International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7189
***Article Received**: 23 April 2023 **Revised:** 12 June 2023 **Accepted:** 28 June 2023*

Intrusion Detection Mechanism for Empowered Intruders Using IDEI

J. Josephin Jinisha[1], Dr. S. Jerine[2]
[1]Research Scholar: Department of Computer Application Noorul Islam Centre for Higher Education
Tamil Nadu, India
jinishamelbin@gmail.com
[2]Associate Professor: Department of Software Engineering,
Noorul Islam Centre for Higher Education
Tamil Nadu, India
ssjerine@gmail.com

Abstract— In the past, intrusion detection has been extensively investigated as a means of ensuring the security of wireless sensor networks. Anti-recon technology has made it possible for an attacker to get knowledge about the detecting nodes and plot a route around them in order to evade detection. An "empowered intruder" is one who poses new threats to current intrusion detection technologies. Furthermore, the intended impact of detection may not be obtained in certain subareas owing to gaps in coverage caused by the initial deployment of detection nodes at random. A vehicle collaboration sensing network model is proposed to solve these difficulties, in which mobile sensing cars and static sensor nodes work together to identify intrusions by empowered intruders. An algorithm for mobile sensing vehicles, called Intrusion Detection Mechanism for Empowered Intruders(IDEI), and a sleep-scheduling technique for static nodes form the basis of our proposal. Sophisticated intruders will be tracked by mobile sensors, which will fill in the gaps in coverage, while static nodes follow a sleep schedule and will be woken when the intruder is discovered close. Our solution is compared to current techniques like Kinetic Theory Based Mobile Sensor Network (KMsn)and Mean Time to Attacks (MTTA) in terms of intrusion detection performance, energy usage, and sensor node movement distance. IDEI's parameter sensitivity is also examined via comprehensive simulations. It is clear from the theoretical analysis and simulation findings that our idea is more efficient and available.

Keywords- Empowered intruders, Intrusion detection, Wireless sensor networks.

I. INTRODUCTION

Because of their low cost and ease of deployment, multi-hop, Wireless Sensor Networks (WSNs) are formed from a large number of wireless sensor nodes via wireless communication. In real-world applications like as environmental perception, current logistics, and military reconnaissance and surveillance, several sensor nodes work together to detect and track specific targets. WSN-based intrusion detection systems may be utilizedto address a wide range of security concerns, including border patrol, region monitoring, and post-disaster relief. In order to offer consistent and high-quality coverage, it is necessary to follow and monitor the invader continuously. This might be referred to as a coverage optimization issue. There are two basiccategories of intrusion detection research. By merging data from several nodes via decision fusion or local voting, the accuracy of target localization and tracking may be improved. Focusing on sensor deployment and mobility strategy is an addition to basic coverage optimization challenges in this research project.

The quality of coverage is strongly influenced by the initial placement of the sensor nodes. As a result of wind and obstructions like trees and mountains, sensors are often spread out from an airplane, but the exact landing location cannot be controlled because of these factors. For example, most sensor deployments (such as border patrol or area monitoring) cannot be handled manually because of distant or hostile sensing conditions (e.g., A lack of adequate sensor coverage in some locations, even with a high number of sensors, or gaps in sensor coverage altogether are also possible (i.e., areas that are not covered by any sensor node).

Since embedded technology and micro robots [2] have recently improved, using some mobile sensors for intrusion detection is crucial to overcoming the problem outlined above. Unlike static sensors, mobile sensors may be relocated after deployment to ensure that they cover all of the necessary locations. Only by deploying these mobile nodes to improve network coverage canintruders be spotted and tracked. In the event that electronic anti-reconnaissance technology is created, an intruder might be equipped with sensors that receive the location information of detection nodes and execute route planning to avoid being spotted in

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7189
***Article Received**: 23 April 2023 **Revised:** 12 June 2023 **Accepted:** 28 June 2023*

real-world settings. We call such an invader an"empowered intruder" since it is able to circumvent sensor nodemonitoring and hence avoid detection. Invaders who are armedand well-equipped provide a significant challenge when it comes to developing an effective intrusion detection system.

A centralized architecture is used in border patrol and regional surveillance intrusion systems. The detection nodes will notify the base station or cluster node as soon as an intruder is identified, and they will subsequently take necessary action. More and more nodes will have to interact with the base stationor cluster node on a regular basis, which will use a growing amount of bandwidth and delay the transmission of crucial information like an intruder fleeing or a sabotage event. When dealing with powerful invaders, it is unsuitable for use in the actual world. The ability of mobile nodes to gather and evaluate intruder tracking trajectories in real time is a key component of a local computing system.

