Journal of Interconnection Networks
Vol. 22, No. 2 (2022) 2149002 (22 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0219265921490025

Energy-Efficient Model for Intruder Detection Using Wireless Sensor Network

Ashok Kumar Rai* and A. K. Daniel†

Computer Science and Engineering Department
Madan Mohan Malaviya University of Technology
Gorakhpur, Uttar Pradesh 273016, India
*ashok7086@gmail.com
†danielak@rediffmail.com

Received 6 March 2022
Accepted 30 October 2022

A wireless sensor network (WSN) can be used for various purposes, including area monitoring, health care, smart cities, and defence. Numerous complex issues arise in these applications, including energy efficiency, coverage, and intruder detection. Intruder detection is a significant obstacle in various wireless sensor network applications. It causes data fusion that jeopardizes the network's confidentiality, lifespan, and coverage. Various algorithm has been proposed for intruder detection where each node act as an agent, or some monitoring nodes are deployed for intruder detection. The proposed protocol detects intruders by transmitting a known bit from the Cluster Head (CH) to all nodes. The legal nodes must acknowledge their identification to the CH in order to be valid; otherwise, if the CH receives an incorrect acknowledgement from a node or receives no acknowledgement at all, it is an intruder. The proposed protocol assists in protecting sensor data from unauthorized access and detecting the intruder with its location through the identity of other legal nodes. The simulation results show that the proposed protocol delivers better results for identifying intruders for various parameters.

Keywords: Base station; cluster head; intruder; residual energy; wireless sensor network.

1. Introduction

Nowadays, the wireless sensor network is economically feasible and flexible to establish in healthcare, defence, surveillance, traffic monitoring, and fire detection. These networks contain economical and easily deployable sensor nodes that sense the data, process it, and send it to the BS. However, nodes are powered by batteries, so energy efficiency is a critical issue in designing such a network (Dwivedi and Kumar, 2020). Security is the key challenge in a WSN, so there are various benefits and drawbacks of the WSN network, such as being scalable, flexible, and not requiring wires or

*Corresponding author.

cables. On the other hand, it is wireless, so it can be hacked. It cannot be used for high-speed data transfer; expensive, energy efficient, etc. Intruders may ruin the confidentiality and integrity of the network. Coverage and connectivity in WSNs play an important role in detecting intruders before reaching the Base Station or other important network locations. WSN has many applications in defence, health care, the environment, and industrial monitoring. However, the network has to design with a longer lifetime, better target coverage, and security.

Intruders are unwanted identities that affect the network confidentiality, connectivity, and security. Intruders may cause different types of security threats like denial of service attacks, routing attacks, and Sybil attacks, where the massive destructive attacks against the sensor network where numerous genuine identities with forged identities are used for getting an illegal entry into a network (Sharma *et al.*, 2016). So, Intruder observation through the network is a very important aspect of WSN as they can reduce the energy efficiency and lifetime of the network; their identification is very important. In some network regions, the probability of intruder entries is considerable, called sensitive region coverage. Let us consider a network having various regions to monitor the intruders. Let us consider Region 1 and Region 2 are the area for intruder entry called very sensitive for intruders entry. So the density of node is increased in region1 and region 2. The nodes are deployed in the sensitive areas more than in less sensitive regions. Figure 1 shows the deployment of the node for the sensitive and less sensitive regions.

Intruders may receive the packets from a single node or multiple nodes, so the transmission energy (E_{TX}) dissipation from single or multiple nodes increases. In the area where a single node's energy dissipation is greater than the average value, an intruder can be detected from a single node, and energy dissipation from multiple nodes is greater than the average value, intrudes are detected from multiple nodes. Identification of intruders by a single node can inform the cluster head to Base Station. Base Station considers it as a legitimate node. Identification of intruders by multiple nodes also informs their CH, and the base station can increase the chance of failure of intruder's effect on the network. The state Base Station considers it a

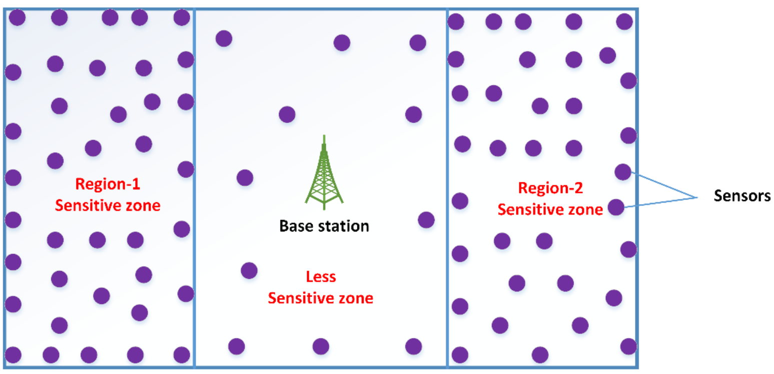

Fig. 1. Deployment of the node for sensitive and less sensitive regions.

potential intruder detection zone, stops receiving data, identifies the intruder as a legitimate node, and deactivates it.

In this paper, the nodes are deployed in area A with different densities. The probability of intruder detection depends upon the density of the node and its residual energy. The model finds the suitable node density for properly detecting an intruder. Sending a known bit from CH to its member nodes allows the proposed protocol to identify the intruder. The legal nodes transmit an acknowledgement to the CH after receiving a known bit. Members nodes that deliver incorrect acknowledgements or fail to send acknowledgements while still receiving packets from the network region are regarded as intruders. The area where an intruder enters the network can be identified through the CH that receives incorrect or no acknowledgement.

