IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON COMMUNICATION AND FOG/EDGE COMPUTING TOWARDS INTELLIGENT CONNECTED VEHICLES (ICVS)

Received January 9, 2020, accepted January 24, 2020, date of publication February 3, 2020, date of current version February 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2970973

Generalized Intrusion Detection Mechanism for Empowered Intruders in Wireless Sensor Networks

WENMING WANG[1,2,3], HAIPING HUANG[1,3,4], (Member, IEEE), QI LI[1,3], FAN HE[1,3], AND CHAO SHA[1,3]

[1]School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[2]School of Computer and Information, Anqing Normal University, Anqing 246011, China
[3]Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China
[4]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

Corresponding author: Haiping Huang (hhp@njupt.edu.cn)

This work was supported in part by the National Key Research and Development Program under Grant 2018YFB0803403, in part by the National Natural Science Foundation of China under Grant 61672297 and Grant 61872194, in part by the Key Research and Development Program of Jiangsu Province under Grant BE2017742, in part by the Sixth Talent Peaks Project of Jiangsu Province under Grant DZXX-017, in part by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX19_0908, and in part by the Key Project on Anhui Provincial Natural Science Study by Colleges and Universities under Grant KJ2019A0579 and Grant KJ2019A0554.

ABSTRACT Intrusion detection as one of the most important approaches to guarantee wireless sensing network security has been studied adequately in previous work. However, with the development of electronic anti-reconnaissance technology, the intruder may obtain the location information of detection nodes and perform path planning to avoid being detected. Such intruder is defined as an ''empowered intruder'' who will bring new challenges for traditional intrusion detection methods. Moreover, some subareas may have coverage holes due to random initial deployment of detection nodes, the desired effect of detection cannot be achieved. To address these issues, we propose a vehicle collaboration sensing network model, where mobile sensing vehicles and static sensor nodes cooperate to provide intrusion detection against empowered intruders. Our proposal (named as IDEI) consists of a target pursuit algorithm of mobile sensing vehicles and a sleep-scheduling strategy of static nodes. Mobile sensing vehicles will track the empowered intruder and fill up the coverage breaches, while static nodes follow a sleep-scheduling mechanism and will be awakened by detection nodes nearby when the intruder is detected. Simulation experiments are conducted to compare our proposal with existing methods such as KMsn and MTTA in terms of intrusion detection performance, energy consumption and moving distance of sensor nodes. The parameter sensitivity of IDEI is also studied with extensive simulations. The theoretical analysis and simulation results indicate that our proposal can achieve better efficiency and availability.

INDEX TERMS Vehicle collaboration sensing network, intrusion detection, target pursuit, empowered intruders, wireless sensor networks (WSNs).

I. INTRODUCTION

Wireless sensor networks (WSNs) is a multi-hop and self-organized network formed from a large amount of wireless sensor nodes via wireless communication [1] which is characterized by low cost and easy to deployed. It has been widely adopted in real world applications such as environment perception, modern logistics and military reconnaissance, where multiple sensor nodes work collaboratively to perform monitoring, detection and tracking of specific targets or intruders. Particularly, WSNs based intrusion detection system can be applied to solve security problems from border patrol, region monitoring and post-disaster rescue [2] and has become one of the focuses of current research. It requires a continuous tracking and monitoring [3] mechanism for the intruder and can therefore be modeled as the coverage optimization problem to achieve persistent and high-quality coverage of the intruder.

The associate editor coordinating the review of this manuscript and approving it for publication was Lei Shu.

Current studies on intrusion detection can be divided into two categories. The first one focuses on conducting more accurate localization [4] and trace prediction of the target by utilizing the sensing information from multiple nodes based on decision fusion or local voting techniques. The second one studies the deployment and movement strategy of sensor nodes to achieve improved dynamic coverage of the target [5], which can be viewed as an extension of traditional coverage optimization problems and is the concern of this paper.

The quality of coverage is significantly affected by the initial deployment location of the sensor nodes. Unfortunately, due to the remote or hostile sensing environments (e.g., border patrol or region monitoring), sensor deployment cannot be performed manually in most applications. Thus, sensors are usually deployed by scattering them from an aircraft; however, the actual landing position cannot be controlled due to the existence of wind and obstacles such as trees and mountains. Consequently, some subareas may not have sufficient sensor coverage no matter how many sensors are dropped, and some subareas may even have coverage holes (i.e., areas that are not covered by any sensor node).

To overcome the above problem, it is crucial to add some mobile sensors for intrusion detection, which can be achieved by the recent advancements of embedded hardware and miniaturized robotics [6]. Mobile sensors have the same sensing capability as static sensors and they are able to move to the correct locations for providing the desired coverage after the initial deployment. Unfortunately, these mobile nodes are not capable of detecting and tracking intruders except to improve the quality of coverage. Even worse, with the development of electronic anti-reconnaissance technology, the intruder in real world applications might be equipped with sensing devices which can obtain the location information of detection nodes and perform path planning to avoid being detected. Such intruder is defined as an "empowered intruder", different from the naive intruder, its smart behavior of getting rid of sensor node's tracking make it intractable. Therefore, how to design an effective intrusion detection scheme for empowered intruders is a challenging problem.

Traditional intrusion detection schemes for border patrol or region monitoring are based on the centralized architecture. When the detection nodes find an intruder, they will send the information to the base station or cluster node which will take corresponding measures after information analysis and processing. The process will require frequent interaction between the detection nodes and the base station or cluster node, which will not only occupy a large amount of network bandwidth but also increase the transmission delay of network, resulting in delayed emergency treatment, such as intruder fleeing or sabotage event. Therefore, the traditional centralized architecture is unsuitable for real scenarios, especially against empowered intruders. To achieve local computing, mobile nodes need to be able to record and process the trajectories of tracked intruders in real time, however, ordinary mobile nodes do not have this capability.

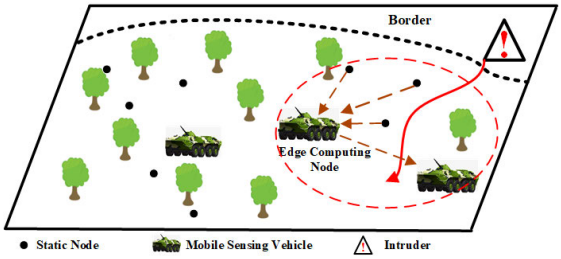


FIGURE 1. Architecture of the vehicle collaboration sensing network for intrusion detection.

The collaboration of mobile sensors and static ones brings a new frontier of research in WSNs. Inspired by the powerful mobile computing, communication, positioning and information processing capabilities of unmanned automatic vehicle, especially unmanned armored vehicle, we take mobile sensing vehicle as the mobile nodes and combine them with the static nodes to form a vehicle collaboration sensing network. In addition, to satisfy the requirements of low latency and high-quality service in intrusion detection, we have incorporated the concept of edge computing into the vehicle collaboration sensing network. Edge computing [7], [8] is a technology that allows computing to be performed at the edge of a network so that computing occurs near data sources. As shown in Fig.1, in our scheme, we select a mobile sensing vehicle to act as an edge computing node in a region. Detection nodes will communicate with the edge computing node when they find an intruder. Subsequently, edge computing node informs the published tracking decisions to all the relevant mobile sensing vehicles, then the corresponding mobile vehicles can follow the instructions to track the intruder and fill the coverage holes.

However, in this paper, we mainly focus on proposing a vehicle collaboration sensing network model, where mobile sensing vehicles and static sensor nodes cooperate to provide intrusion detection against empowered intruders. The model aims to achieve a high coverage rate with less energy consumption caused by detection nodes, and meanwhile to record and process the trajectories of tracked intruders in real time. Therefore, we design a movement strategy of the mobile sensing vehicles and a sleep-scheduling strategy of static nodes.

The contributions and novelty of this paper can be summarized as follows:

- We define and model the movement of empowered intruders for the first time. The empowered intruder is able to obtain location information of detection nodes and will perform path planning to reduce the probability of being detected.
- We propose a vehicle collaboration sensing network model where mobile sensing vehicles and static sensor nodes cooperate to provide intrusion detection against empowered intruders. Furthermore, an intrusion detection mechanism IDEI is designed. Wherein, a distributed

target pursuit algorithm of mobile sensing vehicles is put forward to achieve effective tracking of the empowered intruder. And a sleep-scheduling strategy of static nodes is proposed to reduce the energy consumption and prolong the lifetime of the network. In addition, we select a mobile sensing vehicle as the edge computing node to realize the requirements of low latency and high-quality service.
- Theoretical analysis and simulation experiments demonstrate that our proposal achieves an improved intrusion detection performance with a reasonable energy consumption when compared to other classical intrusion detection methods.

