A Sturdy Intrusion Detection Method for Well-Armed Attackers in Wireless Sensor Networks

BAMULI SWAPNA[1], A. ASHOK[2]

[1, 2]*Assistant professor, Vaagdevi Degree & PG College (Autonomous), Hanamkonda, Telangana.*

Abstract— ***Intrusion detection is one of the most important methods for ensuring the security of wireless sensing networks, and it has received enough attention in recent study. But with the development of electronic anti-reconnaissance gear, an intruder could be able to pinpoint the exact locations of detection nodes and then utilize system data to create a path that will allow them to avoid detection. An attacker with this kind of power is considered a threat since they provide new challenges to intrusion detection systems that are currently in use. Coverage gaps may emerge in specific locations when detection nodes are initially put at random, making it impossible to achieve the desired detection impact. We provide a notion for a sensing network where cars cooperate to provide intrusion detection against armed attackers in order to counter these issues.***

Index Terms- Sensing, Wireless Sensor Networks, Intrusion Detection, Energy Management.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are cost-effective and easy to install. They are built from a large number of wireless sensor nodes with wireless communication. Their use is expanding to a variety of real-world situations, including environmental sensing, modern logistics, and military surveillance. In all these situations, the coordinated efforts of multiple sensor nodes are required to monitor the surroundings and identify potential threats. An area of focus is the development of intrusion detection systems that can be used in a variety of situations, including border security, community monitoring, and post-disaster rescue. This can be seen as an intrusion optimization method to achieve continuous and high coverage of intruders, which requires continuous tracking and monitoring methods. Current research on intrusion detection is of two kinds. The first one uses sensory information from a large number of nodes based on decision fusion or local voting approaches to perform more accurate localization and tracking prediction of targets. The second one can be considered as an extension of the classical coverage optimization problem and is the focus of the proposed system research. It studies the deployment and movement strategies of sensor nodes to improve the dynamic coverage of targets. The initial placement of sensor nodes has a significant impact on the quality of coverage. Sensor deployment is usually not done manually due to the remote and inhospitable nature of the sensor locations. Therefore, it is common for sensors to fall out of aircraft, while the exact landing location is unpredictable due to factors such as wind and natural obstacles such as trees and mountains. Thus, placing sensors in one location may not improve coverage in other locations, and certain areas may experience "interference issues" or problems where no sensor nodes are present. Recent developments in embedded technology and miniature robotics may enable such mobile sensors to be used for intrusion detection, thereby providing a solution to the above problems. While static sensors remain in one location, mobile sensors can be relocated to ensure adequate coverage.

Unfortunately, such participating devices cannot identify and monitor attackers, other than improving coverage. As the science of counter-reconnaissance advances technologically, in real-world applications, attackers can be equipped with sensing devices that can learn the locations of monitoring nodes and plot a course around them. A "motivated attacker" is a strategy in which mobile sensing devices are deployed in specific areas as edge computing components, as shown in Figure 1. The edge computing nodes are notified by the sensing nodes when an intrusion is detected. Once a tracking option is exposed, the edge computing nodes notify their corresponding mobile sensor devices, allowing the mobile sensor devices to follow the instructions to locate the intruder and fill the gaps in coverage. In the proposed system work, we propose a sensor network model in which mobile sensor devices and fixed sensor nodes cooperate to provide intrusion detection against armed attackers. The goal of this model is to maximize coverage while minimizing the energy consumption of the detection nodes and simultaneously record and process the movements of all intruders as they are discovered. As a result, we develop movement plans for mobile sensor devices and downtime plans for fixed nodes. The following key research contributions are described in the proposed system work:

Unlike a "simple intruder", an armed intruder can avoid detection by avoiding tracking by sensor nodes. Therefore, it is a challenging task for an attacker with access to resources to develop an efficient intrusion detection strategy. Centralized intrusion detection techniques have traditionally been used for border patrol and area surveillance. Once an intrusion is detected, the information is forwarded to an access point or cluster component, where the data is analyzed and processed before appropriate action is taken. This process not only consumes a large amount of network bandwidth, but also requires continuous communication between the detection node and the base station or cluster nodes, which increases the network transmission latency and delays emergency response in case of intruder escape or intrusion sabotage. This means that standard centralized designs are not sufficient in the real world, especially when dealing with armed adversaries. Regular mobile nodes do not have the capability to record and interpret the trajectory of a monitored intruder in real time, which is necessary for local data processing.