1.1. *Motivation and contribution*

Energy efficiency is the most important aspect of WSN, so various algorithm has been proposed to increase the network's lifetime. However, confidentiality integrity and security consideration are also important for which various algorithm has been proposed, such as deploying various monitoring nodes in the network. Extra monitoring nodes increase the cost and maintenance of the network. However, in the proposed protocol, no extra monitoring nodes are deployed, legal nodes themselves verify their validity to the CH, and malicious nodes are detected.

Our significant contribution in the article is paraphrased as:

(1) A new model proposed a protocol that detects malicious nodes.
(2) The experiment is done for 5, 10, and 15 intruders for 100, 200 and 300 nodes in an area of $100 \times 100)\,\mathrm{m}^2$.
(3) We send an unknown bit to all the nodes for their legal acknowledgement of identity

The leftover paper is paraphrased as follows: Section 2 discusses the related work. Section 3 discusses the system description, the proposed protocol is discussed in Sec. 4, the Result and discussion is done in Sec. 5, and the conclusion is discussed in Sec. 6.

2. Related Work

In (Onat and Miri, 2005) author proposed a protocol where the nodes know about the behaviour of other nodes, especially of their neighbours. They find and report inconsistencies in data to each other. The network has intelligent nodes that share the information to find any anomalies. The strange behaviour of neighbours is shared with other nodes that confirm the action taken against the attacker(s). In (Mourabit *et al.*, 2014) author proposed a protocol where four mobile agents are used to detect intruder (i) Collector Agent: It gathers the data, store it and give as input to the Misuse Detection Agent(MDA) (ii) MDA: With the use of pattern recognition

Misuse Detection Agent find the unknown behaviour of the network and report to the Anomaly Detection Agent (iii) Anomaly Detection Agent: Anomaly Detection Agent check the unknown behaviour of network to find intruder and report to the Alert agent (iv)Alert Agent: The Alert agent alerts the network from the intruder In (Kharat and Kharat, 2014) author proposed a protocol for intrusion detection. In this protocol, IR sensors and cameras make immediate awareness like the buzzer, SMS, or images to inform the security officers of the entrance of an intruder in the network area. In (Jisha *et al.*, 2010) author proposed a protocol that provides ease for the deployment of sensors, i.e., depending on the type of environment, and is not required continuous monitoring by a human. The author also discusses the suitable topology for intrusion detection. In (Acharya and Karuppayil, 2009) author proposed a protocol that uses an anomaly detection pattern. This pattern sets a baseline for normal traffic between nodes of WSN over a specified time interval. The system compares current traffic with the baseline traffic over the same time interval; after the comparison, the system determines whether a DoS attack occurs or not.

In (Liu and Yu, 2008), the author proposed a detection module with four Phases: (i) Self acquisition: In this phase neighbour's next hop to the sink is indicated by the beacon node. If no. of hops is greater than the estimated hope, a jamming condition arises (ii) Detector Generation: This phase distinguishes the attack from the normal behaviour of a node. (iii) Detection: If the node's behaviour is different from normal behaviour and it detects malicious activity from the neighbour's node, the system triggers an alarm. (iv) Clonal Selection: This phase activates detectors quickly; thus, attacking can detect very fast. In (Chen *et al.*, 2007), the author proposed a lightweight anomaly detection protocol that investigates different main characteristics and rules for WSNs to make an efficient, accurate, and effective system that detects intruders. The author also proposes a moving window function approach to collect the data activities. Cooperation among monitor nodes is not required in the model. In (Marti *et al.*, 2000) author proposed a protocol where the node observes its neighbours and monitors its activities, such as delays in the message and replicates of data that detects an intruder in the network. This protocol can also detect DoS in WSNs. In (Yu and Xiao, 2006) author proposed a protocol that detects selective attacks in WSN based on the multihop acknowledgement technique. In this model, the alarm starts whenever abnormal packet loss occurs and is reported by intermediate nodes to other normal nodes. In (Pires *et al.*, 2004), the author proposed a protocol that compares a receive signal power with observed signal power in the WSN. The difference in the power of signals detects the wormhole and hello flood attack. In (Mishra *et al.*, 2015) author proposed a protocol that focuses on the energy-efficient coverage and connectivity of the network with the minimum number of active nodes. The proposed model has connectivity even in the less communication range.

In (Cardei and Du, 2005) author proposes a protocol that divides the available nodes set into different disjoint sets, and each set covers the entire target in different rounds. This technique improves the performance of the network for an extended period. In (Chaturvedi and Daniel, 2020) author proposed a protocol with rounds that consist of three phases. The first is the Setup phase which determines the requirement of an optimum number of nodes for target coverage. The second is the sensing phase selects the leader node on the basis of residual energy and distance parameters. Transmission of data is done in the third phase as the transmission phase. In (Chaturvedi and Daniel, 2017) author proposed a protocol that uses optimized decision rules to find the number of active nodes by rough set theory. This approach improves network efficiency by minimizing the overhead of nodes. In (Li *et al.*, 2019), the author proposed a protocol that considers the problem in rechargeable WSNs. The network determines the least nodes required for quality coverage for one or more targets. The problem is formulated as an ILP for a small scale target, GRNP, and Target Protection Node Placement (TPNP) approach for a large scale.

