International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Robust Intrusion Detection Mechanism in Wireless Sensor Networks Against Well-Armed Attackers

Antony Joseph Rajan D*[1], Gomathy C K[2]

Submitted: 13/11/2022 **Accepted:** 16/02/2023

Abstract*:* Recent research has given sufficient attention to intrusion detection as one of the most significant techniques to guaranteeing wireless sensing network security. However, with the advent of electronic anti-reconnaissance equipment, the intruder may learn the precise locations of detecting nodes and then use proposed system data to plot a course that will take him or her past them undetected. Such a threat is characterized as an empowered invader who poses novel difficulties for existing intrusion detection techniques. When detection nodes are first deployed at random, coverage gaps may appear in certain places, making it impossible to achieve the intended detection impact. To combat these problems, we provide a concept for a sensing network in which cars work together to offer intrusion detection against armed attackers. Our solution incorporates a sleep-scheduling technique for stationary nodes and an algorithm for mobile sensing devices to pursue targets. To close the coverage gaps, mobile monitoring devices will follow the empowered intruder, meanwhile static nodes will adhere to a sleep-scheduling algorithm and be roused by neighboring detection nodes. To evaluate the efficacy of our concept in terms of intrusion detection, energy consumption, and the range over which sensor nodes may move, we conduct simulation experiments against established methods. Extensive simulations are also run to examine the sensitivity of the parameters. Our idea has been shown to be more efficient and available through theoretical research and simulation.

Keywords: *intrusion detection, wireless sensor networks, attack detection, energy management.*

1. Introduction

Low-cost and simple to install, wireless sensor networks (WSNs) are constructed from a large number of wireless sensor nodes through wireless communication. Its use has spread to a variety of real-world contexts, including environment perception, contemporary logistics, and military surveillance. These contexts all need the coordinated efforts of several sensor nodes to keep tabs on their surroundings and identify any potential threats [1]. One area of attention is the development of intrusion detection systems that may be used in a wide variety of contexts, including border patrol, region monitoring, and post-disaster rescue. It may be treated as the penetration optimization method to obtain continuous and high coverage of the invader, which necessitates a constant tracking and monitoring method [2].

There are two types of recent research on intrusion detection. The first makes advantage of the sensory information from numerous nodes based on decision fusion or local voting approaches to perform more precise localization and trace prediction of the target. The second, which may be seen as an extension of classic coverage optimization issues, is the focus of proposed system study. It investigates the deployment and movement strategy of sensor nodes to obtain enhanced dynamic coverage of the target. Initial deployment placement of the sensor nodes has a major impact on the quality of coverage [3]. The deployment of sensors is typically not a manual process because of the distant or hostile nature of the sensing locations.

As a result, sensors are often dispersed by dropping them from a plane, although the precise landing location is unpredictable owing to factors like wind and natural obstructions like trees and mountains. As a result, dropping sensors in some locations may not improve coverage in others, and certain regions may have "interference problems," or spots where no sensor nodes are present [4]. Recent developments in embedded technology and miniature robotics make it possible to implement such mobile sensors for intrusion detection, providing a potential solution to the aforementioned issue. While static sensors remain in one place, mobile sensors may be relocated to provide the appropriate coverage.

[1] *Research Scholar SCSVMV UNIVERSITY, Kanchipuram, Tamil Nadu, India. *antonyjosephjmj@gmail.com*

[2] *SCSVMV UNIVERSITY, Kanchipuram Tamil Nadu India ckgomathy@kanchiuniv.ac.in*

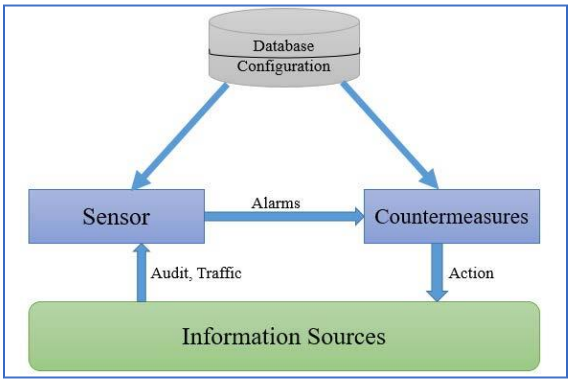

Fig. 1. Overview of Intrusion detection System

Unfortunately, other than bettering coverage, such participating devices are unable to identify and monitor attackers. Furthermore, as technological anti-reconnaissance science advances, the attacker in real-world applications may be armed with sensing devices that may learn the positions of monitoring nodes and then plot a course around them. A "motivated attacker" is one who, unlike a "naive invader," is able to avoid detection by evading the tracking of sensor nodes. Therefore, it is a difficult task to create an efficient intrusion detection strategy for attackers with access to resources. Centralized intrusion detection techniques have traditionally been used for border patrol and area monitoring. When an intrusion is detected, the information is relayed to the access point or cluster component, which then analyses and processes the data before taking appropriate action [5].

