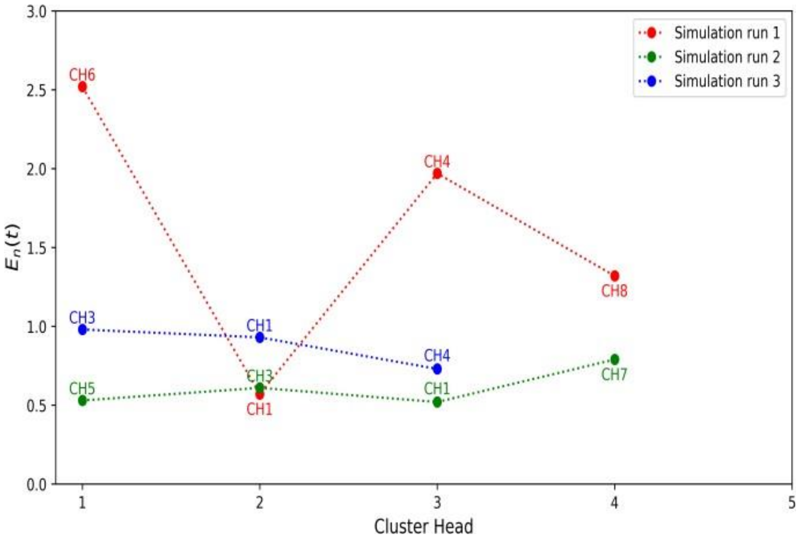

Figure 4. Binary hypothesis testing

Figure 5 depicts the number of sensors and the chance of false alarm detection. This graph shows the link between detection probability, sensor count, and false alarm rate. The case of detection improves as the number of sensors grows and the rate of bogus alarms decreases. We can attain the highest likelihood of detection with optimal sensor counts and false alarm rates. In addition, the LRT hypothesis evaluates the probability of detection. About H0, this test yields the highest likelihood of H1.

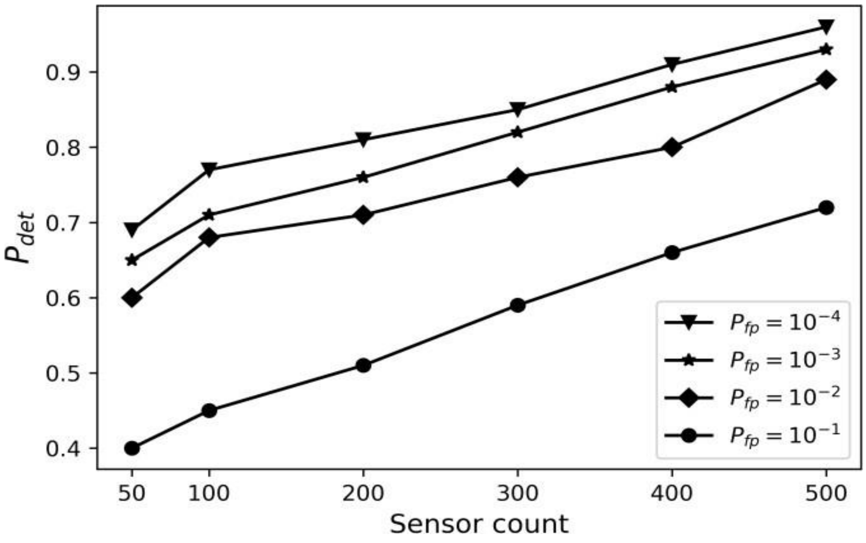

Figure 5. Detection of false alarm

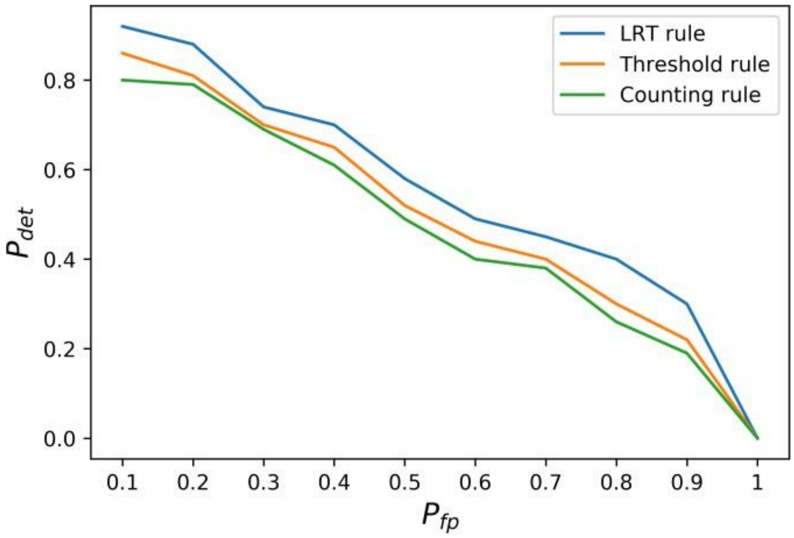

Figure 6. Comparison of different fusion methods (false alarm)

The suggested LRT fusion rule performs similarly to the counting and detection threshold rules at various false alarms. Figure 6 illustrates that the LRT fusion rules are superior to two other fusion rules. The information received is combined with the decisions of the different heads of the fusion centre in Figure 1. Then the findings are fused into a cluster head.