In ILP, rechargeable nodes are placed in cells such that targets are covered properly. In GRNP, fractional nodes are required in cell co-ordinate m, n to cover the cell. In TPNP, only sufficient nodes are placed around the target to satisfy the coverage. In (Ammari and Das, 2006), the author introduced a protocol that analyzes k-covered WSN to find the relationship between coverage and connectivity. The target is monitored by at least k-sensors. Connectivity of network for k target is measured in terms of sensing range of the node. In (Commuri and Watfa, 2006), the author introduced a protocol that optimizes the minimum number of nodes and their placements to determine the complete coverage of a three-dimension network. Sensors are distributed randomly and resolve the problem of selecting a minimum subset of the sensor network.

In (Kim *et al.*, 2010), author introduced a directional sensor network that extends the network lifetime by transmitting the information in each cover set to the base station. It uses a scheduling technique to solve the overlapping target problem. In (Zishan *et al.*, 2018), author proposed a protocol in which targets have predefined requirements for coverage. The authors proposed inter quadratic programming formula to minimize the Euclidian distance between the resultant covered vector and those needed. In (Yu *et al.*, 2015) author introduced a protocol with circumstances where an intruder can demolish any sensor. The author derives the probability for the single sensor and multi-sensor detection models to find the intrude detection zone. In (Guan *et al.*, 2018), the author considers a game model for intrusion detection in WSNs. This model considers the interaction between the normal node and malicious node as two players. Player 1 considers for the malicious node having m possible action strategies for objective r1, and player 2 consider as a normal node with n possible action strategies for objective r2. The final decision for each player gets the objective vector (r1 or r2). In (Mekelleche *etal.*, 2018), the author introduced a protocol that focuses on intrusion detection in WSNs. The author categorizes the intruder detection technique into two classes: signature-based IDS and anomaly-based IDS. Signatures-based IDS use rule-based IDS that analyze the data collected from nodes and compare it with the signature database to identify the attack signature. Anomaly-based IDS checks the system's normal behaviour and detects the intruder from deviation in the behaviour of the network. In (Silva *et al.*, 2005), the author introduced a protocol that deploys some monitors nodes in the network. These monitoring nodes analyze the messages in the network area. Monitoring is done in three phases: the Data acquisition phase, where the monitoring node collects the data from normal nodes. Rule application phase where rules are applied to the collected data and intrusion detection phase or decision phase that detects the intruder after rule application phase. In (Culpepper and Tseng, 2004) author proposed a model that finds out malicious nodes that try to receive the packet from the network. This approach has two phases: The first phase finds out the list of suspicious nodes, and in the second phase BS considers the area with the malicious node as a potential attack zone.

In (Roman *et al.*, 2006), the author proposes an architecture where each node acts as an agent for intrusion detection. The agents are categorized into two classes: first is the Local agent that monitors the local activities of the node, i.e., the information sent and received by the nodes. The second is the Global agent that communication with the neighbour node. In (Chellaian, 2015), the author introduces a protocol that detects Sybil attacks. In Sybil, attack intruders create multiple identities of other nodes. Sybil attack detected through time to time module is applied. This module maintains an observation table to identify the id and position of the node. In (Narayan and Daniel, 2021), the author introduces an energy-efficient protocol by considering two parameters, i.e., residual energy and distance of a node from the BS. The efficient CH selection depends upon the maximum residual energy and minimum distance from the BS that improves the network's lifetime. In (Kim *et al.*, 2010), the author introduces a protocol that focuses on the tracking and monitoring of intruders. To detect the location of the intruder, a binary detection sensing mechanism is used. The sensors are deployed in a grid manner to validate their location. In (Liu *et al.*, 2022) author introduced a protocol using the KNN algorithm that detects the distance of intruder when WSN encounters a DoS attack. A technique was proposed in (M V. and Malladi, 2021) that detects malicious zones and malicious nodes when they are entering a network. For the purpose of locating the intruder, the overhearing rate of all nodes in each zone is determined. In (Rajesh and Sangeetha, 2021) proposed a protocol that uses the AODV algorithm as a routing protocol to detect intrusion in WSNs. In this protocol, routing only takes place in response to requests; for instance, when a source node wants to transmit a packet to a destination, it broadcasts a route request message to the network. In (Boni *et al.*, 2020), a new approach to WSN security has been proposed. Sensors are incorporated into the intrusion detection system in this case. This new IDS device computes the algorithms required to locate and distinguish between an intruder and an authentic node. It creates a virtual compound around the sensors to process all the data they receive. Both of these processes operate together to maintain the network isolated by recording all sensors and verifying their authenticity in order to avoid service interruptions. An additional enhancement to this isolation strategy is the use of feedback signals to warn other sensors in the network about a defective one so that they can stop communicating with it. In (Zhang and Xiao, 2019) proposed protocol based on spatial division, an improved negative selection algorithm has been developed. In real value space, an algorithm evaluates the dispensation of own selves and then divides it into many subspaces. In these subspaces, selves are allocated and the NSA is applied to the space. Only the randomly generated candidate detector can cope with the selves in the sub space with the detector and not all the sub spaces. This operation speeds up the detection of antigens. All parameters required for a better intrusion detection system show good results when this algorithm's efficiency is tested theoretically and experimentally. In (Li *et al.*, 2018) proposed a intrusion detection based on Danger Theory, with the help of a multimode system to detect intrusions. Projection Pursuit Algorithm is used here for danger detection and traffic management. It also makes use of the Extreme Learning Machine algorithm and the Beta distribution to determine how much the nodes trust one another. When it comes to false positive and false negative rates, the danger theory used here outperforms the SNs model.