The rest of this paper is organized as follows. Section II reviews related work. System model and assumptions are described in Section III. In Section IV, we model the empowered intruder and compare it with the traditional naive intruder. The intrusion detection method for empowered intruder based on vehicle collaboration sensing network is proposed in Section V. Simulation results and discussions are presented in Section VI. Section VII concludes the whole paper.

II. RELATED WORK

As mentioned above, the intrusion detection problem of WSNs can be modeled as the coverage optimization problem to achieve continuous and high-quality coverage of the intruder [9]. The coverage optimization of WSNs has been extensively studied and can be classified into three categories: Regional coverage [10], target coverage [11] and barrier coverage [12]–[14]. Target coverage requires the sensor network to monitor and collect data from some given targets while barrier coverage studies the probability of an object being detected when crossing the monitoring area [15]. Both target coverage and barrier coverage can be applied to intrusion detection in WSNs [16]. Based on the mobility of sensor nodes, studies on intrusion detection problem of WSNs can be further divided into the following three categories.

A. STATIC SENSOR NETWORKS

A series of intrusion detection schemes based on static sensor networks have been proposed. Sharmin et al. [17] addressed the joint problem of maximizing the sensing coverage quality and the network lifetime for covering heterogeneous targets and a greedy algorithm is proposed to balance sensing quality and network lifetime. A k-nearest neighbor node tracking algorithm based on Voronoi diagram is suggested by Liu *et al.* [18]. However, the algorithm needs global information to build the Voronoi diagram at initialization stage so it does not scale well when network grows. Silvestri *et al.* designed an optimal construction of barrier coverage which can be applied in building intrusion detection system [19]. However, the number of sensors needed to build a complete barrier is considerably large.

The locations of sensors in static sensor networks are fixed after initial deployment. Therefore, there will be coverage breaches when the network is sparse thus it's hard for static sensor networks to ensure intrusion detection performance.

B. MOBILE SENSOR NETWORKS

Mobility of sensor nodes can be utilized to fill up the coverage breaches and improve the intrusion detection performance [20]. Zhou and Roumeliotis [21] studied the problem of optimal trajectory for a team of mobile sensors tracking a moving target with distance measurements only. Simulation results showed that the proposed algorithm achieved desirable performance with linear time complexity. Keung *et al.* [22] introduced the kinetic theory of gas molecules in physics to model the movement of the intruder and mobile sensors. The result indicated that mobile sensor networks achieve better k-coverage of the intruder. Mahboubi *et al.* [23] proposed a grid-based strategy for mobile sensor networks to track a moving target in obstacle environment. This strategy is proved to be feasible by using the shortest path algorithm. Liu *et al.* [5] discussed the optimal movement strategy of the intruder and mobile sensors which represents a Nash equilibrium of a zero-sum game. It should be noted that this optimal strategy assumes that both participants have complete knowledge of the location and movement information of their opponents, which is not practical in real world applications.

C. HYBRID SENSOR NETWORKS

Mobile sensor networks achieve more satisfactory intrusion detection quality than static sensor networks. However, mobile sensors will increase the sensor network cost, which also makes routing and information exchange become very complicated, thus it is not suitable for large-scale deployment. Hybrid sensor networks which consist of both static and mobile sensors can take advantage of sensors' mobility while taking the deployment cost into account, thus have become the focus of current research.

Lambrou [24] established a hybrid sensor network composed of a sparsely deployed static sensor network and a number of mobile sensor nodes and studied its dynamic coverage. Wang *et al.* [25] proposed a distributed action-force based movement strategy to achieve multiple target tracking by using mobile sensors and static sensors. The method guaranteed tracking success probability with low energy consumption. Zhang and Fok [6] focused on how to redeploy mobile sensor nodes to improve network coverage in hybrid WSNs. They proposed a two-phase coverage-enhancing algorithm for hybrid wireless sensor networks. Considering the particularity of border patrol, Sun *et al.* [26] introduced a hybrid wireless sensor network architecture for border patrol systems. The system can reduce the intensive human involvement and improve the detection accuracy of current border patrol systems.

For the reason that the path exposure [27] can quantify WSNs's continuous monitoring of target, it has been utilized in many literatures to evaluate the performance of intrusion detection schemes. Meguerdichian *et al.* [27] formulated exposure as the integration of the perceptual intensity along

the target trace and studied the minimal path exposure problem (a.b. MEP) to evaluate the worst-case coverage of the target. They proposed a grid-based approach by discretizing the problem into the shortest path problem in weighted graph. Veltri *et al.* [28] obtained the closed-form solution of the single sensor MEP problem and developed a localized approximation algorithm to decide the minimal exposure path. The studies on MEP problem has enlightened us to come up with the empowered intruder model and further investigate the possible intrusion detection methods.

In order to detect and track intruders, movement strategy for mobile sensing vehicles should be considered. Liu *et al.* [29] proposed an intrusion detection algorithm based on parallel intelligent optimization feature extraction and distributed fuzzy clustering in WSNs, but the experiment deployment in the scheme was relatively stable, which could not accurately describe the movement characteristics of intruders and nodes. The pursuit-evasion problem which studies the optimal motion strategy of the pursuer and the evader [30] has been a classical issue in robotic science. Bopardikar *et al.* [31] studied the classic Lion and Man problem in which the sensing abilities of both participants are constrained. They put forward a sweep-pursuit-capture pursuer strategy when the evader follows a reactive model. This sensing constrained situation resembles the intrusion detection problem with empowered intruders. Based on the pursuit-evasion problem, we propose an intrusion detection scheme for empowered intruders based on vehicle collaboration sensing network. The proposed scheme achieves effective monitoring of the empowered intruder with rather low energy consumption.

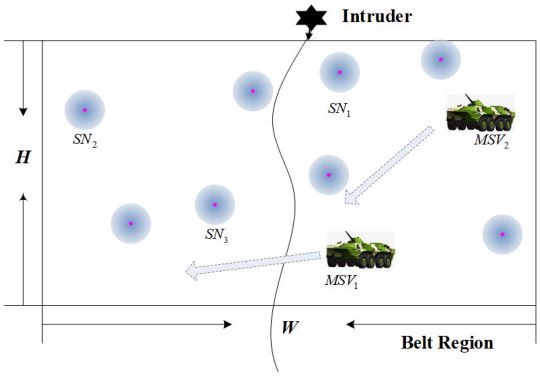


FIGURE 2. Intrusion detection scenario with vehicle collaboration sensing network.

III. PROBLEM STATEMENT AND DEFINITIONS

We consider a hybrid vehicle sensing network scenario consisting of static nodes (*SN*) and mobile sensing vehicles (e.g., armored vehicles) (*MSV*) deployed in a rectangle belt region Z, as shown in Fig.2. The aim of an intruder (I) is to travel across the boundaries of region Z. The static nodes and the mobile sensing vehicles play as detection nodes, which cooperate to locate and track intruders. When some static nodes detect an intruder, the mobile sensing vehicles can take advantage of their mobility to quickly track it. The initial deployment of *SN* and *MSV* follows a spatial Poisson distribution.

The set of *SN* and *MSV* in region Z is denoted as $\{S_i\}$, $i = 1, 2, \ldots, N$, among which the number of *SN* is K and the number of *MSV* is L, we have N=K+L. We then define the perceptual model of node and the performance evaluation metrics of intrusion detection tasks adopted in this paper.

A. PERCEPTUAL MODEL

Definition 1 (Perceptual Intensity): The perceptual intensity [27] of node S_i on target I is defined as:

$$Int\,(S_i) = \frac{\alpha}{[d\,(S_i, I)]^K} \tag{1}$$

where $d\,(S_i, I)$ is the Euclidean distance between the node S_i and the target I. α is a positive constant and K is a distance related parameter. The values of both α and K depend on the sensitivity and technical characteristic of sensing module. Greater distance between the node and target results in less perceptual intensity.