It is now possible to examine WSNs with the use of both mobile and fixed sensors. Unmanned armored vehicles' ability to moveand interpret information on the fly prompted us to design a vehicle cooperation sensing network that includes mobile sensing vehicles and stationary nodes. Additionally, our vehicle cooperation sensing network has included edge computing to satisfy the needs for low latency and high-quality service in intrusion detection. At the edge of a network, calculations can take place near to the source of the data, allowing for more accurate results. Mobile sensing vehicles are used as edge computing nodes in a region, as seen in Figure 1. A node at the edge of the network communicates with the detecting nodes when an intruder is found. Edge computing nodes may then tell all relevant mobile sensing vehicles to monitor and fill any gaps in coverage produced by an intruder's presence when they submit their tracking selections.

It is proposed in this study that mobile sensors and fixed sensors work together to detect incursions by intruders with access to weapons of mass destruction. In addition, in order to achieve a high detection rate with minimal energy consumption from detection nodes, this model tries real-time monitoring of observed intruders. We design a technique for the mobile sensing vehicles' mobility as well as a sleep scheduling approach for the stationary nodes because they must move about.

Here are some of the paper's contributions and innovations: For the first time, we can depict and mimic the movement ofinvading forces with more authority. Armed intruders mighthave a leg up on detection by planning their route and knowingwhere they're going.

An architecture that includes mobile and stationary sensors is proposed to recognize intrusions by attackers with more authority. The intrusion detection system IDEI is also in development. A distributed target pursuit method is employed to monitor the armed invader using mobile sensing vehicles. Additionally, static nodes can benefit from a sleep scheduling strategy that reduces power usage and increases network lifespan. Because of its low latency and high-quality service, a mobility sensing vehicle has been selected to serve as the edge computing node.

According to theoretical research and simulations, an enhanced intrusion detection performance may be reached with a reasonable level of energy consumption when compared to other conventional intrusion detection methods.

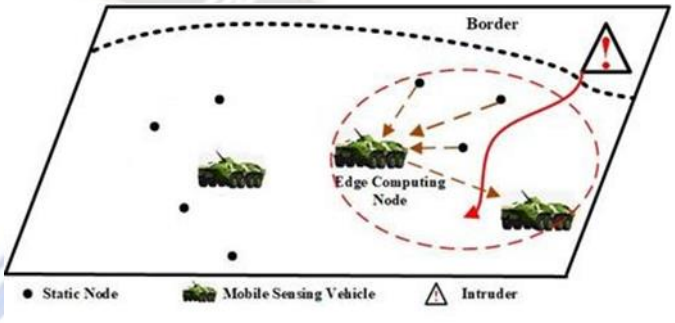


Figure 1: Design of an intrusion detection network based on vehicle cooperative sensing.

II. LITERATURE SURVEY

Coverage optimization may be used to the WSN intrusion detection issue to ensure that the invader is always covered. For WSNs, there are three types of coverage optimization: regionalcoverage, target coverage, and barrier coverage. For target coverage, sensors are required to monitor and gather data from a certain set of targets, while barrier coverage investigates the likelihood that an item will be identified when it crosses the monitoring region. Intrusion detection in WSNs may use both target coverage and barrier coverage. WSN intrusion detection research may be further classified into the following three groups based on the mobility of sensor nodes.

A. Static Sensor Network

Static sensor networks have been presented as a means of detecting intrusions. It was suggested by Sharmin et al. [3] to balance sensing quality and network lifespan for diverse targetsby using a greedy approach to maximise the sensing coverage quality. Liu et al. [4] propose a k-next-neighbor node tracking technique based on Voronoi diagrams. Although the approach requires global information to initialise, the Voronoi diagram does not scale effectively as

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7189
***Article Received**: 23 April 2023 **Revised:** 12 June 2023 **Accepted:** 28 June 2023*

the network increases in size. ' For building intrusion detection systems, Silvestri et al. developed an optimum barrier structure [5]. There are, however, a huge number of sensors required for a full barrier.

After initial deployment, the positions of sensors in static sensor networks are predetermined. When the network is sparse, therewill be gaps in coverage, making it difficult for static sensor networks to detect intrusions.