3. System Description

The proposed protocol is an energy-efficient model that identifies the network's intruder. For energy efficiency, the proposed protocol considers a two-parameter, i.e., residual energy and distance of a node from BS, for the selection of Cluster Head (CH). The nodes that have residual energy more than the threshold energy and their distance from the base station is minimum can participate in the election of CH.

Assume that static sensor nodes are uniformly deployed in Region Y, as shown in Fig. 2.

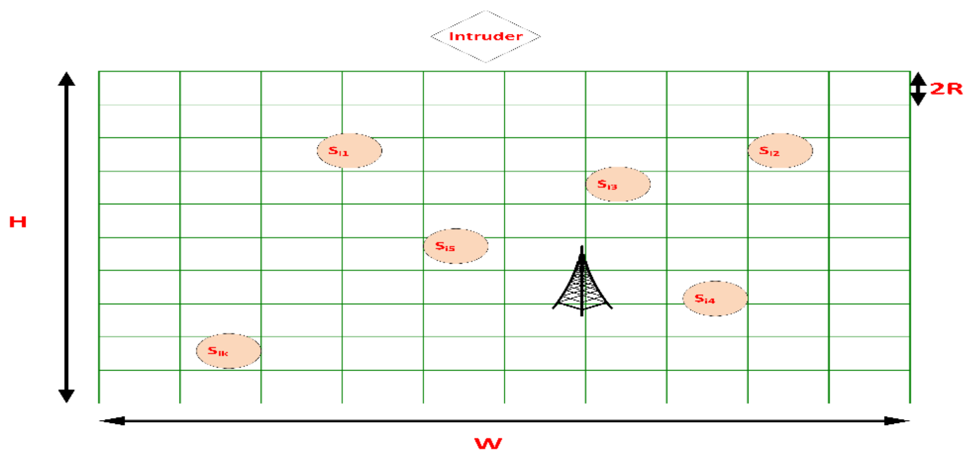

Fig. 2. Intruder detection with grid system.

An intruder's goal is to cross the parallel boundary of region Y. If the legitimate node enters the sensing range of the sensors, the intrusion is said to be detected. As a result, if at least k sensors detect an intruder along its crossing path, a Multiple Sensor Region (MSN) is considered a k-barrier covered.

To determine the likelihood of k-barrier coverage for intruder detection, the following assumptions are made.

(1) A square grid with each side having a length of 2R. (with sensing radius R of the node). At any given time, just one sensor can seem to be inside one specific grid, based on whether the sensor's centroid falls within this grid.
(2) R $\ll$ W and R $\ll$ H (W is the width of region Y, and H is the height of region Y) show the size of the belt region, which is much larger than the grid.
(3) We use the disc-based sensing method for computational tractability, which means a sensor can identify an intruder with probability 1 when the intruder is within its sensing range and with zero chance of a false report.

4. Proposed Protocol

The proposed protocol detects the intruder by identifying legal nodes that acknowledge the CH. CH sends an unknown bit to all the normal nodes in the cluster; only legal nodes know the unknown bits where they have to acknowledge their identity number to the CH. If CH receives incorrect acknowledge or no acknowledge from normal nodes, it will be an intruder.

The proposed protocol detects an intruder in the area of WSN. Nodes are deployed with two different densities. α of a node is deployed in the critical area where the intruder has the maximum chance of entry, and γ of a node is deployed in the less critical area where the intruder has less chance of entry. The cluster head identifies the area from which the intruder attacks the network. Cluster Head detects the intruder and informs the BS. BS deactivates the intruder.

In the proposed protocol, every node acts as a sensing node. The intruder can identify by a single sensor or multiple sensor nodes.

4.1. *Threshold density for intruder detection system*

In the proposed model, the probability of intruder detection depends on the threshold density of nodes in an area of WSNs. Threshold density for Intruder Detection is defined as

$$\left\{\begin{matrix} \dfrac{n}{x \times y} \geq T_a, P \geq T_p \\ else\ P < T_p \end{matrix}\right\} \tag{1}$$

where $n =$ No. of nodes
$x \times y =$ Area in m^2
$P =$ Probability for intruder detection

T_a = Threshold density
T_p = Threshold Probability

Threshold density depends upon the critical and less critical area for intruder entry.

4.2. *Probability density function for intruder detection*

The probability density function $f(x)$ for intruder detection

$$P(s \le x = t) = \int_s^t f(x)dx. \tag{2}$$

That must satisfy the condition

$$\begin{gathered} f(x) \ge \text{for all } x \\ \int_{-\infty}^{\infty} f(x)dx = 1. \end{gathered} \tag{3}$$

Where
P is the probability of intruder detection
s and t is the bound area for maximum probability

This is shown graphically in Fig. 3.

$$\begin{cases} P \ge m & s \le \text{area} \le t \\ P < m & s > \text{area} > t \end{cases} \tag{4}$$

Where m = threshold Probability for Intruder Detection

4.3. *Intruder detection*

Given parameter
N_A = Total no. of awake nodes in the network.