Definition 2 (Perceptual Probability): We adopt the probabilistic sensor model in [10] where sensor S_i can detect target I with a probability of:

$$c(S_i) = \begin{cases} 0, & if\ d\,(S_i, I) \geq R_0 \\ e^{-\lambda a^\beta}, & if\ R_1 < d\,(S_i, I) < R_0 \\ 1, & if\ d\,(S_i, I) < R_1 \end{cases} \tag{2}$$

where $a = d\,(S_i, I) - R_1$ and R_0, R_1 are critical sensing ranges. Namely the target will always be detected by some nodes if the distance between the two is less than R_1 and will never be detected if the distance is greater than R_0. λ and β are parameters that measure detection probability when the distance is between R_0 and R_1. The values of λ and β depend on the technical characteristics of various types of physical sensor devices. Compared with the binary sensor model, the probabilistic sensor model considers the influence of error and noise, which conforms to features of real sensor nodes.

B. PERFORMANCE EVALUATION METRICS

The probability of target I at point u being undetected by nodes is:

$$\mathrm{Prob}_{\mathrm{neg}}(u) = \prod_{i=1}^{N} (1 - c(S_i)) \tag{3}$$

where $c(S_i)$ is defined in Eq. (2) and u is a point inside the monitoring area. Target I to be undetected at point u indicates it will not be detected by both *SN* and *MSV*, thus the probability is the product of all individual probabilities.

Definition 3 (Probability of the Intruder Remaining Undetected While Crossing): Consider the intruder crosses the monitoring area along path P, the probability of the intruder

remaining undetected is:

$$\text{Prob}_{\text{neg}}(P) = \prod_{u_i \in P} \text{Prob}_{\text{neg}}(u_i) \tag{4}$$

Namely, the intruder will not be detected at all points along the path. Thus, the overall probability of the intruder remaining undetected is the product of probabilities at each individual point.

Eq. (4) can be used to evaluate the performance of intrusion detection, especially in the case of sparsely deployed sensor networks where the detection rate of intruders cannot be guaranteed.

Definition 4 (Path Exposure): If the intruder crosses the network along path $p(t)$ in time interval $[t_1, t_2]$, then the path exposure [32] in the process is defined as:

$$\text{E}(p(t), t_1, t_2) = \int_{t_1}^{t_2} I(F, p(t)) \left| \frac{dp(t)}{dt} \right| dt \tag{5}$$

which is a path integral along $p(t)$ where $I(F, p(t))$ represents the perceptual intensity on target I at time t. We have:

$$I(F, p(t)) = \sum_{i}^{N} Int(S_i) \tag{6}$$

namely, the perceptual intensity is the sum of the intensities from all individual nodes. $Int(S_i)$ is defined in Eq. (1). Eq. (5) is also used to evaluate the intrusion detection quality of the sensor networks.

To formulate the movement strategy of the empowered intruder and the mobile sensing vehicles, the following assumptions are made with regard to their moving and sensing capabilities.

1. The empowered intruder has a maximal velocity of V_I and is able to move with any velocity within $[0, V_I]$ in any chosen direction. The empowered intruder is capable of discovering both static nodes and mobile sensing vehicles nearby within a range of R_{senI} and knows about their respective distance and orientation from the intruder itself.

2. The mobile sensing vehicles have a maximal velocity of V_{msv} and can move with any velocity within $[0, V_{msv}]$ in any chosen direction. Similarly, mobile sensing vehicles can sense the intruder and other static nodes nearby and obtain their distance and orientation information.

3. There is a mobile sensing vehicle that acts as an edge computing node in each monitoring area. The edge node can integrate the information obtained from the static nodes and other mobile vehicles and make the corresponding scheduling decision.

4. The static nodes follow the sleep-scheduling scheme in [33] when the network is not involved in intrusion detection tasks.

IV. THE EMPOWERED INTRUDER

With the above problem statement and definitions, we now introduce the model of the empowered intruder. The goal of the empowered intruder is to plan its path according to the knowledge of detection nodes' locations to minimize its path exposure when crossing the monitoring area. Instead, the design goal of intrusion detection system is to maximize this path exposure to achieve a high-quality monitoring of the intruder.

A grid-based algorithm to solve the general MEP problem is proposed in [27]. The algorithm constructs a weighted graph (the weight represents the exposure level of corresponding path) according to the deployment of sensors and transforms the MEP problem into a shortest path problem of the weighted graph. The construction of the weighted graph relies on the global information. In the intrusion detection context, this means that the intruder should know about the locations of detection nodes in the network in order to find a minimal exposure path. It is hardly possible for intruders in practical applications to have such complete knowledge of the whole sensor field, therefore empowered intruders cannot perform path planning with the algorithm in [27].

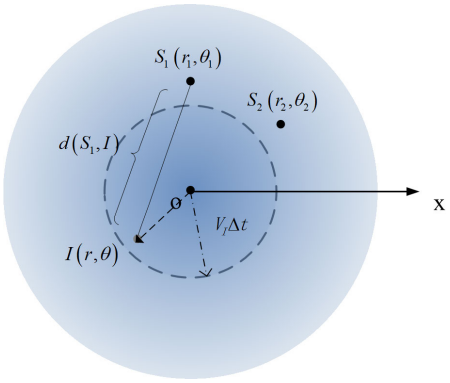


FIGURE 3. The intruder and nearby nodes.

A naive approach to minimize path exposure is to minimize the integral term $I(F, p(t))$ in Eq. (5). A polar coordinate system with the origin at current location of the intruder is established in Fig.3. Substitute Eq. (1) into Eq. (6), we have:

$$\begin{aligned} I(F, p(t)) = I(r, \theta) &= \sum_{i=1}^{N'} \frac{\alpha}{d(S_i, I)^K} \\ &= \alpha \sum_{i=1}^{N'} \left(r^2 + r_i^2 - 2rr_i \cos(\theta - \theta_i) \right)^{-K/2} \end{aligned} \tag{7}$$

where N' represents the number of detection nodes (involved mobile sensing vehicles and static nodes) within the sensing range of the intruder, (r_i, θ_i) is the coordinate of sensor S_i, (r, θ) is the coordinate of the destination of the intruder. To obtain the minimum of $I(F, p(t))$, we need to solve the following optimization problem:

$$\begin{aligned} &\min \ \alpha \sum_{i=1}^{N'} \left(r^2 + r_i^2 - 2rr_i \cos(\theta - \theta_i) \right)^{-K/2} \\ &s.t. \begin{cases} r \le V_I \cdot \Delta t \\ \theta \in [0, 2\pi) \end{cases} \end{aligned} \tag{8}$$

where Δt is the time slot between two path planning calculations, which can be assigned the same value as the sensing circle of sensor node. This is an extremum problem of bivariate function in which the extremum will be obtained at stationary point or on the boundary. We then calculate the partial derivative as follows:

$$\begin{cases} \dfrac{\partial I(r,\theta)}{\partial r} = -\dfrac{\alpha K}{2} \cdot \sum\limits_{i=1}^{N'} \left\{ \left[r^2 + r_i^2 - 2rr_i \cos(\theta - \theta_i) \right]^{\left(-\frac{K}{2}-1\right)} \right. \\ \qquad \left. \cdot \left[2r - 2r_i \cos(\theta - \theta_i) \right] \right\} = 0 \\ \dfrac{\partial I(r,\theta)}{\partial \theta} = -\dfrac{\alpha K}{2} \cdot \sum\limits_{i=1}^{N'} \left\{ \left[r^2 + r_i^2 - 2rr_i \cos(\theta - \theta_i) \right]^{\left(-\frac{K}{2}-1\right)} \right. \\ \qquad \left. \cdot \left[2rr_i \sin(\theta - \theta_i) \right] \right\} = 0 \end{cases} \tag{9}$$

There is no analytic solution for the above equations and calculating a numerical solution will incur significant calculation overhead for the intruder. Besides, the accuracy of the numerical solution relies heavily on the accuracy of the known quantities. Considering the fact that there are noises and errors in the localization process which results in the inaccuracy of r_i and θ_i, the approach to minimize $I(F,p(t))$ is not appropriate.

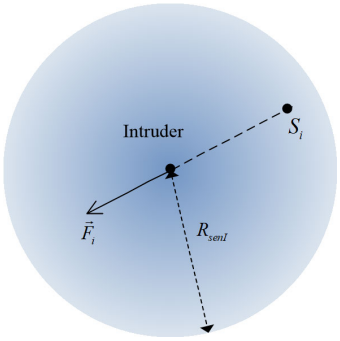


FIGURE 4. The force that acts on the intruder.