B. Mobile Sensor Network

The mobility of sensor nodes may be used to fill up the gaps in coverage and improve intrusion detection performance, however, this is not always feasible. Following a moving object based solely on distance data may be difficult, according to Zhou and Roumeliotis [6]. Simulations showed that the proposed strategy worked effectively and had a linear time complexity. Mobile sensor networks outperformed fixed sensor networks in detecting the intruder. A grid-based method proposed by Mahboubi et al. [7] allows mobile sensor networksto follow a moving item in an obstacle environment. Using the shortest path methodology, we can see that this method works.

[1] It's possible that invaders and mobile sensors may operate in a "zero-sum game," according to Liu and his colleagues. Unlessboth players have complete knowledge of their rivals' positions and movements, this optimum strategy is not applicable in real-world situations.

C. Hybrid Sensor Network

Mobile sensor networks beat static sensor networks when it comes to detecting intruders. Sensor networks that use mobile sensors, on the other hand, are more expensive and difficult to deploy, making them unsuitable for general use.In order to take use of sensors' mobility while keeping deployment costs in mind, researchers are now focusing on hybrid sensor networks that include both stationary and mobile sensors.

At Lambrou[8], dynamic coverage was examined by combining a sparingly installed static and a slew of mobile sensor nodes. Dispersed action force-based movement method utilizes mobileand stationary sensors. The approach ensured a high rate of tracking success while using little energy. Zhang and Fok [2] investigated how mobile sensor nodes may be redeployed in hybrid WSNs to increase network coverage. Their technique for improving the coverage of hybrid wireless sensor networks involves two phases. Sun et al. [9] proposed a hybrid wireless sensor network architecture for border patrol systems in light ofthe peculiarity of border patrol.The method has the potential to minimise the amount of time and effort required by border patrols while increasing their detection accuracy.

Numerous studies have evaluated the effectiveness of intrusion detection systems by measuring WSNs' continual monitoring of the target using the path exposure [10].An exposure issue was addressed to determine the worst-case target coverage by Meguerdichian and colleagues [10] who defined exposure as a perceptual intensity along the target track. With the use of weighted graphs, they came up with an efficient grid-based method for solving the issue. Single sensor MEP issue was solved by Veltri et al. [11] and an approximation approach was devised to determine the shortest exposure route. As a result of our research into the MEP issue, we were able to develop the empowered intruder model and explore further intrusion detection options. The mobility strategy of mobile sensing vehicles must be taken into account while attempting to identifyand track intruders. While Liu et al. [12] proposed a distributed fuzzy clustering technique for intrusion detection, they found the experiment deployment to be relatively slow. As a result, neither the invaders nor the nodes' movements could be fully characterised.In robotics, the pursuit-evasion problem has beena long-standing one, focusing on the best approach for the pursuer and evader. The classic Lion and Man dilemma was explored by Bopardikar et al. [13] in which the perceptive capacities of both individuals were restricted.In this case, the pursuer employs a sweep-pursuit-capture approach to apprehend the fleeing criminals. The intrusion detection challenge with empowered attackers is similar to this confined sensing condition. The use of vehicle cooperation sensing networks as an intrusion detection approach for invaders with increased authority is suggested. According to the recommended strategy, the intruder may be efficiently watched with a reasonably low energy consumption.

D. Detection of intrusions by Empowered intruders

We've developed a way for identifying more powerful intrudersusing vehicle cooperative sensing networks. Mobile sensing vehicles' motion is used to synchronise the sleep periods of static nodes in the proposed technique.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7189
***Article Received**: 23 April 2023 **Revised:** 12 June 2023 **Accepted:** 28 June 2023*

E. Movement Strategy

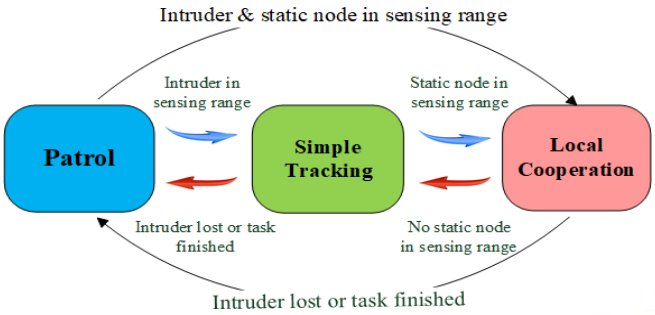


Figure2:Mobile sensing vehicle-state transition diagram

There are three modes of operation for mobile sensing vehicles: patrol, simple tracking, and local collaboration. Mobile sensingvehicles are often set up in patrol mode with no intruders present when they first arrive on the scene. Local cooperation mode is activated when it detects both intruders and static nodes, and basic tracking mode is activated when it detects just invaders. Patrol mode is automatically switched back to when there aren't any potential threats in the area, such as intruders orstatic nodes. Fig.2 shows the full status chart.