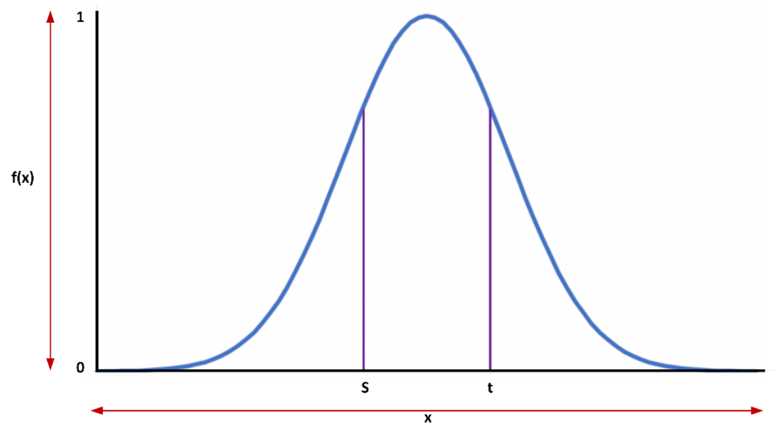

Fig. 3. Probability density function.

N_s = Total no. of sleep nodes in the network.
ETX = Data Transmission Energy
ERX = Data receiving Energy
T = Total energy consumption of network for transmission of data
R = Total energy consumption of network to receive the data

Energy consumption in the transmission and receiving of data in WSN verify the intruder attack using the following two conditions

4.3.1. *Based on the total energy consumption of the network for transmission of data*

$$\begin{cases} T = (N_A) \times (ETX), & \text{intruder} = \text{null} \\ T > (N_A) \times (ETX), & \text{intruder in the network} \end{cases} \tag{5}$$

4.3.2. *Based on the total energy consumption of the network to receive the data*

$$\begin{cases} R = (N_A) \times (ERX), & \text{intruder} = \text{null} \\ R > (N_A) \times (ERX), & \text{intruder in the network} \end{cases} \tag{6}$$

4.4. *Proposed protocol for intruder detection*

Algorithm:

Given parameter
Region R1 and Region R2 is the sensitive region for intruder entry; Region R3 is the less sensitive region for intruder entry, N= No. of sensor nodes deployed in a given area, P = Probability for Intruder Detection, m = Threshold probability, d = Node density, s = lower limit area bound t = upper limit area bound S_{ij} = Sensor id $(x \times y)$ m2 = Area for the deployment of nodes
Begin
/* Node deployment*/
α Sensor node S1j to S1k deploy in Region R1
β Sensor node S2j to S2k deploy in Region R2
γ Sensor node S3j to S3k deploy in Region R3
/* Intruder detection Probability*/
In Region Ri
BEGIN
DO WHILE Alive node= 0
: for (R1:R3)

```
Algorithm:
: If
:   (s/Ri) < = d ¡= (t/Ri)
:   P > = m
: else
:   P < m
: END
: END WHILE
: /* Intruder Detection*/
: In Region Ri
: DO WHILE Alive node = 0
: for (S1j : S1k)
:   Cluster Head Transmit a bit to each node known legality of node
:   Node response their id as an acknowledgement to Cluster head
: If
:     Sensors Node S1m not respond or transmit a wrong acknowledgement
:  THEN
: It is an intruder
: Else
:     Legal node
: END
: Else
:   Legal node
: End
: END WHILE
```

5. Result and Discussion

The simulation of the proposed protocol is done on MATLAB and validates the implementation of the proposed protocol. Simulation result for homogeneous WSN is performed for the area (100×100) m^2. Nodes $n = 100, 200$, and 300 deployed in the given area. The deployment of a node depends on the parameter used in Table 1.

5.1. *Experiments*

Experiment 1: This experiment proves the hypothesis that optimum node density can improve the area coverage. The simulation result compares the percentage of Area Covered by 100, 200, and 300 nodes, respectively, for an area of $(100 \times 100)\,\mathrm{m}^2$. Figure 4 shows the %age of the area covered in $(100 \times 100)\,\mathrm{m}^2$. One hundred nodes covered the area of 100% up to 2000 rounds, two hundred nodes covered 100% up to 3500 rounds, and three hundred nodes covered 100 % area up to 4000 rounds shown in Fig. 5. Comparison between 100, 200, and 300 nodes for Area Covered in 16000 round is shown in Table 2.

Table 1. Parameter for simulation.

Parameter	Specification
No. of nodes (x)	100/200/300
E_0	1.5J
E_{elec}	40*10 ∧ (−9) j
P_{opt}	0.1
Data Bits	4000 bits
X axis of BS	50 m
Y axis of BS	50 m
Transmission Energy (ETX)	40*10 ∧ (−9) j
Energy Consumption for data receiving (ERX)	40*10 ∧ (−9) j
EDA	40*10 ∧ (−9) j
Efs	20*10 ∧ (−12) j
Emp	.0013*10 ∧ (−12) j

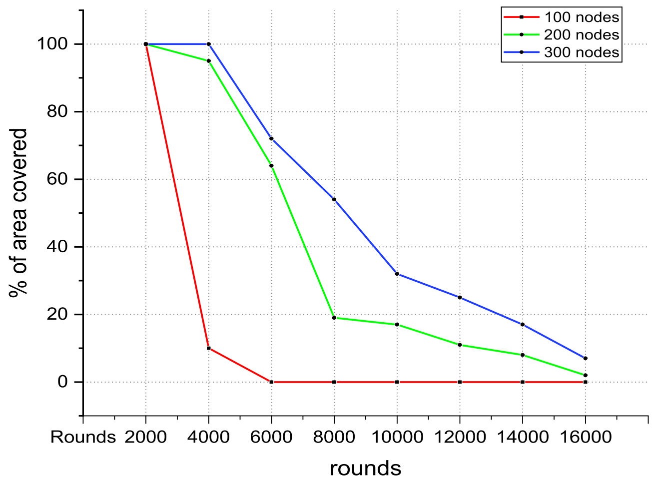

Fig. 4. % of the area covered in $(100 \times 100)\,\mathrm{m}^2$.