In view of this, we will take a low-complexity heuristic movement strategy for the empowered intruder. As shown in Fig.4, the empowered intruder discovers all detection nodes around itself within a range of R_{senI} and acquires the correlative distance and orientation information. It then tries to move away from these modes. Eq. (10) considers the action force from nodes S_i on the intruder:

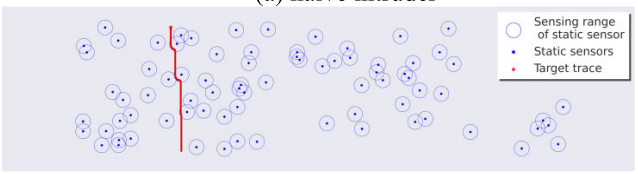
$$\vec{F}_i = \frac{k_r}{d(S_i, I)^{\gamma}} \cdot \vec{e}_{S_i I} \tag{10}$$

where $\vec{e}_{S_i I}$ is the unit vector from S_i to I, k_r is the coefficient of action force and γ is the distance parameter. The magnitude of the action force shows inverse correlation with the distance between S_i and I because the intruder tends to move away from the nearest neighboring node in the first priority. Denote the set of detection nodes (involved mobile sensing vehicles and static nodes) within the sensing range of the intruder as S', we have the final action force which decides the direction of the intruder's movement:

$$\vec{F} = \sum_{i=1}^{N'} \vec{F}_i = \sum_{i=1}^{N'} \frac{k_r}{d(S_i, I)^{\gamma}} \cdot \vec{e}_{S_i I} \tag{11}$$

The strategy of moving along $\vec{F}$ indicates the following results: first, the intruder will escape from the nearest node to avoid being accurately detected; second, when there are multiple nodes around, $\vec{F}$ will point towards the coverage breach where there are less or no detection nodes. Therefore, the intruder will be moving towards the coverage hole and will not be detected. It should be mentioned that the computational cost of this action force is negligible compared to the optimization problem of Eq. (9).

(a) naive intruder



(b) empowered intruder

FIGURE 5. The trajectories of two types of intruders in static sensor networks.

Simulation experiments are conducted to analyze the effect of the strategy taken by the empowered intruder. The empowered intruder and the naive intruder will cross the same random deployed static sensor network and their respective average path exposure will be compared. Parameters except for the number of sensors are described in Tab.1. Fig.5 shows the procedure of intruder crossing the monitoring area with 100 sensors deployed, and the circles in Fig.5 are the sensing range of sensors. Fig.5-(a) shows the trace of the naive intruder which is not capable of deliberately avoiding sensors while Fig.5-(b) shows the trace of the empowered intruder. It can be seen that by taking the action-force-based moving strategy, the empowered intruder is able to adjust its moving direction to avoid being detected by sensors.

Fig.6 shows the comparisons regarding the average path exposure of the naive intruder and the empowered intruder when separately crossing the sensor field. The result is the average of 100 experiments. It can be seen that the average path exposure of the empowered intruder is significantly less than that of the naive intruder, which indicates that the empowered intruder can effectively avoid being detected by traditional intrusion detection systems of WSNs. Besides, the

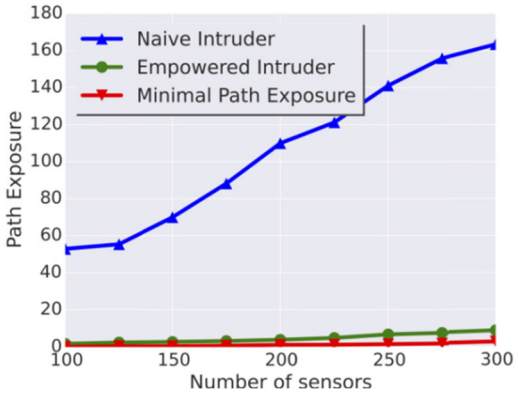


FIGURE 6. The path exposure of various type of intruders.

"minimal path exposure" in Fig.6 is the result of the grid-based approach in [27] and is further less than the path exposure of empowered intruder. However, the global information is required by this approach and its time complexity is very great.

The time complexity of the algorithm in [27] is $O(V^3)$, where V is the number of vertices of the constructed weighted graph. The running time will be $c_1 \cdot V^3 \cdot t_0$, where t_0 is the average running time of basic calculation statement and c_1 is a constant, which are both platform dependent. Furthermore, the action force-based moving strategy taken by the empowered intruder only relies on local information and has a time complexity of $O(1)$ for making a single decision. Therefore, the total running time is $c_2 \cdot f \cdot T \cdot t_0$, where f is the frequency of decision making, T is the total time to travel across the sensor field and c_2 is a constant.

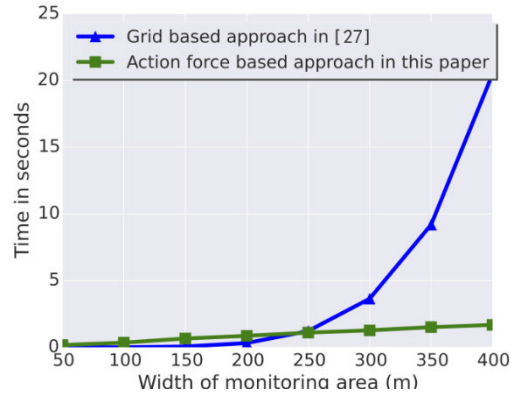


FIGURE 7. The running time of two path planning algorithms.

Fig.7 shows the running time of the two approaches (the experimental environment is described in Section VI) under different sizes of the monitoring area, here we set f as 50 Hz and the aspect ratio of the area is fixed as 4:1. Construction details of the weighted graph and the value of V can be found in [27]. It can be seen from Fig.7 that the running time of the strategy taken by the empowered intruder grows significantly slower than that of the grid-based algorithm when the size of network grows.

V. INTRUSION DETECTION FOR EMPOWERED INTRUDERS

In this section, we propose the intrusion detection mechanism for empowered intruders based on vehicle collaboration sensing network. The proposed scheme includes a movement strategy of mobile sensing vehicles and a sleep-scheduling mechanism of static nodes.

A. MOVEMENT STRATEGY OF MOBILE SENSING VEHICLES

Mobile sensing vehicles can switch between three different motion states: patrol, simple tracking and local cooperation.

Generally, the mobile sensing vehicle is initialized in patrol mode with no intruder around. It will switch to simple tracking mode when there is an intruder within its sensing range and to local cooperation mode when there are both intruders and static nodes around. It will switch back to patrol mode to save energy when there are no intruder or static nodes around. The detailed state chart is illustrated in Fig.8.

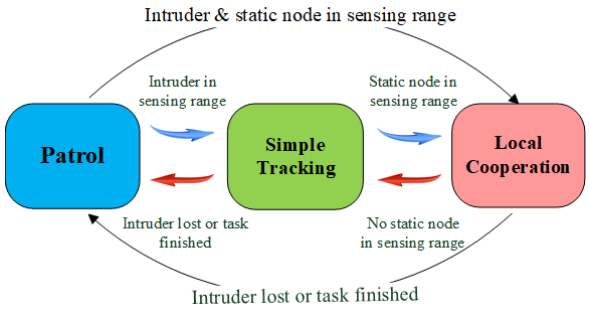


FIGURE 8. The state transition diagram of mobile sensing vehicles.

1) PATROL

In the absence of an intruder within the mobile sensing vehicle's sensing range, the mobile sensing vehicle will be in the low-speed patrol state. It will follow uniform motion to monitor the uncovered area and its velocity will be limited in order to save energy. It will only change the direction of its velocity when arriving the boundary of the area. It will switch to other motion states when there is an intruder inside its sensing range.

2) SIMPLE TRACKING

When the mobile sensing vehicle discovers that there is an intruder inside its sensing range while there are no static nodes inside its sensing range, it will switch to simple tracking mode. This means that the mobile sensing vehicle will adopt a simple yet effective strategy to decide its movement: it will move towards the position where the intruder was last discovered.