In addition to consuming a lot of network bandwidth, the process will necessitate constant communication between the detection nodes and the base station or cluster node, which will increase the transmission delay of network and delay emergency treatment in the event of an intruder fleeing or a sabotage. This means that the standard, centralised design isn't going to cut it in the real world, especially not when dealing with armed adversaries. Ordinary mobile nodes lack the capability to record and interpret the trajectories of monitored invaders in real time, which is necessary for local computing [6].

Having mobile and fixed sensors work together opens up a new area of study for WSNs. We take mobile sensing devices as the mobile nodes and incorporate them with the base stations to form a vehicular collaboration sensing network, which is inspired by the robust mobile computing, communication, positioning, and information process technology of autonomous fully automated vehicle, particularly unmanned armoured vehicle. Further, we have included the idea of edge computing through into vehicle collaboration sensing network to meet the needs of low latency and high-quality performance in intrusion detection. With edge computing, computations may be executed close to the origins of the data they process. In our strategy, as illustrated in Fig.1, a movable sensing device is chosen to serve as an edge computing component in a certain area. The edge computing node will be notified by the detection nodes if an intrusion is detected [7].

After the tracking choices have been published, the edge computing node notifies the appropriate mobile sensing devices so that they may follow the directions to locate the intruder and patch any gaps in coverage. In proposed system research, we propose a model for a sensing network in which movable sensing devices and stationary sensor nodes work together to offer intrusion detection against armed attackers [8]. The model's goals are to maximise coverage while minimising energy drain from detecting nodes, and to simultaneously log and process the movements of any trespassers as they are discovered. As a result, we devise a plan for the motion of the mobile sensing devices as well as a plan for the resting of the stationary nodes [9].

The following main research contributions are elaborated in proposed system paper:

- Initially, we define motivated invader motion and model it using a set of specific assumptions. With proposed system newfound knowledge, the empowered intruder may find out where the detection nodes are and design a route around them to lessen the likelihood of being spotted.
- To combat the problem of armed intruders, we present a vehicle partnership sensing network approach in which mobile sensing devices and static sensor nodes work together to offer intrusion detection. In addition, a system for identifying intrusions is developed. With the goal of efficiently following the armed intruder, a decentralized target pursuit method using mobile sensing devices is proposed.
- We show through conceptual model and simulated tests that our solution outperforms conventional intrusion detection techniques while maintaining a manageable energy impact.

2. Existing Work

As was previously indicated, WSNs' intrusion detection issue may be treated as the penetration optimal control problem with the goal of maintaining continuous, high-quality coverage of the intruder. There has been a lot of research on how to best optimise the range of wireless sensor networks (WSNs), and the results may be broken down into three categories: area penetration, focus exposure, and obstacle exposure. Protective penetration investigates the likelihood of detecting an object entering the monitoring region, whereas target coverage demands the sensor network to watch and gather data from a set of predetermined targets. Intrusion detection in WSNs can use both objective protection and obstacle penetration strategies. Multiple intrusion detection techniques employing stationary sensor networks were presented [10].

A greedy approach is presented to strike a compromise between sensing quality and network lifespan after Sharmin et al. tackled the challenge of maximising both at the same time for covering diverse targets with sensing coverage. Liu et al. propose a Voronoi-based k-nearest neighbor node tracking technique. The approach doesn't quite expand well with increasing network size since it requires global knowledge during the startup phase in order to construct the Graph representation. The best structure of barrier coverage was created by Silvestri et al. for use in intrusion detection systems for buildings [11].

However, there would be a very high demand for the number of sensors required to construct a full barrier. Once deployed, sensors in stable sensor networks remain in the same places. Therefore, it is difficult for static sensor networks to guarantee intrusion detection performance since coverage breaches will occur when the network is sparse. It is possible to increase the effectiveness of intrusion detection by using the mobile nature of sensor nodes to fill up coverage gaps. Effective direction for a group of mobile sensors following a moving object with just distance data was investigated by Zhou and Roumeliotis. The suggested technique was shown to deliver the desired throughput with continuous time consumption in numerical simulations [12].