Experiment 2: The second experiment compares the probability of intruder detection on the deployment of 100, 200 and 300 nodes. The simulation result compares the probability of intrusion detection for 100, 200, and 300 nodes, respectively, for an area of $(100 \times 100)\,\mathrm{m}^2$. Probability of intruder detection for 100 nodes is 93%, 89% and 83% for 100 nodes in area of $(100 \times 100)\,\mathrm{m}^2$, $(200 \times 200)\,\mathrm{m}^2$ and $(300 \times 300)\,\mathrm{m}^2$ respectively, 95%, 95% and 89% for 200 nodes in area of $(100\times100)\,\mathrm{m}^2$, $(200\times200)\,\mathrm{m}^2$ and $(300 \times 300)\,\mathrm{m}^2$ respectively, 98%, 97%, and 96% for 300 nodes in the area of $(100\times100)\,\mathrm{m}^2$, $(200\times200)\,\mathrm{m}^2$, and $(300\times300)\,\mathrm{m}^2$ respectively as shown in Fig. 6. A comparison between 100, 200, and 300 nodes for the Probability of Intruder detection is shown in Table 3.

Experiment 3: Third Experiment compares the number of intruders detected on the deployment of 100, 200 and 300 nodes for 5, 10, and 15 intruders.

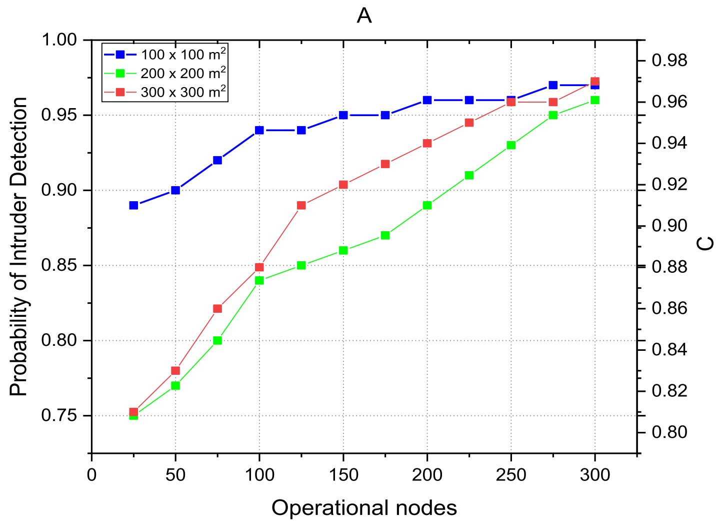

Fig. 5. Probability of intrusion detection (100, 200, and 300 nodes).

Table 2. Comparison between 100, 200, and 300 nodes for Area Covered in 16000 round.

Percentage of Area Covered			
	No. of Nodes		
	100	200	300
Rounds	% Area Covered	% Area Covered	% Area Covered
2000	100	100	100
4000	10	95	100
6000	00	64	72
8000	00	19	54
10000	00	17	32
12000	00	11	25
14000	00	8	17
16000	00	2	7

The simulation result for five intruders compares the number of intruders deactivated with the number of rounds. On the deployment of 100 nodes in an area of $(100 \times 100)\,\mathrm{m}^2$, all five intruders are deactivated in 500 rounds, whereas on the deployment of 200 and 300 nodes in an area of $(100 \times 100)\,\mathrm{m}^2$, all intruders are deactivated in 300 and 100 rounds, respectively as shown in Fig. 6.

The simulation result for ten intruders compares the number of intruders deactivated with the number of rounds. On deploying 100 nodes in an area of $(100 \times 100)\,\mathrm{m}^2$, all ten intruders are deactivated in 800 rounds. In contrast, on the deployment of 200 and 300 nodes in an area of $(100 \times 100)\,\mathrm{m}^2$, all intruders are deactivated in 600 and 200 rounds, respectively; on overall comparison between

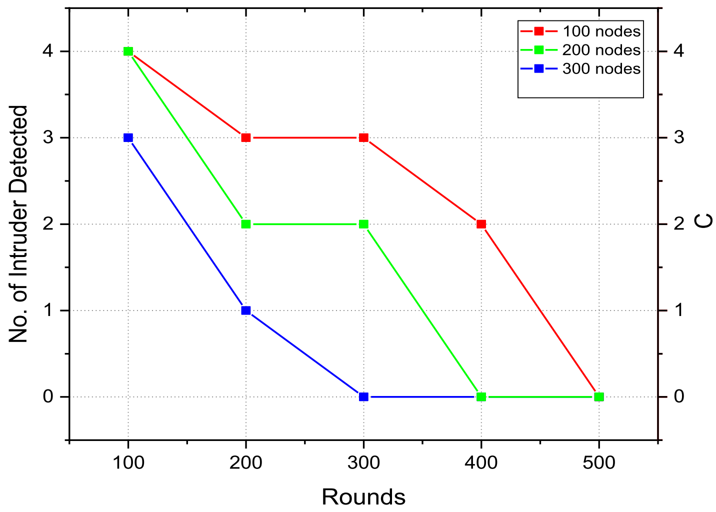

Fig. 6. Number of intruder detection for five intruders (100, 200, and 300 nodes)

Table 3. Comparison between 100, 200, and 300 nodes for Probability of Intruder detection.