Consider the situation in Fig.9 at time t, it assumes that the intruder has the same maximal speed with the mobile sensing vehicle (the influence of maximal speed will be analyzed in Section VI). P_t, E_t are the locations of the pursuer and the evader (the intruder) respectively. The mobile sensing vehicle will move along $\overrightarrow{P_t E_t}$ by adopting simple tracking strategy. P_{t+1}, E_{t+1} are the locations of the pursuer and the

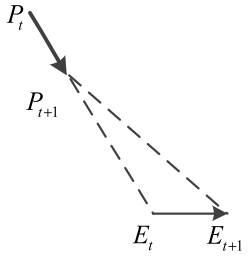


FIGURE 9. The simple tracking scene.

evader (the intruder) respectively at time $t+1$. Then we have $|P_{t+1}E_{t+1}| \leq |P_{t+1}E_t| + |E_tE_{t+1}| = |P_{t+1}E_t| + |P_tP_{t+1}| = |P_tE_t|$, which indicates that the distance between the intruder and mobile sensing vehicle is non-incremental. Note that the distance remains unchanged when and only when the evader also moves along the vector from P_t to E_t. However, the intruder also needs to avoid static nodes along its path so the direction of its velocity will change over time, which results in the decrease of the distance between the mobile sensing vehicle and the intruder and that satisfies $\lim_{t\to\infty} |P_tE_t| = 0$.

The above discussion demonstrates the effectiveness of the simple tracking strategy.

3) LOCAL COOPERATION

When the mobile sensing vehicle discovers that there are both intruder and static nodes inside its sensing range, it will switch to local cooperation state. As the strategy taken by the empowered intruder is to escape from detection nodes and move towards the coverage hole, it is reasonable to utilize the mobility of mobile sensing vehicle to achieve two effects. Firstly, the mobile sensing vehicle should shorten the distance between the intruder and itself, secondly, it should try to fill the coverage hole of the static node network.

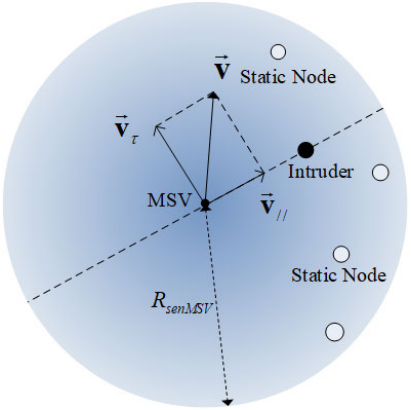


FIGURE 10. The local cooperation strategy.

Consider the situation in Fig.10, the velocity of mobile sensing vehicle *MSV* is composed of two mutually independent vectors. Vector $\vec{\mathbf{v}}_{//}$ targets at I from *MSV* and its magnitude is set as 1. $\vec{\mathbf{v}}_{//}$ represents the tendency to be closer to the target. Vector $\vec{\mathbf{v}}_\tau$ is perpendicular to the line connecting *MSV* and I and points to the side which has less static nodes. The magnitude of $\vec{\mathbf{v}}_\tau$ is $k_1 \cdot (\Delta n)^\omega$, where Δn is the difference of the number of static nodes on both sides of the line connecting *MSV* and I, k_1, ω are constant coefficients which can be set to modify the weights of the two motion components.

In local cooperation mode, the mobile sensing vehicle will try to get closer to the intruder and compensate for the coverage breach of static nodes. Mobile sensing vehicles cooperate with static ones to provide more effective intrusion detection.

In summary, the mobile sensing vehicle will decide its motion state with the information perceived and adjust its velocity accordingly. It should be noted that the speed of the mobile sensing vehicle in state 2 and state 3 should be relatively high (might reach maximal speed if necessary) in order to track the intruder effectively.

B. SLEEP-SCHEDULING MECHANISM OF STATIC NODES

In order to reduce the energy consumption of the entire network and prolong its lifetime, a sleep-scheduling mechanism should be considered when designing intrusion detection scheme. In this paper, the static nodes in IDEI adopt the following sleep-scheduling strategy:

1. When the network is in idle state, the network formed by static nodes will follow SPAN [33] to save energy;
2. When an active static node detects the existence of the intruder, it will broadcast wake-up signal to all nodes within its communication range;
3. When a mobile sensing vehicle detects the existence of the intruder and static nodes, it will broadcast wake-up signal to all nodes within its communication range;
4. A sleeping static node wakes up after receiving wake-up signal from step 2 or 3 and stays active for time interval T_0, during which it will be able to perform intrusion detection task. If no intruder is detected by the node, it will switch to step 1 and follow the original sleep-scheduling algorithm.

The mobile sensing vehicles in IDEI do not follow any sleep-scheduling mechanism and are always awake to detect and track intruders.

By introducing the above sleep-scheduling mechanism, IDEI is able to guarantee high-quality detection of the intruder while reducing network energy consumption and prolonging network lifetime.

VI. SIMULATION AND DISCUSSION

In this section, we conduct simulation experiments to testify the performance of IDEI against empowered intruders based on vehicle collaboration sensing network and compare the results with existing intrusion detection approaches based on WSNs. The sensitivity of some key parameters of IDEI will also be analyzed in this section.

The simulation is implemented on an Intel(R) Core(TM) i7-7700HQ (2.8GHz) computer using MATLAB. The main parameter settings are shown in Tab.1 unless otherwise specified. The result is the average of 100 experiments. The setting of relevant parameters is specified as follows:

When studying the perceptual intensity on the intruder, what we care about is the relative value among different schemes. So we only need to guarantee the same value of α for all schemes and we can simply set $\alpha = 1$. For the value of K, it can be referred to [35]. The values of β and λ can be found in [10]. For k_r, as we only need to decide the direction of the action-force, k_r can be set as 1 for simplicity and the value of γ is described in [10]. The values of ω and k_l can be adjusted to modify the weights of the two movement strategies in local cooperation state, and their values in Tab.1 can achieve desirable intrusion detection performance in our simulations. The values of k_{recv} and k_{trans} can be seen in [34] and k_{sen} in [35].

TABLE 1. Notations and simulation settings.

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 [31]
β	Parameter of perceptual probability	0.5 [10]
λ	Parameter of perceptual probability	0.5 [10]
k_r	Constant of virtual force from node to intruder	1
γ	Distance parameter of virtual force from node to intruder	1 [10]
k_l	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_{senI}	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 [35]
k_{recv}	Constant of energy consumption in receiving task	50 nJ/bit [34]
k_{trans}	Constant of energy consumption in transmitting task	100pJ/bit/m^2 [34]

A. COMPARISONS WITH EXISTING APPROACHES

IDEI will be compared with three intrusion detection schemes of WSNs which are Static RD (random deployed static sensor networks), KMsn (mobile sensor network based on kinetic theory from [22]) and MTTA (target tracking with wireless sensor networks in [25]). We will investigate the path exposure, probability of remaining undetected, energy cost and average displacement distance among the four schemes.

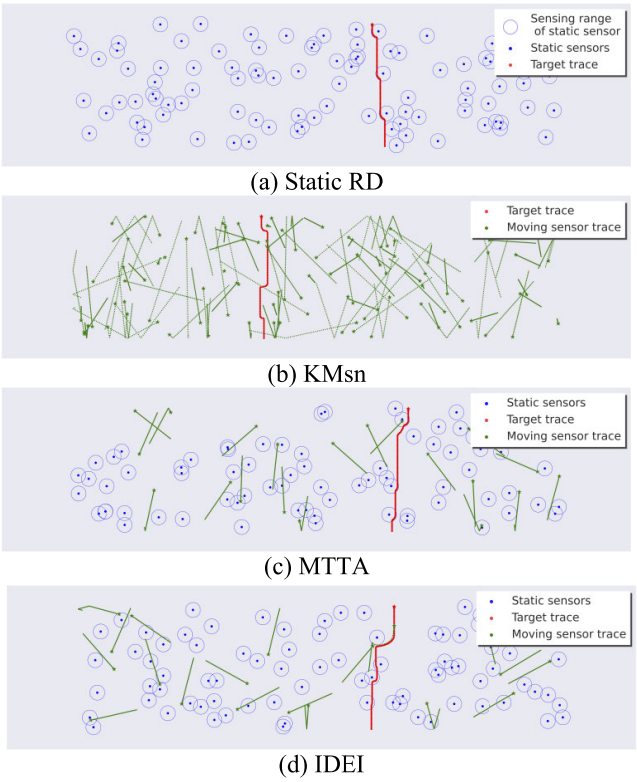


FIGURE 11. The trajectories of intrusion detection with different schemes.