1) Patrol

During low-speed patrol, the mobile sensing vehicle does notdetect any intruders inside its field of vision. Monitor the exposed area in a consistent manner and restrict its speed to save energy. The only time it will change course is when it reaches the end of the area. When it detects an intruder, it will transitionto a different motion state.

2) Easy tracking

While there are no static nodes in its sensing area, a mobile sensing vehicle will go into tracking mode if it detects an intruder. If the mobile sensing vehicle follows this basic but successful technique, it will proceed toward the location wherethe invader was last detected.

At time t, assume that the intruder has the same maximum speed as the mobile sensing vehicle. Both the pursuer and evader (the invader) may be found at Pt and Et. The mobile sensing vehicle will follow a basic tracking technique as it moves along Pt and Et. Et+1 is the intruder's position at the moment of Pt+1, whereas Pt+1 is the pursuer's. When the evader moves along a vector from Pt to Et, the distance between them does not change. This is indicated by the formula: When the evader moves along a vector from Pt to Et, their distance does not change. An intrusion must avoid static nodes along its route in order to modify its velocity over time, which reduces the distance between the invader and the mobile detecting vehicle. It is clear from the foregoing explanation that a basic tracking method may be useful.

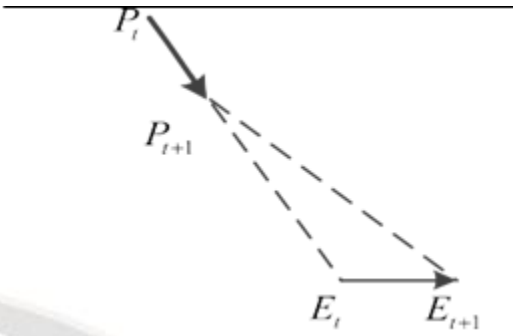


Figure 3: Tracking vector

3. Localization

An intruder and static nodes will be detected by the mobile sensing vehicle, and it will convert to a local cooperative state. A mobile sensing vehicle may be used to accomplish both of these goals because of the intruder's tactic of evading detecting nodes and moving toward the coverage hole. Firstly, a mobile sensing vehicle must minimise the distance between the intruder and itself; and secondly, it must try to fill in thecoverage hole of a static node network. To compensate for the static nodes' lack of coverage, the mobility sensing vehicle willtry to get closer to the intruder. Intrusion detection is improved when mobile and stationary sensors work together. As a result, the mobile sensing vehicle will modify its speed based on the information it receives. State 2 and State 3 of a mobile sensing vehicle should be able to follow the intruder at a pretty high pace, maybe even at its maximum speed (if required).

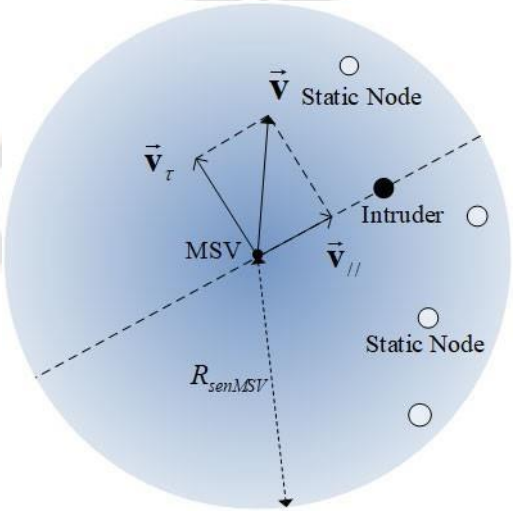


Figure 4: Localization strategy

Sleep Scheduling mechanisms

1. Collect information of current available energy E1;

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7189
***Article Received**: 23 April 2023 **Revised:** 12 June 2023 **Accepted:** 28 June 2023*

2. Broadcast E1 and collect the energy ranks of its currentlyawake neighbors N1.

Let R1 be the set of these ranks.