II. EXISTING WORK

As previously mentioned, the issue of intrusion detection in wireless sensor networks (WSNs) can be addressed as an optimal control problem, with the aim of ensuring continuous and high-quality monitoring of intruders. Extensive research has been conducted on optimizing the range of WSNs, which can be categorized into three areas: area penetration, target exposure, and obstacle exposure. Area penetration focuses on detecting objects entering the monitored region, while target coverage requires the sensor network to observe and collect data from specific targets. Intrusion detection in WSNs can employ both target protection and obstacle penetration strategies. Several

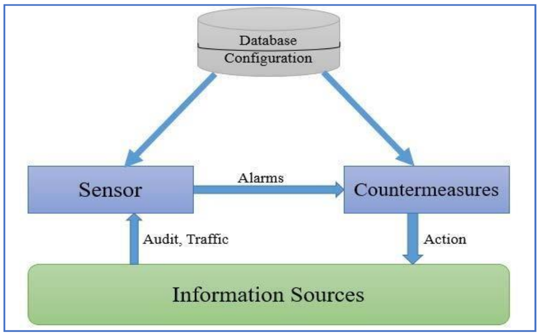

Fig. 1. Overview of Intrusion detection System

Techniques using stationary sensor networks for intrusion detection have also been proposed.

Following Sharmin et al., a greedy approach is presented to achieve a trade-off between sensor quality and network lifetime. took on the challenge of maximizing both simultaneously to cover a range of targets with sensor coverage. Liu et al. propose a Voronoi-based k-nearest neighbor tracking method. This approach does not scale well as the network size increases because it requires global knowledge in the start-up phase to build the graph representation. The best barrier covering structure was reported by Silvestri et al., which was developed for use in a building intrusion detection system.

However, a very large number of sensors are required to build a complete barrier. Once deployed, sensors remain at the same location in a stable sensor network. Therefore, it is difficult to ensure intrusion detection performance in a static sensor network, as a sparse network would result in coverage violations. The mobility of sensor nodes can be exploited to fill coverage gaps and increase the effectiveness of intrusion detection. Effective orientation determination for a group of mobile sensors tracking moving objects using only range data was studied by Zhou and Roumeliotis. The proposed technique provided a desirable throughput in numerical simulations at a continuous time scale.

To simulate the behavior of an intruder and a mobile sensor, Keung et al. used the theory of motion of gas molecules from physics. The results showed that mobile sensor networks are superior in intruder coverage. To track moving targets in an obstacle-cluttered environment, Mahboubi et al.proposed a grid-based technique for mobile sensor, networks. The shortest path method is used to demonstrate the, practicality of the proposed system tactics.,

A zero-sum game, ideal intruder movement approach, Nash equilibrium with mobile sensors was proposed by,Liu et al., and investigated. It should be emphasized that for the proposed system approach to work, both actors require accurate knowledge of each other's location and behavior, which is rarely the case in practice. The quality of intrusion detection via mobile sensor networks is higher than that of static sensor networks. However, mobile sensors introduce complexities in sensor network transmission and data distribution, making them less suitable for widespread deployment. Therefore, researchers focus on hybrid sensor networks that combine static and wearable sensors to maximize mobility while minimizing deployment costs.

Lambrou built and analyzed the dynamic insurance of a hybrid sensor community including a moderately allotted static sensor community and a group of cell sensor nodes. To accomplish multiple-goal monitoring the use of cell and static sensors, Wang et al. supplied a allotted motion force-primarily based totally motion technique.

Proposed device strategy, we have been capable of make certain a excessive threat of a success monitoring even as additionally minimizing the desired quantity of energy. In order to decorate insurance in hybrid WSNs, Zhang and Fok targeted on the way to redeploy cell sensor nodes. They supplied a technique to enhance hybrid Wi-Fi sensor networks` insurance in stages.

Considering the particular necessities of boundary protection, Sun et al. designed a heterogeneous Wi-Fi sensor community framework. There can be much less of a want for human beings to preserve an eye fixed at the border, and the era can be extra correct at detecting unlawful activity. Path publicity has been used notably within side the literature to degree the efficacy of intrusion detection strategies due to its cap potential to quantify the consistent surveillance of a goal through WSNs. To examine the worst-case insurance of the goal, Meguerdichian et al. framed publicity as the mixing of the perceptual depth alongside the goal hint and investigated the minimum course publicity problem. After discrediting it right into a shortest course trouble in a weighted graph, they advanced a grid-primarily based totally method. The least publicity course for a unmarried sensor changed into solved in closed shape through Veltri et al., who additionally devised a localized approximation technique.