To simulate the actions of the invader and the mobile sensors, Keung et al. implemented the kinetic theory of gas molecules from physics. This finding demonstrated that mobile sensor networks are superior at providing k-coverage of the invader. To follow a moving target in an obstacle-filled environment, Mahboubi et al. presented a grid-based technique for mobile sensor networks [13]. The shortest path method is utilised to demonstrate the practicability of proposed system tactic.

The Nash equilibrium with a zero-sum game, the ideal mobility approach of the invader and mobile sensors was explored by Liu et al. It should be emphasised that in order for proposed system best approach to work, both players would need perfect foreknowledge of the other's whereabouts and actions, which is seldom the case in practise. The quality of intrusion detection achieved by mobile sensor networks is higher than that of static sensor networks. Nevertheless, due to the complexity introduced by mobile sensors in the sensor network's transportation and data dissemination, it is not well suited for widespread use. As a result, researchers are focusing on hybrid sensor networks, which combine static and portable sensors to maximise mobility while minimising deployment costs [14].

Lambrou constructed and analysed the dynamic coverage of a hybrid sensor network consisting of a sparsely distributed static sensor network and a collection of mobile sensor nodes. To accomplish multiple-target tracking using mobile and static sensors, Wang et al. presented a distributed action force-based movement technique. With proposed system strategy, we were able to ensure a high chance of successful tracking while also minimising the required amount of energy [15]. In order to enhance coverage in hybrid WSNs, Zhang and Fok focused on how to redeploy mobile sensor nodes. They presented an approach to improve hybrid wireless sensor networks' coverage in two stages.

Considering the unique requirements of boundary protection, Sun et al. designed a heterogeneous wireless sensor network framework. There will be less of a need for humans to keep an eye on the border, and the technology will be more accurate at detecting illegal activity. Path exposure has been used extensively in the literature to measure the efficacy of intrusion detection techniques because of its ability to quantify the constant surveillance of a target by WSNs [16]. To assess the worst-case coverage of the target, Meguerdichian et al. framed exposure as the integration of the perceptual intensity along the target trace and investigated the minimal path exposure problem. After discretizing it into a shortest path issue in a weighted graph, they developed a grid-based method. The least exposure path for a single sensor was solved in closed form by Veltri et al., who also devised a localised approximation approach.

Knowledge gained from studying the MEP problem led us to develop the motivated attacker paradigm and explore further intrusion detection strategies. The best way to spot and follow intruders is to plan ahead for their movements, which means taking mobile sensing devices into account. Although Liu et al. recommended an intrusion detection methodology for WSNs that relied on concurrent computational intelligence background subtraction and administered fuzzified grouping, the scheme's observation deployment was relatively stable, meaning that it failed to adequately represent the movement characteristic features of attackers and endpoints [17].

The best mobility technique of the adversary and the objective of proposed system study is studied in the pursuit-evasion problem, a classic subject in robotics. When both players' senses are limited, as they are in the classic Lion and Man issue, Bopardikar et al. When the evader employs a reactive strategy, they propose a sweep-pursuit-capture pursuer approach [15]. This sensing-limited scenario is analogous to the armed intruder detection challenge. We present an intrusion detection technique for armed intruders based on a vehicle cooperation sensing network and the pursuit-evasion issue.

This proposed method efficiently keeps tabs on the armed intruder with minimal performance degradation.

3. Proposed System

Here, we consider a situation in which a sensing network is set up in a rectangular girdle area (A) using a combination of fixed nodes (N) and wireless sensor devices (M). An unauthorised visitor (J) wants to leave area A by whatever means necessary. Intruders can be located and followed with the use of both stationary and mobile detection nodes. Mobile sensing devices can take use of their movement to swiftly track an invader after some stationary nodes have detected it. Initial SN and MSV release occur in a spatially-dispersed Poisson fashion. Numbers N as well as M in section A are represented by the notation, where N is the length of the set (L) and M is the length of the set (N). We proceed to develop the node perceptual model and the performance assessment criteria of the intrusion detection methods used in proposed system study. Node T_j 's perceived strength on threshold J is described as:

$$PS(T_j) = \frac{\beta}{[e(T_j, J)]^L}$$

Where $e(T_j, j)$defines Euclidean remoteness among the nodeT_j and the targeted node j. To clarify, is a positive constant, while L is a distance-dependent variable. L and β are parameters whose values are sensitive to the technical characteristics and sensitivity of the sensor module. The perceived strength decreases as the gap among the node and the destination grows wider. The stochastic sensor paradigm is used, where device $T_j$has a detection likelihood of:

$$d(T_j) = \begin{cases} 0, & while\ e(T_j, J) \geq S_0 \\ e^{-\vartheta b^{\alpha}}, & while\ S_1 < e(T_j, J) < S_0 \\ 1, & while\ (T_j, J) < S_1 \end{cases}$$