Probability of Intruder detection			
	Area		
	$(100 \times 100)\,\mathrm{m}^2$	$(200 \times 200)\,\mathrm{m}^2$	$(300 \times 300)\,\mathrm{m}^2$
No. of operational nodes $(\alpha + \beta + \gamma)$	Probability %	Probability %	Probability %
25	89	81	75
50	90	83	77
75	92	86	80
100	94	88	84
125	94	91	85
150	95	92	86
175	95	93	87
200	96	94	89
225	96	95	91
250	96	96	93
275	97	96	95
300	97	97	96

100 and 200 nodes, the performance is better for 100 nodes up to the detection of nine intruders, i.e., detected in 500 rounds whereas for 200 nodes nine intruders are detected in 550 rounds as shown in Fig. 7.

The simulation result for 15 intruders compares the number of intruders deactivated with a number of rounds. On deploying 100 nodes in an area of $(100\times100)\,\mathrm{m}^2$, all 15 intruders are deactivated in 800 rounds. In contrast, on deploying 200 and 300 nodes, all intruders are deactivated in 800 and 100 rounds, respectively, as shown in

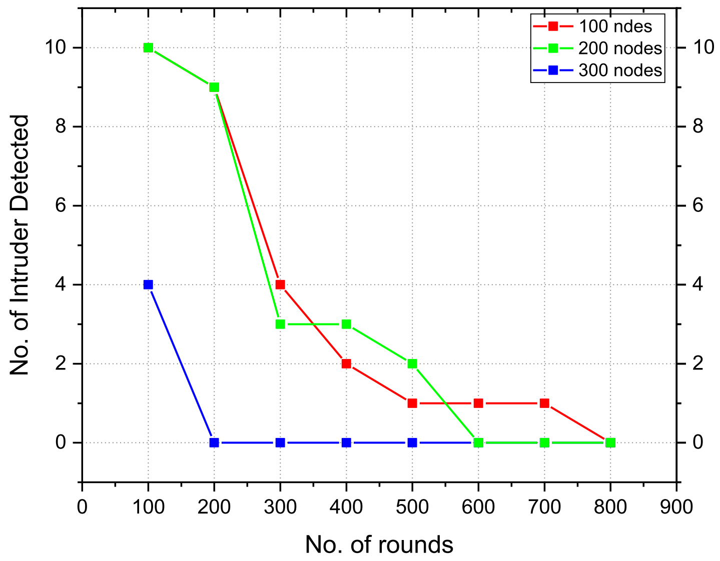

Fig. 7. Number of intruder detection or ten intruders (100, 200, and 300 nodes).

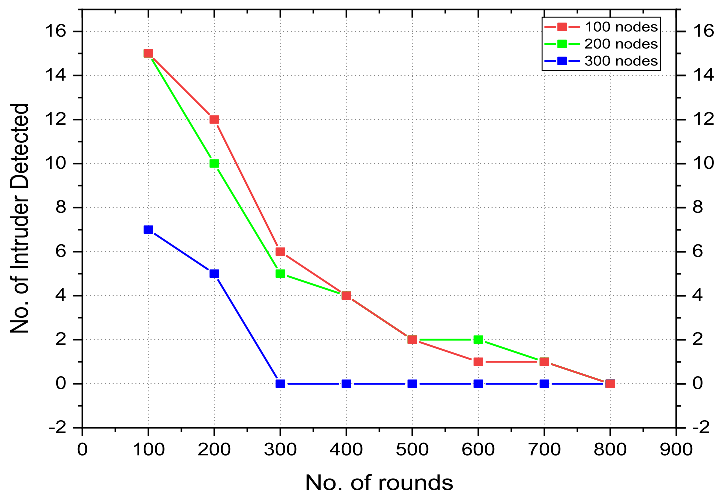

Fig. 8. Number of intruder detection or fifteen intruders (100, 200, and 300 nodes).

Fig. 8. Table 4, Table 5 and Table 6 shows the comparison between 100, 200, and 300 nodes for five, ten and fifteen intruders detection, respectively.

Experiment 4: Compares residual energy of the network on the deployment of 100, 200 and 300 nodes for 5, 10 and 15 intruders in 16000 rounds.

The simulation result compares the amount of residual energy up to 16000 rounds for 100, 200, and 300 nodes in an area of $(100 \times 100)\,\mathrm{m}^2$ for 5, as shown in Fig. 9.

The simulation result compares the amount of residual energy up to 16000 rounds for 100, 200, and 300 nodes in an area of $(100 \times 100)\,\mathrm{m}^2$ for 10, as shown in Fig. 10.

Table 4. Comparison between 100, 200, and 300 nodes for five intruders detection.

Total Intruder = 5			
	No. of Nodes		
	100	200	300
Rounds	Intruder alive	Intruder alive	Intruder alive
100	4	4	3
200	3	2	0
300	2	2	0
400	1	0	0
500	0	0	0

Table 5. Comparison between 100, 200, and 300 nodes for ten intruders detection.

Total Intruder = 10			
	No. of Nodes		
	100	200	300
Rounds	Intruder alive	Intruder alive	Intruder alive
100	10	10	4
200	9	9	0
300	4	3	0
400	2	3	0
500	1	2	0
600	1	0	0
700	1	0	0
800	0	0	0

Table 6. Comparison between 100, 200, and 300 nodes for fifteen intruders detection.