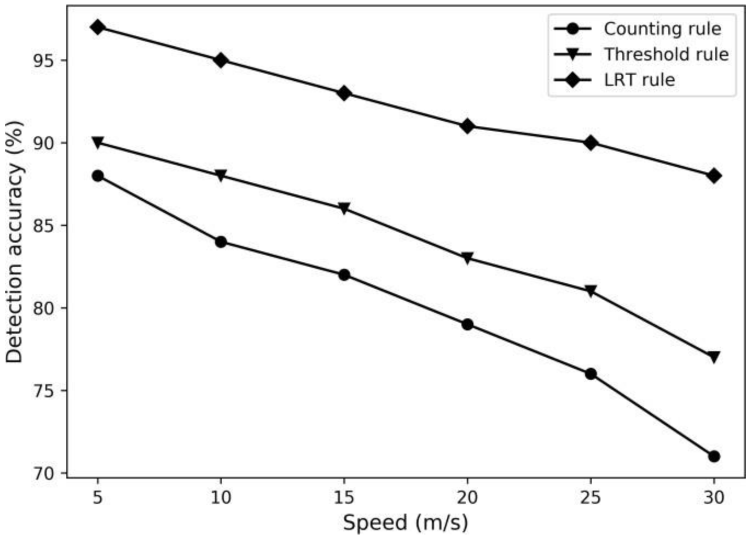

Figure 7. Comparison of different fusion methods (speed measurement)

The accuracy of the mobile intruder speed measurement was defined in Figure 7. Because the speed of the fusion rule for mobile intrusion detection is a critical factor with increased intruding speed, the detection accuracy decreases. The proposed fusion rule also indicates that speed increases are far more effective when mobile intruders are detected than other fusion regulations.

Conclusion

To accurately detect mobile intruders over wireless sensor networks, Fusion rules play an essential role in monitoring sensitive areas. This research paper, therefore, proposed a three-level fusion sensor hierarchy algorithm for intrusion detection because of its suitability. The K-medium baseline clustering groups the randomly installed nodes in the sensor. The main objective is to optimize the chance of intrusion detection and minimize counterfeit alarms. The received signals are fused into the cluster head first to achieve maximum detection probability. Thus, they will be connected using the Likelihood Ratio Test at the fusion centre, according to the suggestion for a rule on fusion. The results of the simulations show that the suggested sensor count fusion rule, mobile intrusion rate, probability of detection, precise detection, and false alarm rate are optimal and correct. State estimation theory is used to determine the most likely locations of the invaders and quantify the associated error rates. The mistake is the space between the mobile intruder's actual and estimated positions. Locations with the highest likelihood of a mobile invader moving through them are the most likely destinations. The mobile intruder model also can determine the mobile intruder's following potential locations, which aids in the scheduling of deployed sensor nodes.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

Abrardo, A., Martalo, M., & Ferrari, G. (2017). Information fusion for efficient target detection in large-scale surveillance wireless sensor networks. Information Fusion, 38, 55-64.

Ciuonzo, D., Rossi, P. S., & Willett, P. (2017). Generalized Rao test for decentralized detection of an uncooperative target. IEEE Signal Processing Letters, 24(5), 678-682.

Jusoh, S., & Almajali, S. (2020). A systematic review on fusion techniques and approaches used in applications. IEEE Access, 8, 14424-14439.

Katenka, N., Levina, E., & Michailidis, G. (2007). Local vote decision fusion for target detection in wireless sensor networks. IEEE Transactions on Signal Processing, 56(1), 329-338.

Li, D., & Hu, Y. H. (2003). Energy-based collaborative source localization using acoustic microsensor array. EURASIP Journal on Advances in Signal Processing, 2003(4), 1-17.

Li, Y., Jha, D. K., Ray, A., & Wettergren, T. A. (2015, July). Feature level sensor fusion for target detection in dynamic environments. In 2015 American Control Conference (ACC) (pp. 2433-2438). IEEE.

Lou, L., Zhang, J., Xiong, Y., & Jin, Y. (2019). Robust static vehicle detection method based on the fusion of GPS SNR and magnetic signal. IEEE Sensors Journal, 19(21), 10111-10120.

Nardelli, P. H. J., Ramezanipour, I., Alves, H., de Lima, C. H., & Latva-Aho, M. (2016). Average error probability in wireless sensor networks with imperfect sensing and communication for different decision rules. IEEE sensors journal, 16(10), 3948-3957.

Niculescu, D., & Nath, B. (2001, November). Ad hoc positioning system (APS). In GLOBECOM'01. IEEE global telecommunications conference (Cat. No. 01CH37270), 5, 2926-2931.

Niu, R., Varshney, P. K., & Cheng, Q. (2006). Distributed detection in a large wireless sensor network. Information Fusion, 7(4), 380-394.

Onur, E., Ersoy, C., Deliç, H., & Akarun, L. (2007). Surveillance wireless sensor networks: Deployment quality analysis. IEEE Network, 21(6), 48-53.

Varshney, P. K. (2012). Distributed detection and data fusion. Springer Science & Business Media.

Xiong, J., Li, F., & Liu, J. (2015). Fusion of different height pyroelectric infrared sensors for person identification. IEEE Sensors Journal, 16(2), 436-446.

Yazici, A., Koyuncu, M., Sert, S. A., & Yilmaz, T. (2019). A fusion-based framework for wireless multimedia sensor networks in surveillance applications. IEEE Access, 7, 88418-88434.

Zhu, M., Ding, S., Wu, Q., Brooks, R. R., Rao, N. S., & Iyengar, S. S. (2010). Fusion of threshold rules for target detection in wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 6(2), 1-7.

Bibliographic information of this paper for citing:

Josephin Jinisha, J. & Jerine, S. (2023). Mobile Host Intrusion Detection in Surveillance Wireless Sensor Networks with Fusion of Sensor Data. *Journal of Information Technology Management,* 15 (Special Issue), 67-77. https://doi.org/ 10.22059/jitm.2023.91568