Where $b = e(T_j, J) - S_1$ and S_0,S_1 represents crucial detecting choices. In particular, whereas if range between the nodes is smaller than S_1, the destination will always be identified by some nodes, whereas if it is more than S_0, it will never be detected. Whenever the range is between S_0 and S_1, the detection probability is measured by the parameters α andϑ. In other words, different types of physical sensors have different technological requirements, which affects the values of α andϑ. The stochastic sensor paradigm more closely matches the characteristics of actual sensor nodes since it considers the impact of error and noise.

That is, there is no location anywhere along route where the invader may be spotted. As a result, the total likelihood of the intruder being undiscovered is the sum of the possibilities at each stage. This is useful for gauging the efficacy of intrusion detection systems, particularly in sensor networks with limited coverage. These following hypotheses are made about the movement and sensing capabilities of the empowered invader and the mobile sensing devices in order to develop their movement plan. The armed invader can travel at the maximum speed of VI in any direction, at any speed within the range. As a result of their enhanced capabilities, intruders may detect neighbouring static nodes and mobile sensing devices, as well as their distances and directions. These mobile sensing devices are capable of speeds up to their maximum and can go at any speed within their spectrum and in any orientation.

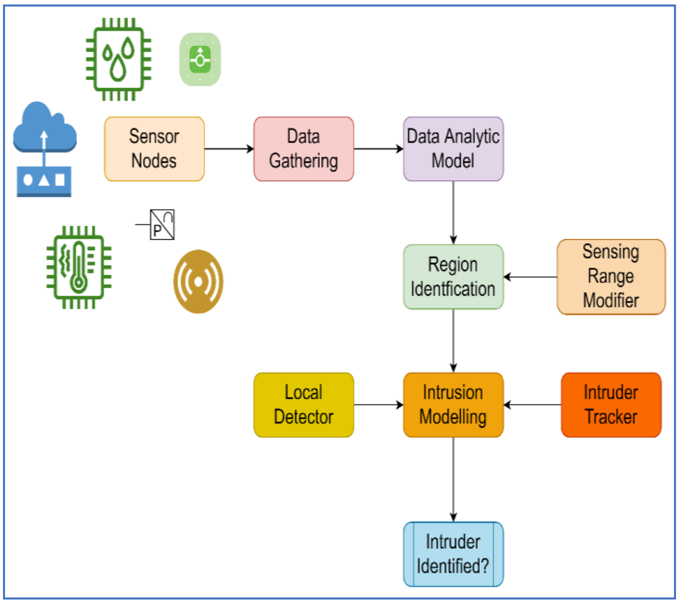

Fig. 2. Proposed System architecture

Devices equipped with sensing capabilities may also detect the invader and surrounding fixed nodes to determine their location and direction. In each observation zone, a mobile sensing vehicle serves as an edge computing node. Edge nodes are able to make scheduling decisions by combining data from stationary nodes and other moving devices. While the system is not performing intrusion detection activities, the deterministic nodes adhere to the sleep-scheduling strategy. Having established the problem and its definitions, we will now provide the concept of the motivated attacker. An armed intruder can use information about the positions of detection nodes to plot a course across the monitored region that will expose him or her to the fewest number of sensors.

Instead, a well-designed IDS should maximise proposed system route exposure to ensure thorough surveillance of the invader. It is proposed to use a grid-based approach to resolve the general MEP problem. In order to convert the MEP issue together into shortest path problem of the set of vertices, the algorithm builds a weighted graph in which the weight indicates the exposure level of associated path depending on the placement of sensors. Weighted graphs are built from data from all across the world. The intruder, in the context of intrusion detection, has to be aware of where detection nodes are deployed across the network in order to devise a route with the smallest possible impact on system resources. Since it is highly unlikely that an adversary, even one with access to all of the sensors, would have such comprehensive knowledge in a real-world scenario, the technique is useless for empowering adversarial path planning.