Fig.11 shows the deployment of sensors as well as the trajectories of the empowered intruder and mobile nodes (if any) with a total of 100 nodes. The blue circle represents the sensing range of static sensors while the red curves and green lines represents the trajectory of the intruder and mobile sensing vehicles respectively. Fig.11-(a) illustrates the situation where the empowered intruder travels across a static sensor network, it can be seen that the empowered intruder is able to plan its path and keep undetected by static sensors. KMsn in Fig.11-(b) utilizes the mobility of sensors to cover more areas. However, the mobile sensor in KMsn travels with a fixed velocity and does not have a corresponding strategy against the empowered intruder's behavior thus high-quality monitoring cannot be achieved. MTTA adopts a mechanism where static sensors and mobile sensors work together to construct intrusion detection system. However, the success of MTTA requires the intruder being detected by some static sensors, which is not likely to happen with the empowered intruder. Fig.11-(c) shows that MTTA cannot perform well against the empowered intruder. As a contrast, by using the strategy of simple pursuit and local cooperation, the mobile sensing vehicle in IDEI can monitor the empowered intruder effectively, as shown in Fig.11-(d) where the trajectory of a mobile sensing vehicle overlaps with that of the intruder to perform continuous monitoring.

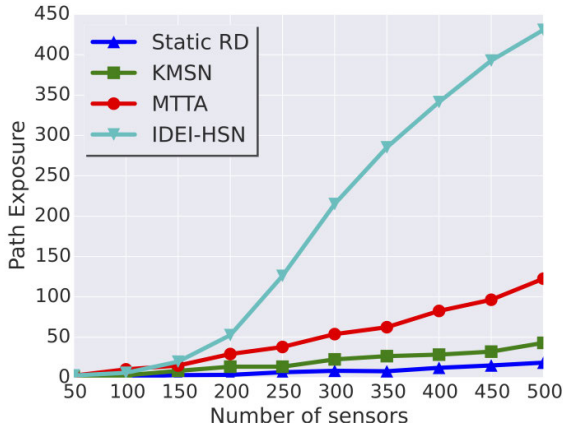


FIGURE 12. Path exposure of the 4 schemes.

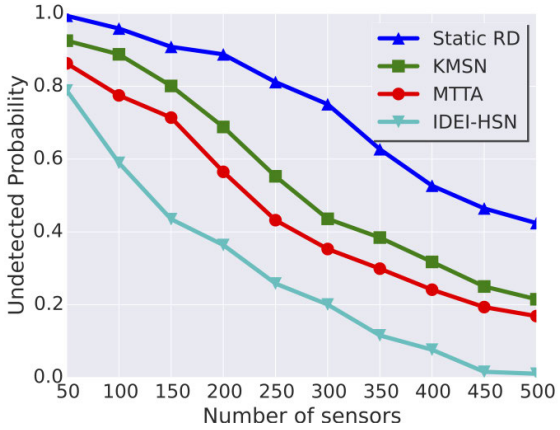


FIGURE 13. The probability of the empowered intruder to remain undetected.

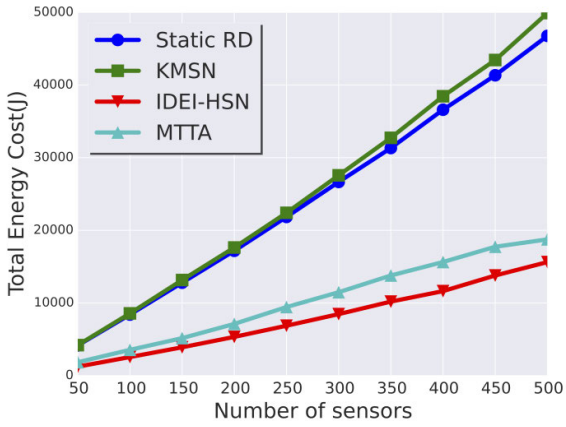


FIGURE 14. Energy consumption of the 4 schemes.

1) PATH EXPOSURE

Fig.12 shows the path exposure of the four intrusion detection schemes when the total number of nodes grows from 50 to 500. It can be seen that Static RD and KMsn have lower path exposure in all cases. The reason is that sensors in these two schemes cannot counter the strategy of the empowered intruder. Compared with the former two, MTTA has a greater path exposure intensity, but less than that of IDEI. As discussed above, the cooperation mechanism of MTTA relies on the success detection by some static sensors, which often fails due to the strategy of the empowered intruder.

The results of the path exposure are consistent with the illustrations of trajectories in Fig.11. In addition, when the total number of nodes grows, the path exposure of all four schemes increases. Among them, the path exposure of IDEI increases significantly, which indicates that by adopting the pursuit and cooperation mechanism, the newly added sensors are utilized effectively to provide better intrusion detection service. On the contrary, the increment of the number of nodes results in rather limited improvement in intrusion detection performance with Static RD and KMsn.

2) PROBABILITY OF REMAINING UNDETECTED WHEN CROSSING THE AREA

Fig.13 shows the probability of the empowered intruder to remain undetected when crossing the area in all four schemes where the total number of nodes grows from 50 to 500. We can see that IDEI comes with the lowest probability, followed by MTTA. On the contrary, there is a great chance that the empowered intruder can cross the monitoring area without being detected in Static RD and KMsn, which indicates a poor intrusion detection performance. As the empowered intruder takes a strategy of escaping from detection nodes, it successfully keeps its distance from nodes in Static RD, KMsn and MTTA to reduce the probability of being detected. The probability of all four schemes decreases when the number of nodes increases, which means that a dense network leads to more opportunities of detection which is consistent with practical experience.

3) ENERGY COST OF INTRUSION DETECTION TASK

Fig.14 displays the energy consumption of the four schemes in intrusion detection tasks. The node consumes energy to perform basic tasks such as data transmitting and data acquisition [34], [35], which can be formulated as $E = k_{sen} \cdot r_1 + k_{recv} \cdot r_2 + k_{trans} \cdot r_3 \cdot d^2$, where r_1, r_2, r_3 are the amount of data sampled, received and transmitted respectively and d is the distance between the transmitter and the receiver. We can see that MTTA and IDEI have a similar level of energy consumption, much superior to Static RD and KMsn which do not include any sleep-scheduling mechanism. Both MTTA and IDEI are designed with a sleep-scheduling mechanism to reduce the network's energy consumption. In MTTA, some static nodes will act as local control centers and will broadcast information about the intruder, resulting in extra energy cost in data transmitting. In IDEI, both static nodes and mobile sensing vehicles will broadcast wake-up signals to nearby nodes when necessary, which also leads to extra data transmitting energy consumption. Overall, both MTTA and IDEI have desirable energy consumption but only IDEI can detect empowered intruders effectively.

4) DISPLACEMENT DISTANCE OF MOBILE SENSING NODES

Movement of a mobile sensing node will consume its energy, therefore an ideal movement strategy will try to minimize the displacement distance of sensors while guaranteeing desirable intrusion detection performance. Fig. 15 shows the total moving distance of mobile nodes in KMsn, MTTA and IDEI (mobile sensing vehicles) when the number of nodes grows from 50 to 500. It can be seen that the total moving distances of MTTA and IDEI are significantly less than that of KMsn. The fact that mobile nodes in KMsn always conduct uniform motion, which results in unnecessary displacement distance in the detection process. Considering its poor intrusion detection quality and high energy consumption, KMsn is not the ideal scheme for intrusion detection against empowered intruders.

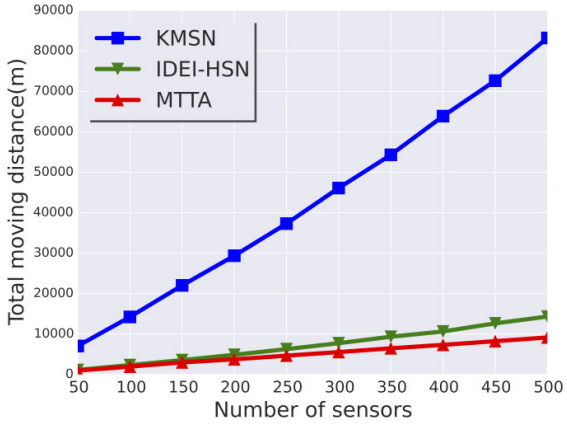


FIGURE 15. Displace distance of the 4 schemes.