3. Broadcast R1 and receive Rv from each Tv ∈ N1

4. If |N1| < k or |Nv| < k for any sv ∈ Nv, remain awake. Return.

5. Compute E1 = {sv|sv ∈ N1 and E-rank v > E-rank u};

6. Go to sleep if both the following conditions hold. Remain awake otherwise.
   - Any two nodes in E1 are connected either directly themselves or indirectly through nodes which is in the su's 2-hop neighborhood that have E – rank v larger than E – rank u;
   - Any node in N1 has at least k neighbors from E1.

7. Return.

Sleep scheduling should be addressed in the design of an intrusion detection system to save energy and extend the network's lifespan. According to this study, the IDEI static nodes schedule their sleep as follows:

Whenever a mobile sensing vehicle detects a static node or an intruder, it will send out a wake-up signal to all nodes within its range of communication. All nodes in its communication range will get a wake-up signal if an active node detects an intruder and other static nodes. If an intruder or other static nodes are detected within the communication range of a sleeping static node, the node will send out a wake-up signal to all nodes within that range.If the node detects no intruders, it will return to the previous sleep-scheduling algorithm and proceed to step 1.

There is no sleep schedule for the mobile sensors in IDEI, so they are continuously alert to identify and track intruders.

Additionally, IDEI is possible to reduce network energy usage and extend the network's lifespan by using the sleep-schedulingmethod described in this article.

PERFORMANCE EVALUATION

Below is the mathematical expression used for evaluating the performance of the proposed method.

i) Perceptual Intensity

$$Int\,(S_i) = \frac{\alpha}{[d\,(S_i, I)]^K}$$

Distance between the node Si and its target I is d (Si, I) = d (Si/I)
+ K = d (Si/I). A sensor module's sensitivity and other technological characteristics influence the values of and K. Perceptual intensity decreases with increasing separation between the node and the target.

ii) Perceptual Probability

$$c(S_i) = \begin{cases} 0, & if\ d\,(S_i, I) \geq R_0 \\ e^{-\lambda a^{\beta}}, & if\ R_1 < d\,(S_i, I) < R_0 \\ 1, & if\ d\,(S_i, I) < R_1 \end{cases}$$

iii) The likelihood that the intruder will go undetected when theycross the border

$$\mathrm{Prob}_{\mathrm{neg}}\,(P) = \prod_{u_i \in P} \mathrm{Prob}_{\mathrm{neg}}\,(u_i)$$

iv) Path Exposure

$$\mathrm{E}\,(p\,(t)\,, t_1, t_2) = \int_{t_1}^{t_2} I\,(F, p\,(t)) \left|\frac{dp\,(t)}{dt}\right| dt$$

III. RESULT AND DISCUSSION

IDEI is compared to current WSN-based intrusion detection algorithms when it comes to detecting empowered invaders. Additionally, a few crucial IDEI parameters will be examined for their sensitivity in this section.

The simulation is done on a computer with an Intel(R) Core(TM) i7-7700HQ processor (2.8GHz). Tab.1 usually contains the most important parameter settings, unless noted differently. The average of 100 tests yields this result. According to the instructions, the required parameters are set asfollows:

Table 1: Simulation Parameters

Notation	Description	Value
L	Length of monitoring area	1200m
W	Width of monitoring area	300m
N	Total number of nodes	100
N_{ms}	Number of moving sensing vehicles	20
α	Constant of perceptual intensity	1
K	Distance parameter of perceptual intensity	4
β	Parameter of perceptual probability	0.5
λ	Parameter of perceptual probability	0.5
k_r	Constant of virtual force from node to intruder	1
γ	Distance parameter of virtual force from node to intruder	1
k_t	Constant of vertical moving vector of Intruder	0.2
ω	Distance parameter of vertical moving vector of Intruder	0.5
R_0, R_1	Critical sensing range of nodes (involved mobile vehicles and static ones)	10m, 2m
V_{msv_low}	Velocity of moving sensing vehicles in phase 1	4m/s
V_{msv_high}	Velocity of moving sensing vehicles in phase 2 & 3	10m/s
R_{sent}	Sensing range of empowered intruder	10m
V_I	Velocity of intruder	10m/s
k_{sen}	Constant of energy consumption in sensing task	150 mJ/sample
k_{recv}	Constant of energy consumption in receiving task	50 nJ/bit
k_{trans}	Constant of energy consumption in transmitting task	100pJ/bit/m^2