The following equations have no known analytic solution, and developing a numerical solution would place a heavy computational burden on the invader. Furthermore, the precision of the known values has a significant impact on the precision of the numerical solution. Inaccuracy stems from the localization process, which is prone to noise and human mistake. Therefore, we will use a heuristic movement plan with a minimal degree of complexity for the armed invader. An armed intruder learns about all nearby detection units within a certain range, acquiring data on their relative positions and directions. Afterward, it tries to abandon these ruts. Because the invader often moves away from the nearest neighbouring node in the first place, there is an inverse association between the magnitude of the action force and the distance between Tj and J.

As a result of adopting proposed system course of action, we might anticipate the subsequent outcomes: Initially, the attacker will flee the area of the node closest to it in order to avoid being correctly identified; second, if many nodes are present, proposed system will indicate the coverage breach as the area with the fewest or no surveillance clusters. That means the burglar is heading in the direction of the blind spot, where they won't be spotted. It's worth noting that proposed system action force has a far lower computing cost than the problem formulation does. This mobile sensing device is normally started up in patrol mode, assuming there is no intruder nearby. When an intruder is detected inside its range of sensors, it will transition to a more basic tracking mode, and when both intruders and stationary nodes are present, it will enter a local cooperation mode.

When there are no more intruders or static nodes in the area, it will revert to patrol mode to conserve energy. This mobile sensing device will remain inside the low-speed patrol condition if it does not detect any intruders within its sensing range. It will move in a consistent pattern in order to keep an eye on the exposed area, and its speed will be capped so as to save power. When it reaches the area's border, only then will it reverse the direction of its speed. As soon as it detects an intruder, it will transition to a different motion mode. The mobile sensing vehicle will switch to basic tracking mode if it detects an intruder inside its sensing range but no static nodes are present. So, the sensor management vehicle will use a basic yet effective technique to determine its next step. It will head in the direction from whence the invader was last seen. Whenever the mobile sensing device detects both an intruder and a static node within its sensing range, it will enter a state of local cooperation.

The empowered intruder's plan of action is to avoid detection nodes and go towards the coverage gap; therefore it makes sense to take use of the mobility of a mobile sensing vehicle to accomplish both goals. Two primary goals of mobile sensing devices are (1) closing the gap between themselves and an intruder, and (2) compensating for the gaps in coverage provided by stationary nodes. When operating in local collaboration mode, a mobile sensing device will attempt to repair the gap in coverage caused by stationary nodes by moving closer to the invader. In order to improve the efficiency of intrusion detection, mobile sensor devices collaborate with stationary ones.

In conclusion, based on the data it collects, the mobile sensing vehicle will determine its current mobility state and modify its speed accordingly. When building an intrusion detection strategy, it is important to consider the potential benefits of incorporating a sleep-scheduling mechanism to cut down on the network's overall energy consumption and increase its lifespan. In the event that an intruder is detected by an active static node, that node will send out an actually woke message to all other nodes in its vicinity.

4. Results and Discussion

Here, we do simulated studies to attest to proposed system's effectiveness against powerful invaders based on vehicle cooperation monitoring infrastructure and compare the findings to those of existing intrusion detection systems based on WSNs. In proposed system part, we will also examine the degree of sensitivity of certain important proposed system factors. The simulation runs on a 2.8GHz Intel(R) core(TM) i7-7700HQ computer. MATLAB is used for the implementation. The data represents a mean over a sample size of one hundred separate tests displays the placement of one hundred sensors and the paths taken by one hundred empowered intruder and mobile nodes.

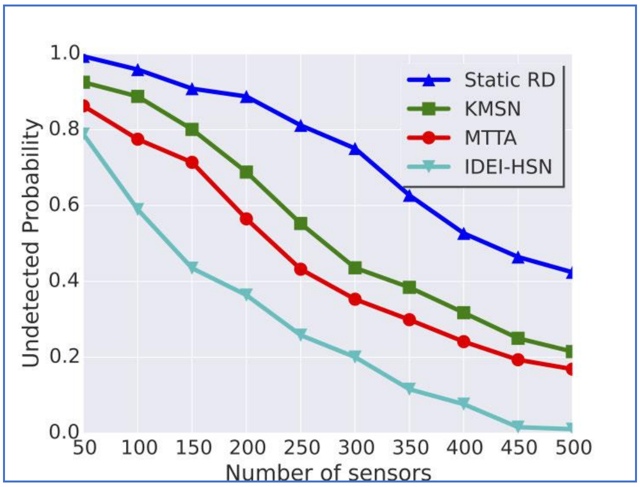

Fig. 3. Comparing risk intrusion detection.