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

Insights gained from the study of the MEP problem led us to develop the motivated attacker paradigm and consider additional attack detection strategies. The best way to detect and track an intruder is to plan his movements in advance, which means taking mobile sensing devices into account. Liu et al. recommended an attack detection method for WSNs based on simultaneous background subtraction with computational intelligence and fuzzy grouping, but the observed results of this scheme were relatively stable. This means that the unique movement characteristics of the attacker and the endpoints cannot be adequately represented.

The pursuit-evasion problem, a classic topic in robotics, investigates the optimal movement techniques of the adversary and the goal of the proposed system research. When both players' senses are impaired, as in the classic lion-man problem, Bopardikar et al. propose that the evaders use a post-hoc strategy, i.e., a sweep-buy-catch-purchase approach. This limited perception scenario is similar to the challenge of detecting armed intruders. We propose an armed intruder intrusion detection technique based on a vehicle-cooperative sensor network and the chase-and-avoid problem.

This proposed method efficiently keeps tabs on the armed intruder with minimal performance degradation. Insights gained from the study of the MEP problem led us to develop the motivated attacker paradigm and consider additional attack detection strategies. The best way to detect and track an intruder is to plan his movements in advance, which means taking mobile sensing devices into account. Liu et al. recommended an attack detection method for WSNs based on simultaneous background subtraction with computational intelligence and fuzzy grouping, but the observed results of this scheme were relatively stable. This means that the unique movement characteristics of the attacker and the endpoints cannot be adequately represented. The pursuit-evasion problem, a classic topic in robotics, investigates the optimal movement techniques of the adversary and the goal of the proposed system research. When both players' senses are impaired, as in the classic lion-man problem, Bopardikar et al. propose that the evaders use a post-hoc strategy, i.e., a sweep-buy-catch-purchase approach. This limited perception scenario is similar to the challenge of detecting armed intruders. We propose an armed intruder intrusion detection technique based on a vehicle-cooperative sensor network and the chase-and-avoid problem.

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

III. 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 unauthorized 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:
AndS_1, the detection probability is measured by the Parameters and. ϑ In other words, different types of physical sensors have different technological requirements, Which affects the values of and. ϑ The stochastic sensorparadigm 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 wherethe invader may be spotted. As a result, the total likelihoodof 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 neighboring 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.

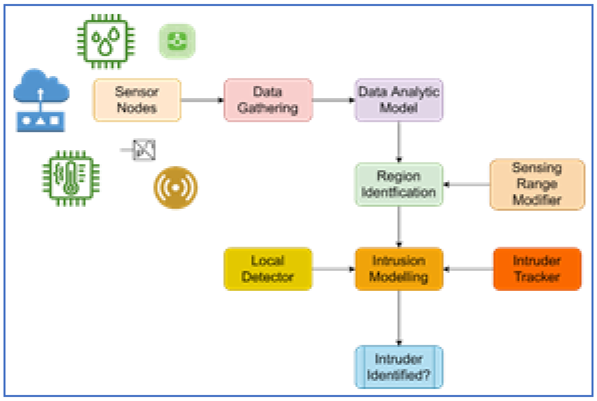

Fig. 2. Proposed System architecture

Where $e(T_j, j)$defines Euclidean remoteness among the node T_j and the targeted node j. To clarify is a positive constant, while is a distance-dependent variable. 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:

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

Where $b = e(T_j,J) - S_1$ and S_0,S_1 represents crucial detecting choices. In particular, whereas if range betweenthe 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 S_0 detected. Whenever the range is between

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.

IV. 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 displaysthe placement of one hundred sensors and the paths taken by one hundred empowered intruder and mobile nodes. consistent with those depictions. Not only that, but route exposure grows for all four systems as the number of nodes in the network increases.