Figure 5: Intrusion detection trajectories

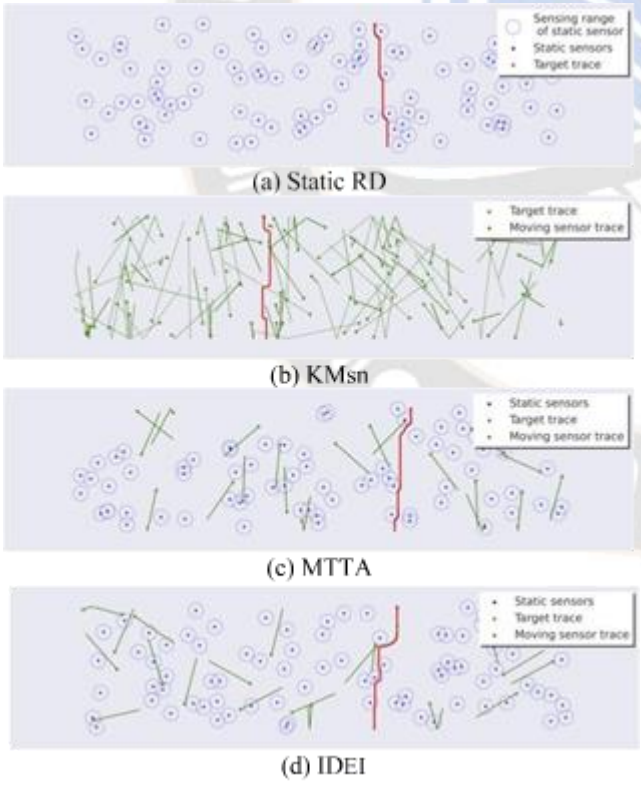
International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7189
***Article Received**: 23 April 2023 **Revised:** 12 June 2023 **Accepted:** 28 June 2023*

A. Proposed vs Existing method

Randomly deployed static sensor networks, kinetic theory-based mobile sensor networks, and mobile sensor networks based on MTTA will be compared to IDEI's static RD (target tracking with wireless sensor networks).All four methods will

range is shown by the blue circle. This enlightened invader is able to plan their route and avoid detection by the static sensor network, as seen in Fig. 5-(a). KMsn is able to cover a bigger area in Fig. 5-(b) because to the sensor mobility. Due to its fixed pace and lack of strategy for dealing with the empowered intruder's behaviour, the mobile sensor in KMsn cannot providehigh-quality monitoring.It uses a combination of static and mobile sensors to build an intrusion detection system. Static sensors are required for the MTTA to work,

which is unlikely to happen if the invader has been enabled. Asseen in Fig. 5-(c), MTTA is unable to deal with an armed intruder. A mobile sensing vehicle in IDEI may effectively monitor a powerful invader using the concept of simple pursuit and local collaboration, as shown in Figure 5-(d), where the trajectory of a mobile sensing vehicle overlaps with the intruder's route to conduct continuous monitoring.



(a) Static RD

(b) KMsn

(c) MTTA

(d) IDEI

B. Exposure of the path

Each of the four intrusion detection techniques has a different route exposure as the node count climbs from 50 to 500. The route exposure for Static RD and KMsn is reduced in all circumstances, as can be observed. Because sensors in these two methods are unable to oppose the intruder's technique, this is the main reason. MTTA's route exposure intensity is higher thanthat of IDEI, but lower than that of the previous two. Due to the tactics of the empowered invader, the collaboration mechanism of MTTA depends on static sensors that frequently fail toidentify success.

Fig.6's depiction of trajectories is consistent with the route exposure findings. With increasing node count, all four approaches have more route exposure. IDEI's route exposure rises dramatically, which implies that the newly installed sensors are successfully exploited to offer improved intrusion detection service by adopting the pursue and collaborationmethod. With Static RD and KMsn, increasing the number of nodes has little effect on intrusion detection performance.

C. When crossing the area, how likely is it that you will be spotted?

It is shown in Figure 7 that the likelihood of the empowered intruder remaining undiscovered while traversing the region rises from 50 to 500 nodes for each of the four approaches. Following IDEI is the least likely MTTA in terms of probability. On the other side, low intrusion detection performance in Static RD and KMsn shows that an attacker can pass through the monitoring zone unnoticed. Static RD, KMsn, and MTTA are only a few of the techniques the invader employs to avoid being detected and hence remain undetected. The probability of all four techniques of detection decreases as the number of nodes increases, which is consistent with real-worldpractise.