The intruder's path is depicted by the red curves, and the path of mobile sensing devices is depicted by the green lines; the blue circle indicates the detecting range of static sensors. This scenario depicts the empowered intruder's journey over a static sensor network, demonstrating how the intruder may plot its course and remain unnoticed. The flexibility of sensors is exploited in proposed system way to increase coverage. However, high-quality monitoring cannot be done since the mobile sensor moves at a constant speed and lacks a commensurate strategy against the empowered intruder's behaviour. It uses a process in which stationary and moving sensors collaborate to form a comprehensive security network.

However, the intruder must be noticed by some stationary sensors for proposed system to work, which is highly unlikely given the invader's enhanced capabilities. Evidence like these demonstrates MTTA's ineffectiveness against the armed invader. However, in proposed system, the mobile sensing vehicle is able to successfully keep tabs on the empowered intruder thanks to the strategy of simple pursuit and local collaboration, which allows the vehicle to undertake continuous monitoring in situations when its trajectory coincides with that of the intruder's.

The graph depicts the route exposure of the four intrusion detection techniques as the network size increases from fifty to five hundred nodes. It's plain to observe that they're always at a lesser risk of being in harm's way on the walk. The reason for proposed system is that detectors in these two designs can't deal with the tactics of an armed invader. The route exposure intensity is higher than the previous two but lower than proposed system. Detection of the intruder's success by certain stationary sensors is crucial to the cooperative mechanism of proposed system, but these sensors are notoriously unreliable owing to the intruder's tactic of using their superior strength. The depictions of trajectories in the results of the channel analysis are consistent with those depictions. Not only that, but route exposure grows for all four systems as the number of nodes in the network increases.

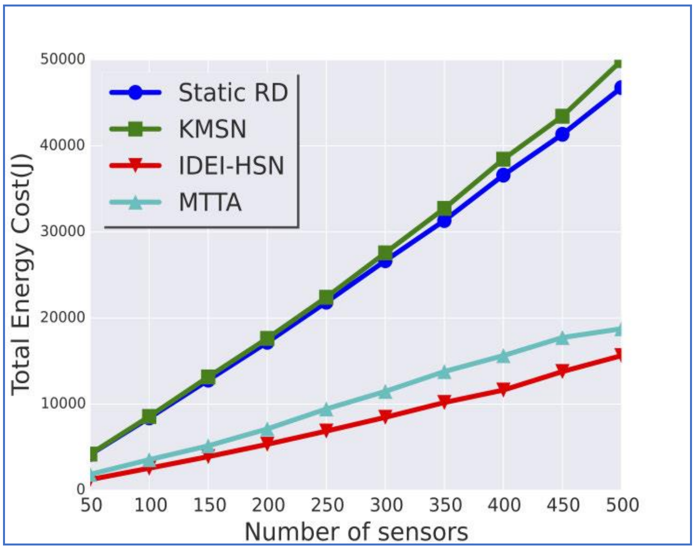

Fig. 4. Comparing energy consumed.

Notably, the proposed system path exposure rises dramatically, suggesting that the newly additional sensors are being put to good use in order to improve the intrusion detection service. However, intrusion detection effectiveness only marginally improves as the number of nodes increases. This illustrates how, as the total amount of nodes in the region increases from 40 to 700, the possibility that the empowered intruder will pass through the area unnoticed also increases. There is clear evidence that proposed system has the lowest likelihood, followed closely. However, there is a high likelihood that the powerful attacker can pass through the surveillance region undetected, pointing to subpar intrusion detection effectiveness.

Due to its empowered intruder's approach of evading detection nodes, it effectively maintains a safe distance from nodes. All four techniques have a lower likelihood the more nodes there are, therefore it stands to reason that a denser network will also have more detection possibilities. Thus, they can observe that their energy usage is comparable, with the exception that the former is far superior since they lack a sleep-scheduling system. In order to cut down on the network's overall power usage, they have an automated sleep scheduler. As a result, the cost of data transmission will increase since certain fixed nodes will serve as local control centres, broadcasting information about the invader. When it's necessary, proposed system's stationary nodes and moving sensing devices will send out wake-up signals to other nodes in the area, resulting in additional data transmission costs.