Note that the moving distance of mobile nodes in MTTA is slightly less than that of IDEI. In fact, the mobile nodes in MTTA follow instructions from special static nodes (L_0 in [25]) and move towards the target. However, L_0 cannot detect the empowered intruder effectively due to its evasion strategy so it probably would not broadcast such instructions, which results in less moving distance for MTTA. Considering that IDEI has significant superiority of intrusion detection performance, a slightly increment of moving distance is acceptable.

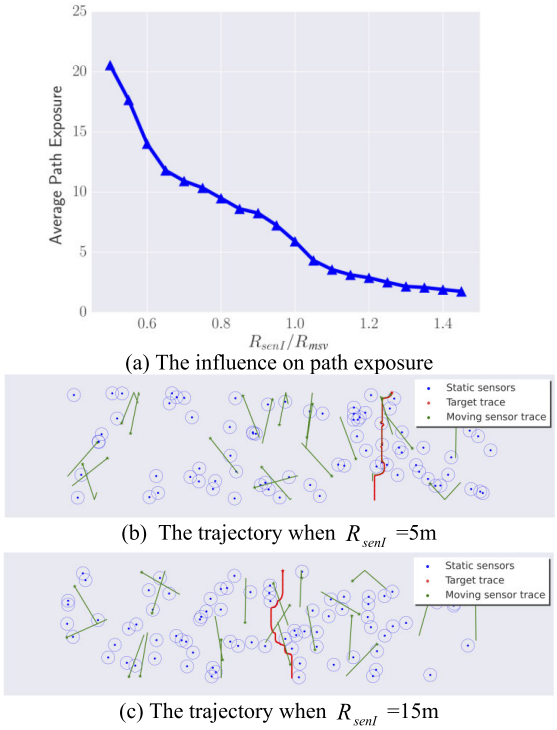
The above simulation experiments verify that IDEI achieves a satisfactory intrusion detection performance with less energy consumption and total moving distance.

B. SENSITIVITY ANALYSIS OF KEY PARAMETERS

In the context of intrusion detection for empowered intruders, the sensing and moving ability of the intruder against that of the detection nodes has critical influence on the performance of IDEI. The proportion of mobile sensing vehicles will also influence the quality of intrusion detection. In this subsection, we will conduct simulations to study the impact of some key parameters on the performance of IDEI.

1) SENSING RANGE OF THE INTRUDER

The sensing ability of the empowered intruder will affect the detection performance of IDEI. We study the influence of R_{senI} by fixing the sensing range of detection nodes (involved mobile sensing vehicles and static ones) and altering R_{senI} to compare the path exposure in different settings. It can be seen from Fig.16-(a) that the path exposure decreases gradually when R_{senI} increases. The reason is that a greater R_{senI} enables the empowered intruder to discover detection nodes farther away thus has sufficient time to react. It might change its direction even before entering the sensing range of detection nodes when R_{senI} is large enough. The result of path exposure coincides with the trajectories illustrated in Fig.16-(b) ($R_{senI} = 5$m) and Fig.16-(c) ($R_{senI} = 15$m).



(a) The influence on path exposure

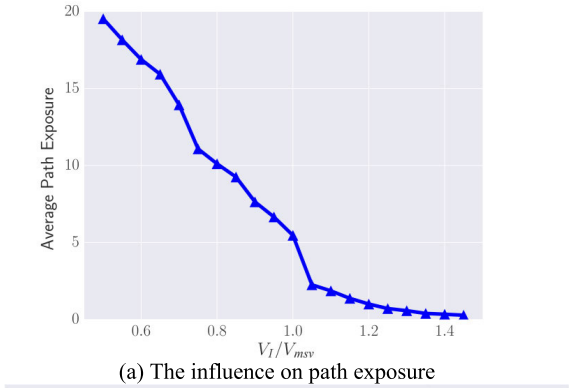
(b) The trajectory when R_{senI} =5m

(c) The trajectory when R_{senI} =15m

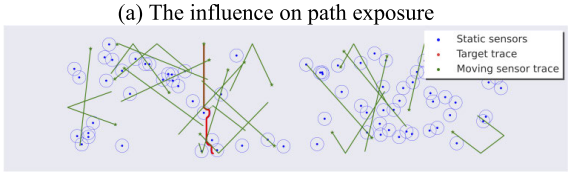
FIGURE 16. The impact of the intruder's sensing range.

2) MAXIMAL VELOCITY OF THE INTRUDER

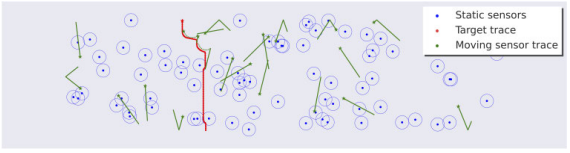
The mobility ability of the intruder is mainly decided by its maximum speed. Here we fix the maximum speed of mobile sensing vehicles (10m/s) and alter V_I to compare the average path exposure. We can see from Fig.17-(a) that the path exposure decreases when V_I increases. The reason is that a greater V_I enables the empowered intruder to escape quickly when it finds detection nodes around. In addition, when the speed of the intruder becomes greater than V_{msv}, mobile sensing vehicles can no longer track the intruder continuously, so the path exposure continues to decrease, which is in consistent with the trajectories in Fig.17-(b) and Fig.17-(c). However, we can see from Fig.17-(c) that even in the case where $V_I > V_{msv}$, the mobile sensing vehicles in IDEI will



(a) The influence on path exposure

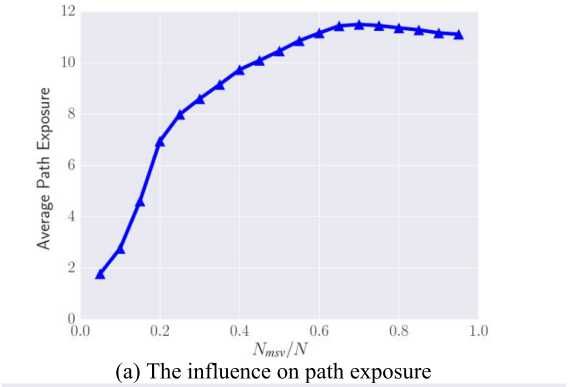


(b) The trajectory when V_I =5m/s

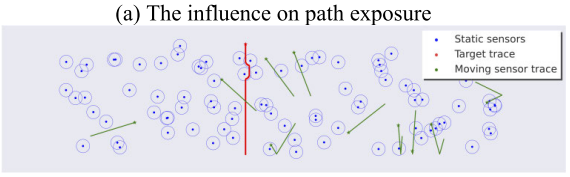


(c) The trajectory when V_I =15m/s

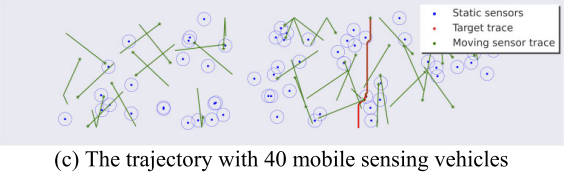
FIGURE 17. The impact of the intruder's maximal velocity.



(a) The influence on path exposure



(b) The trajectory with 10 mobile sensing vehicles



(c) The trajectory with 40 mobile sensing vehicles

FIGURE 18. The impact of the proportion of mobile sensing vehicles.

still try to track the intruder as long as possible. Compared with the case in KMsn where nodes move independently regardless of the location of the intruder, IDEI makes use of the mobility of sensing vehicle more effectively.

3) PROPORTION OF MOBILE SENSING VEHICLES

Another key parameter of IDEI is the proportion of mobile sensing vehicles among all detection nodes. Here the total number of nodes is fixed ($N = 100$) and the proportion of mobile sensing vehicles is varied to compare the average path exposure in different settings. Fig.18-(a) shows that the intrusion detection performance improves when the number of mobile sensing vehicles increases. Fig.18-(b) and Fig.18-(c) show that the trajectories of nodes at different numbers of mobile sensing vehicles. The reason for this change tendency is that more mobile sensing vehicles can result in more opportunities of tracking the intruder and filling the coverage holes. However, when the proportion of mobile sensing vehicles reaches a certain value (0.65 in our case), the path exposure no longer increases. In fact, the excessive number of mobile sensing vehicles means insufficient static nodes, which will result in the failure of the local cooperation strategy. In view of this, the proportion of mobile sensing vehicles should be carefully chosen in practical applications according to task requirements and cost constraints.