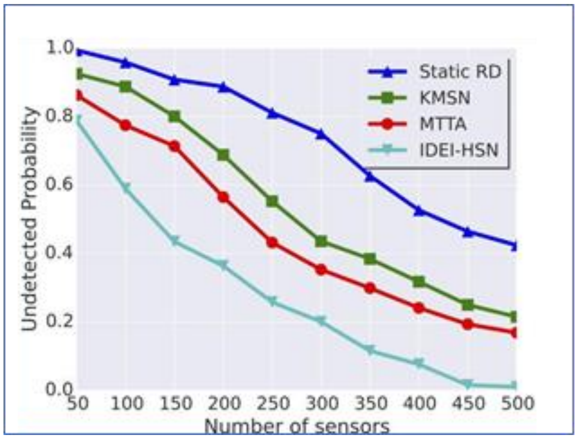

Fig. 3. Comparing risk intrusion detection.

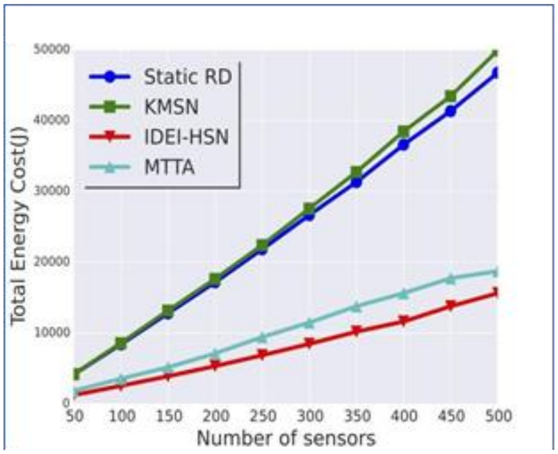

Fig. 4. Comparing energy consumed.

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 remains 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 behavior. 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 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.

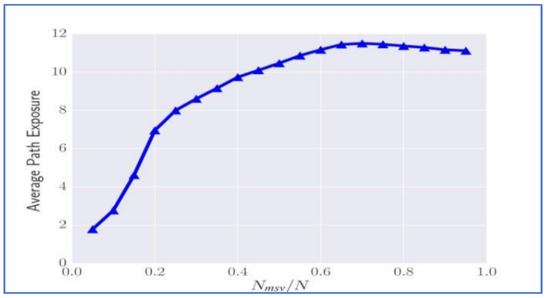

Fig. 5. Intruder movement analysis

But 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.

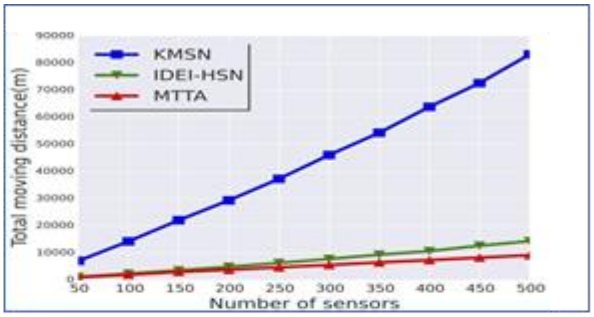

Fig. 6. Displacement analysis

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.

CONCLUSION

Our research starts with the paradigm of an armed intruder. Intruders can more easily identify and escape from detection nodes in an area, so they are less likely to be detected. To address the attacker's difficulties, we propose a distributed intrusion detection approach based on a sensor network formed by cooperation between vehicles. We enhance surveillance by tracking motivated attackers using mobile sensor vehicles, and develop an energy-saving sleep scheduling method for fixed detectors. In addition, mobile sensor devices act as edge computing nodes in each monitoring area, meeting the demands of low latency and high performance. Numerical simulations show that the proposed strategy provides better intrusion detection performance against armed attackers while reducing energy costs. The impact of key factors on the efficiency of the proposed system is also demonstrated through statistical methods.

REFERENCES

[1] Alippi, G. Anastasi, C. Galperti, F. Mancini, and Veltri, Q. Huang, G. Qu, and M. Potkonjak, wireless embedded sensor networks,'' in Proc. 1st Int.Conf. Embedded Networked Sensor Syst., 2003, pp. 40–50.

[2] 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.

[3] 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.

[4] 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.

[5] M. Roveri, ''Adaptive sampling for energy conservation in wireless sensor networks for snow monitoring applications,'' in Proc. IEEE INTERNATONALConf. Mobile Adhoc Sensor Syst.,Oct.2007, pp.1-6.

[6] 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.

[7] 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

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

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

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