D. Cost of intrusion detection tasks

Energy usage in intrusion detection tasks is shown in Fig. 8. Basic functions like as sending and acquiring data use energy from the node. Static RD and KMsn, which do not include a sleep-scheduling system, require nearly the same amount of energy as MTTA and IDEI.Network energy consumption may be reduced by using sleep scheduling mechanisms in both the MTTA and IDEI networks. Local control centres will be established in MTTA, which will result in additional energy costs for sending information on the invader. In IDEI, wake-up signals are sent to neighbouring nodes by both stationary nodes and mobile sensing vehicles, resulting in an increase in data transmission energy consumption. MTTA and IDEI are both energy efficient, however only IDEI is capable of detecting intruders who have been armed.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7189
***Article Received**: 23 April 2023 **Revised:** 12 June 2023 **Accepted:** 28 June 2023*

E. Positioning distance between mobile sensors.

A mobile sensing node's best movement strategy would be one that minimizes sensor displacement distance while maintaining required intrusion detection performance. It is shown in Fig. 9 that the total distance travelled by mobile nodes in the three networks is shown.

When the number of nodes increases from 50 to 500, (mobile sensing vehicles). MTTA and IDEI's total movement distances are much less than KMsn's. As mobile nodes in KMSn always move in the same direction, this means that the detection process is slowed down by needless distance. KMSn is not the best method for detecting powerful attackers since it has low intrusion detection quality and a large energy usage.

The above-mentioned simulated studies demonstrate that IDEI is capable of detecting intrusions while using less power and covering a shorter travel distance.