VII. CONCLUSION AND FUTURE WORK

In this paper, we first put forward the model of empowered intruder. Compared with naive intruders, the empowered intruder can locate detection nodes nearby and escape from them to reduce the probability of being detected. Aiming at the challenge brought by the empowered intruder, a distributed intrusion detection scheme IDEI based on vehicle collaboration sensing network is proposed. Mobile sensing vehicles are utilized to track the empowered intruder to achieve high-quality monitoring and a sleep-scheduling mechanism is designed for static sensors to reduce energy consumption. In addition, there is a mobile sensing vehicle that acts as an edge computing node in each monitoring area to satisfy the requirements of low latency and high-quality service.

The simulation results demonstrate that compared with existing methods, the proposed scheme has better intrusion detection performance against empowered intruders as well as improved energy cost. Sensitivity analysis also reveals the impact of some important parameters on the performance of IDEI.

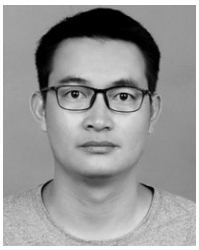
For future work, we plan to combine our scheme with trace prediction method based on data fusion techniques to form a more complete intrusion detection system. In addition, combination of intrusion detection and edge computing is an important research direction, but how to select the optimal edge nodes in the system is still a challenge. Therefore, in the following work, we will focus on the selection strategy of the edge nodes to improve the efficiency of intrusion detection.

ACKNOWLEDGMENT

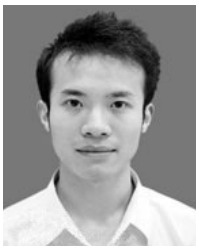
The authors would like to thank the anonymous reviewers of this paper for his/her objective comments and helpful suggestions while at the same time helping us to improve the English spelling and grammar throughout the manuscript.

REFERENCES

[1] M. H. Anisi, G. Abdul-Salaam, M. Y. I. Idris, A. W. A. Wahab, and I. Ahmedy, "Energy harvesting and battery power based routing in wireless sensor networks," *Wireless Netw.*, vol. 23, no. 1, pp. 249–266, Jan. 2017.
[2] M. Mukherjee, L. Shu, L. Hu, G. P. Hancke, and C. Zhu, "Sleep scheduling in industrial wireless sensor networks for toxic gas monitoring," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 106–112, Aug. 2017.
[3] F. Xiao, Z. Wang, N. Ye, R. Wang, and X.-Y. Li, "One more tag enables fine-grained RFID localization and tracking," *IEEE/ACM Trans. Netw.*, vol. 26, no. 1, pp. 161–174, Feb. 2018.
[4] F. Xiao, W. Liu, Z. Li, L. Chen, and R. Wang, "Noise-tolerant wireless sensor networks localization via multinorms regularized matrix completion," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2409–2419, Mar. 2018.
[5] 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. 2013.
[6] 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.
[7] T. 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.
[8] T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on fog computing in sensor–cloud system," *Future Gener. Comput. Syst.*, to be published, doi: 10.1016/j.future.2018.05.049.
[9] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. B. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," in *Proc. Conf. Comput. Commun., 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (IEEE INFOCOM)*, vol. 3, Apr. 2001, pp. 1380–1387.
[10] Y. Zou and K. Chakrabarty, "Sensor deployment and target localization in distributed sensor networks," *Trans. Embedded Comput. Syst.*, vol. 3, no. 1, pp. 61–91, Feb. 2004.
[11] R. 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.
[12] S. 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.
[13] C.-I. 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.
[14] H. 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.
[15] H. Kim, J. Ben-Othman, S. Cho, and L. Mokdad, "A framework for IoT-enabled virtual emotion detection in advanced smart cities," *IEEE Netw.*, vol. 33, no. 5, pp. 142–148, Sep. 2019.
[16] M. Naderan, M. Dehghan, H. Pedram, and V. Hakami, "Survey of mobile object tracking protocols in wireless sensor networks: A network-centric perspective," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 11, no. 1, p. 34, 2012.
[17] 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.
[18] 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. 2016.
[19] S. Silvestri and K. Goss, "MobiBar: An autonomous deployment algorithm for barrier coverage with mobile sensors," *Ad Hoc Netw.*, vol. 54, pp. 111–129, Jan. 2017.
[20] B. Wang, H. B. Lim, and D. Ma, "A survey of movement strategies for improving network coverage in wireless sensor networks," *Comput. Commun.*, vol. 32, nos. 13–14, pp. 1427–1436, Aug. 2009.
[21] 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. 2008.
[22] G. Y. Keung, B. Li, and Q. Zhang, "The intrusion detection in mobile sensor network," *IEEE/ACM Trans. Netw.*, vol. 20, no. 4, pp. 1152–1161, Aug. 2012.
[23] 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. 2017.
[24] T. P. Lambrou, "Optimized cooperative dynamic coverage in mixed sensor networks," *ACM Trans. Sensor Netw.*, vol. 11, no. 3, pp. 1–35, Feb. 2015.
[25] T. 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.
[26] 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 2011.
[27] S. Meguerdichian, F. Koushanfar, and G. Qu, "Exposure in wireless ad-hoc sensor networks," in *Proc. 7th Annu. Int. Conf. Mobile Comput. Netw.*, 2001, pp. 139–150.
[28] G. 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.
[29] Z. 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.
[30] T. H. Chung, G. A. Hollinger, and V. Isler, "Search and pursuit-evasion in mobile robotics," *Auton. Robot*, vol. 31, no. 4, pp. 299–316, Nov. 2011.
[31] S. D. Bopardikar, F. Bullo, and J. P. Hespanha, "Sensing limitations in the Lion and Man problem," in *Proc. Amer. Control Conf.*, Jul. 2007, pp. 5958–5963.
[32] T. Clouqueur, V. Phipatanasuphorn, and P. Ramanathan, "Sensor deployment strategy for detection of targets traversing a region," *Mobile. Netw. Appl.*, vol. 8, no. 4, pp. 453–461, 2003.
[33] B. Chen, K. Jamieson, and H. Balakrishnan, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *Wireless Netw.*, vol. 8, no. 5, pp. 481–494, 2002.
[34] W. 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.
[35] C. 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.



WENMING WANG received the M.S. degree from the College of Information Science and Technology, Jinan University, Guangzhou, China, in 2014. He is currently pursuing the Ph.D. degree with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China. He is a Lecturer with the School of Computer and Information, Anqing Normal University. His research interests include wireless sensor networks and information security.

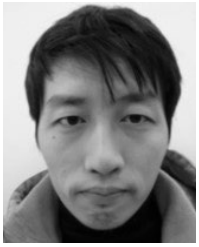


HAIPING HUANG (Member, IEEE) was born in Sanming, Fujian, China, in 1981. He received the B.Eng. and M.Eng. degrees in computer science and technology from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2002 and 2005, respectively, and the Ph.D. degree in computer application technology from Soochow University, Suzhou, China, in 2009.

From May 2013 to November 2013, he was a Visiting Scholar with the School of Electronics and Computer Science, University of Southampton, Southampton, U.K. He is currently a Professor with the School of Computer Science, Nanjing University of Posts and Telecommunications. His research interests include information security and privacy protection of wireless sensor networks.

Dr. Huang was awarded the 2nd prize of advance of science and technology twice by Ministry of Education of China (ranked 2nd and 3rd, respectively). As the young and middle-aged academic leader (the third level) of the "333 Project" of Jiangsu Province, he was listed in the high-level training talents for the "Six Talent Peaks Program" of Jiangsu Province, in 2015. He is currently an Associate Editor of *International Journal of Communication Systems* and an Editor of *International Journal of Distributed Sensor Networks*.

QI LI received the Ph.D. degree in computer system architecture from Xidian University, Xi'an, China, in 2014. He is currently an Associate Professor with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include cloud security, information security, and applied cryptography.



FAN HE received the B.Eng. degree in applied physics from Peking University, Beijing, China, in 2013. He is currently with successive postgraduate and doctoral programs of study with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interest includes coverage optimization and data gathering of wireless sensor networks.

CHAO SHA received the B.Eng., M.Eng., and Ph.D. degrees in computer science and technology from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2005, 2008, and 2010, respectively. He is currently an Associate Professor with the School of Computer Science, Nanjing University of Posts and Telecommunications. His research interests include mobile data collection and energy hole avoidance in wireless rechargeable sensor networks.