Overall, their energy efficiency is good, although only proposed system can reliably detect armed invaders. Power is limited on a portable sensing node; therefore, an efficient movement strategy will aim to reduce the total distance sensors are moved while yet providing enough protection against unwanted intruders. The uniformity with which KMsn's mobile nodes move causes superfluous relocation length to be calculated during detection. KMsn is not the best scheme for intrusion detection against armed attackers because to its low detection quality and excessive energy consumption. Keep take mind that in this mobile node travel shorter distances than in proposed system. In this mobile node really go in the direction of the goal in response to instructions from dedicated static nodes.

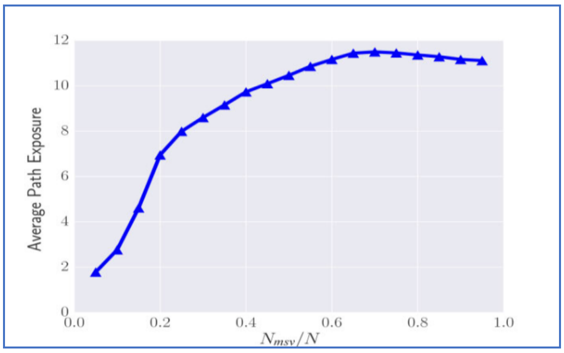

Fig. 5. Intruder movement analysis

But since L0's evasive tactic makes it difficult to spot the empowered invader, L0 is unlikely to broadcast such instructions, leaving MTTA with less room to manoeuvre. proposed system's markedly enhanced intrusion detection performance justifies the little increase in travel time. From what we can tell from the aforementioned simulated trials, is able to accomplish a respectable level of intrusion detection efficiency while using less energy and covering less ground overall. Comparing the intruder's sensing and movement capabilities to those of the detection nodes is a key factor in determining how well proposed system performs in the situation of intrusion detection for armed intruders. The efficiency of intrusion detection will also be affected by the number of mobile sensing devices deployed.

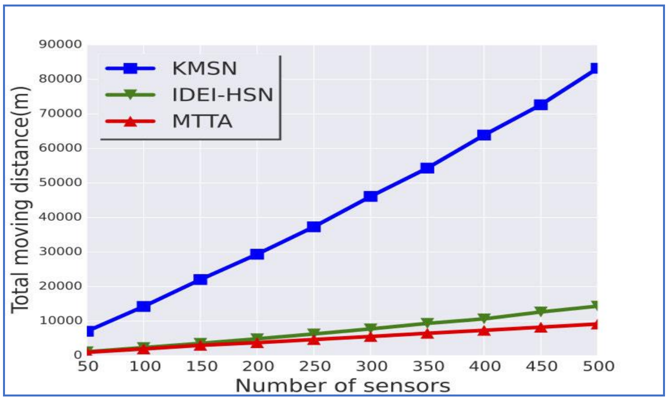

Fig. 6. Displacement analysis

Here, we'll use simulations to examine the effect that changing a few important factors has on proposed system's overall performance. The percentage of mobile sensing devices relative to total detection nodes is another crucial proposed system characteristic. Here, we examine the average route exposure under different conditions by holding the total number of nodes constant and changing only the percentage of mobile sensing devices. This demonstrates how expanding the quantity of mobile sensor devices may boost intrusion detection effectiveness. This demonstrates how the paths of nodes vary with the amount of this in use.

Increases in the number of mobile sensing devices may help increase chances of locating the intruder and closing coverage gaps, which may explain the observed shift. The path's exposure, however, stops growing when a particular threshold has been reached (1.49 for proposed system example). Actually, having too many mobile sensing devices implies having too few stationary nodes that will cause the local cooperation approach to fail. As a result, in real-world applications, the right mix of mobile sensing devices should be chosen with consideration for both the nature of the work at hand and the available budget.

5. Conclusion

The study begins by proposing the armed intruder paradigm. The unauthorized person has a lower chance of being discovered because he or she may more easily identify detection nodes in the area and flee from them. Targeting the difficulty provided by the attacker, we offer a decentralized intrusion detection approach relying on a sensor network formed through collaboration amongst vehicles. Elevated surveillance is achieved by using mobile sensing vehicles to follow the motivated attacker, and an energy-saving sleep-scheduling method is developed for stationary detectors. Additionally, in each monitoring region, a mobile sensing device serves as either an edge computing node, allowing us to meet the demands for low delay and high performance. The numerical simulations show that the suggested strategy improves upon the energy cost while also providing greater intrusion detection performance against armed attackers. The effect of key factors on the suggested system's efficiency is also shown through statistical method.