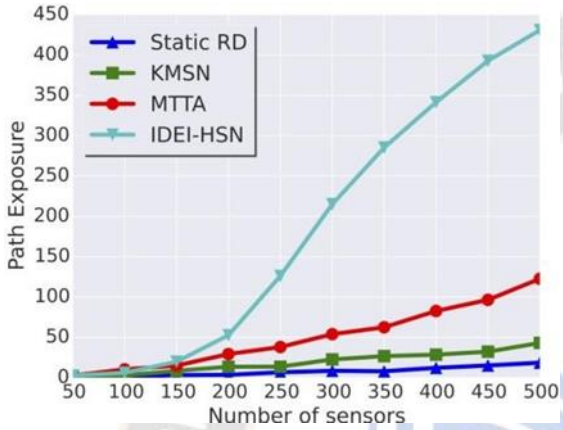


Figure 6: Path Exposure

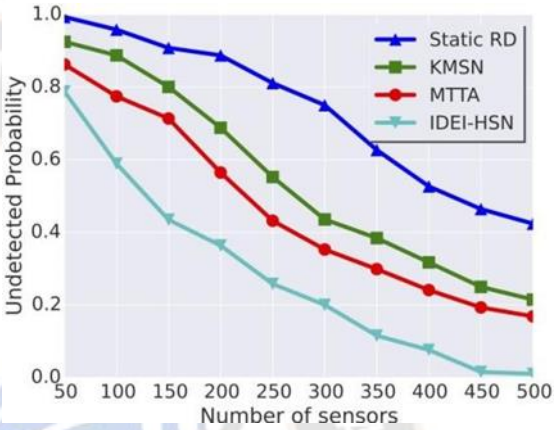


Figure 7: Remaining Un-detection probability

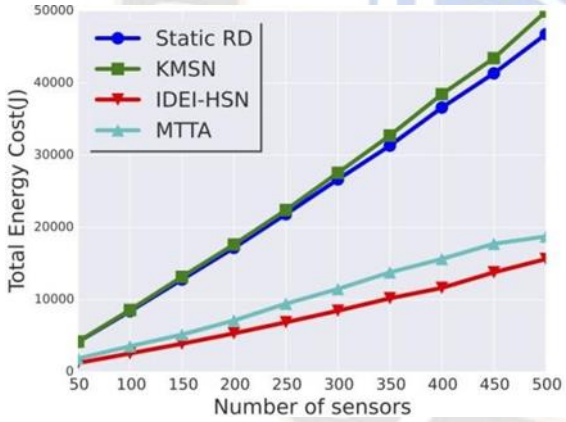


Figure 8: Energy Consumption

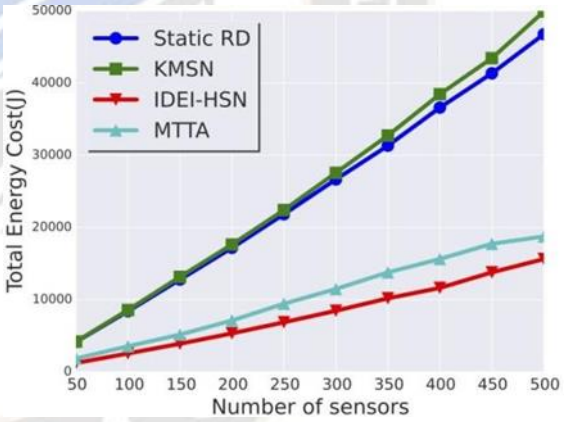


Figure 9: Displacement Distance

IV. CONCLUSION

In this paper, a model of a powerful invader is first offered. The empowered intruder has the ability to locate and avoid detection nodes in order to minimise detection risk. The threat posed by the empowered intruder is addressed with a distributed intrusion detection system (IDEI) based on vehicle cooperative sensing network. Using mobile sensing vehicles to follow the empowered intruder and a sleep-scheduling approach created monitoring is achieved. Using a mobile sensing vehicle as an edge computer node, each monitoring region is able to provide low latency and high-quality service. According to simulation findings, suggested approaches provide superior intrusion detection effectiveness against empowered intruders and a lower energy cost than other systems already in use. In addition, IDEI's performance may be evaluated using sensitivity analysis.

REFERENCES

[1] B. Liu, O. Dousse, P. Nain, and D. Towsley, ‘‘Dynamic coverage of mobile sensor networks,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 2, pp.301–311, Feb. 2021.

[2] Q. Zhang and M. Fok, ‘‘A two-phase coverage- enhancing algorithm for hybrid wireless sensor networks,’’ Sensors, vol. 17, no. 12, p. 117, Jan. 2017.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7189
***Article Received**: 23 April 2023 **Revised:** 12 June 2023 **Accepted:** 28 June 2023*

[3] S. Sharmin, F. N. Nur, M. A. Razzaque, M. M. Rahman, A. Almogren, and M. M. Hassan, ''Tradeoff between sensing quality and network lifetime for heterogeneous target coverage using directional sensor nodes,'' IEEE Access, vol. 5, pp. 15490–15504, 2017.

[4] Y. Liu, J.-S. Fu, and Z. Zhang, ''K-nearest neighbors tracking in wireless sensor networks with coverage holes,'' Pers. Ubiquitous Comput., vol. 20, no. 3, pp. 431–446, Jun. 2019.

[5] Tripathi, A. ., Pandey, R. ., & Singh, A. . (2023). Comparison of Performance of Boneh-Shaw Finger Printing Codes with Tardos Under Randomized Bits Collusion Attacks . International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 01–10. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2501

[6] S. Silvestri and K. Goss, ''MobiBar: An autonomous deployment algo- rithm for barrier coverage with mobile sensors,'' Ad Hoc Netw., vol.54, pp. 111–129, Jan. 2020.

[7] K. Zhou and S. Roumeliotis, ''Optimal motion strategies for range-only constrained multisensor target tracking,'' IEEE Trans. Robot., vol. 24, no. 5,pp. 1168–1185, Oct. 2021.

[8] Joseph Miller, Peter Thomas, Maria Hernandez, Juan González, Carlos Rodríguez. Exploring Ensemble Learning in Decision Science Applications. Kuwait Journal of Machine Learning, 2(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/206

[9] H. Mahboubi, W. Masoudimansour, A. G. Aghdam, and K. Sayrafian-Pour, ''An energy-efficient target- tracking strategy for mobile sensor networks,'' IEEE Trans. Cybern., vol. 47, no. 2, pp. 511–523, Feb. 2020.

[10] T. P. Lambrou, ''Optimized cooperative dynamic coverage in mixed sensor networks,'' ACM Trans. Sensor Netw., vol. 11, no. 3, pp. 1–35, Feb. 2021.

[11] Z. 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 2019.

[12] S. Meguerdichian, F. Koushanfar, and G. Qu, ''Exposure in wireless ad- hoc sensor networks,'' in Proc. 7th Annu. Int. Conf. Mobile Comput. Netw., 2020, pp. 139–150.

[13] 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., 2021, pp. 40–50.

[14] Z. Liu, W. Wei, H. Wang, Y. Zhang, Q. Zhang, and S. Li, ''Intru- sion detection based on parallel intelligent optimization feature extrac- tion and distributed fuzzy clustering in WSNs,'' IEEE Access, vol. 6, pp. 72201–72211, 2018.

[15] S. D. Bopardikar, F. Bullo, and J. P. Hespanha, ''Sensing limitations in the Lion and Man problem,'' in Proc. Amer. Control Conf., Jul. 2019,pp. 5958–5963.