References

[1] Alippi, G. Anastasi, C. Galperti, F. Mancini, and M. Roveri, ‘‘Adaptive sampling for energy conservation in wireless sensor networks for snow monitoring applications,’’ in Proc. IEEE INTERNATONAL Conf. Mobile Adhoc Sensor Syst.,Oct.2007, pp.1-6.

[2] Falcon, X. Li, and A. Nayak, ‘‘Carrier-based focused coverage formation in wireless sensor and robot networks,’’ IEEE Trans. Autom. Control, vol. 56, no. 10, pp. 2406–2417, Oct. 2011.

[3] Heinzelman, A.Chandrakasan, and H. Balakrishnan,‘‘Energy-efficient Communication protocol for wireless microsensor networks,’’ in Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci., Aug. 2005, p. 10

[4] Kim and J. Ben-Othman, ‘‘A collision-free surveillance system using smart UAVs in multi domain IoT,’’ IEEE Commun. Lett., vol. 22, no. 12, pp. 2587–2590, Dec. 2018.

[5] Kumar, T. H. Lai, M. E. Posner, and P. Sinha, ‘‘Maximizing the lifetime of a barrier of wireless sensors,’’ IEEE Trans. Mobile Comput., vol. 9, no. 8, pp. 1161–1172, Aug. 2010.

[6] Lambrou, ‘‘Optimized cooperative dynamic coverage in mixed sensor networks,’’ ACM Trans. Sensor Netw., vol. 11, no. 3, pp. 1–35, Feb. 2015.

[7] Liu, W. Wei, H. Wang, Y. Zhang, Q. Zhang, and S. Li, ‘‘Intrusion detection based on parallel intelligent optimization feature extraction and distributed fuzzy clustering in WSNs,’’ IEEE Access, vol. 6, pp. 72201–72211, 2018.

[8] Meguerdichian, F. Koushanfar, and G. Qu, ‘‘Exposure in wireless adhoc sensor networks,’’ in Proc. 7th Annu. Int. Conf. Mobile Comput. Netw., 2001, pp. 139–150.

[9] Rajan, D. Antony Joseph, and E. R. Naganathan. "Long and Strong Security using Reputation and ECC for Cloud Assisted Wireless Sensor Networks." Scalable Computing: Practice and Experience 21.1 (2020): 85-92.

[10] Rajan, D. Antony Joseph, and E. R. Naganathan. "Trust Based Anonymous Intrusion Detection for Cloud Assisted WSN-IOT." Global Transitions Proceedings (2022).

[11] Rajan, D. Antony Joseph, and E. R. Naganathan. "Identity verification-based cryptography for detecting intrusion in wireless sensor networks." International Journal of Vehicle Information and Communication Systems 4.4 (2019): 375-387.

[12] Sun, P. Wang, M. C. Vuran, M. A. Al-Rodhaan, A. M. Al-Dhelaan, and I. F. Akyildiz, ‘‘BorderSense: Border patrol through advanced wireless sensor networks,’’ Ad Hoc Netw., vol. 9, no. 3, pp. 468–477, May 2011.

[13] Umamaheswari, S. "Hybrid optimization model for energy efficient cloud assisted wireless sensor network." Wireless Personal Communications 118.1 (2021): 873-885.

[14] Veltri, Q. Huang, G. Qu, and M. Potkonjak, ‘‘Minimal and maximal exposure path algorithms for wireless embedded sensor networks,’’ in Proc. 1st Int. Conf. Embedded Networked Sensor Syst., 2003, pp. 40–50.

[15] Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, ‘‘A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing,’’ IEEE Internet Things J., vol. 6, no. 3, pp. 4831–4843, Jun. 2019.

[16] Wang, Z. Peng, J. Liang, S. Wen, M. Z. A. Bhuiyan, Y. Cai, and J. Cao, ‘‘Following targets for mobile tracking in wireless sensor networks,’’ ACM Trans. Sensor Netw., vol. 12, no. 4, pp. 1–24, Sep. 2016.

[17] Weng, C.-Y. Chang, C.-Y. Hsiao, C.-T. Chang, and H. Chen, ‘‘On-supporting energy balanced k-barrier coverage in wireless sensor networks,’’ IEEE Access, vol. 6, pp. 13261–13274, 2018.