Total Intruder = 15			
	No. of Nodes		
	100	200	300
Rounds	Intruder alive	Intruder alive	Intruder alive
100	15	15	7
200	10	12	5
300	5	6	0
400	4	4	0
500	2	2	0
600	2	1	0
700	1	1	0
800	0	0	0

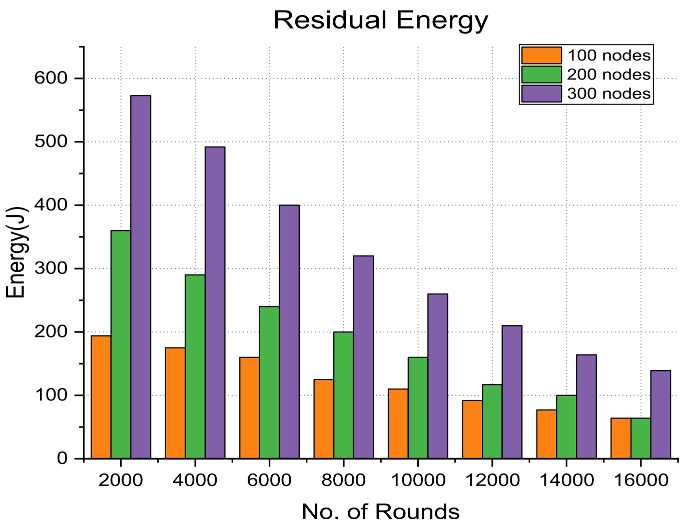

Fig. 9. Residual Energy of 100,200 and 300 nodes in area of $(100 \times 100)\,\text{m}^2$for five intruders.

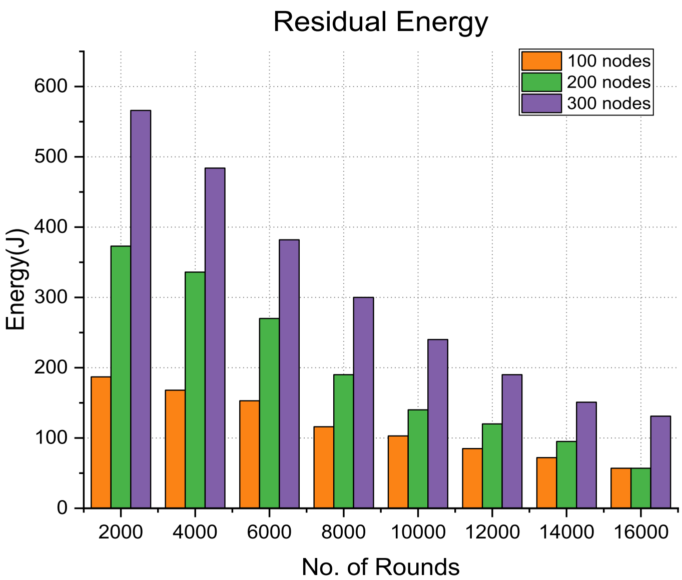

Fig. 10. Residual Energy of 100, 200 and 300 nodes in an area of $(100 \times 100)\,\text{m}^2$for 10 intruders.

The simulation result compares the amount of residual energy up to 16000 rounds for 100, 200, and 300 nodes in an area of $(100 \times 100)\,\text{m}^2$ for 15, as shown in Fig. 11.

Table 7, Table 8 and Table 9 shows the comparison between Residual Energy of 100, 200, and 300 nodes in 16000 rounds for five, ten and fifteen intruders detection, respectively.

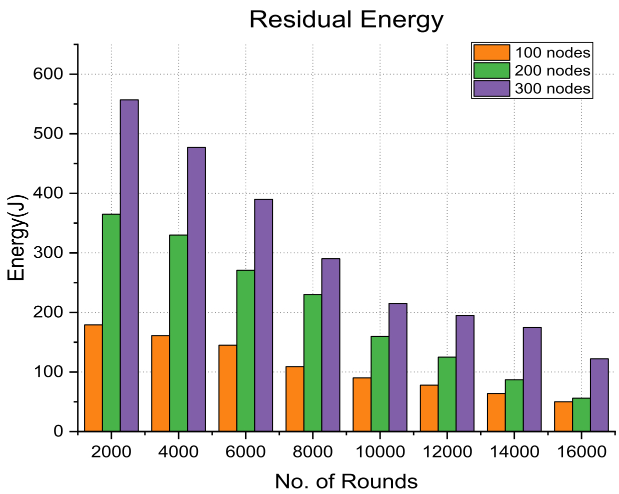

Fig. 11. Residual Energy in area of $(100 \times 100)\,\mathrm{m}^2$ for 15 intruders.

Table 7. Comparison between Residual Energy of 100, 200, and 300 nodes in 16000 rounds for five intruders detection.

Total Intruder = 5			
	No. of Nodes		
	100	200	300
Rounds	Residual Energy	Residual Energy	Residual Energy
2000	194	360	573
4000	175	290	492
6000	160	240	400
8000	125	200	320
10000	110	160	260
12000	92	117	210
14000	77	100	164
16000	64	64	139

Table 8. Comparison between Residual Energy of 100, 200, and 300 nodes in 16000 rounds for ten intruders detection.

Total Intruder = 10			
	No. of Nodes		
	100	200	300
Rounds	Residual Energy	Residual Energy	Residual Energy
2000	187	373	566
4000	168	336	484
6000	153	270	382
8000	116	190	300
10000	103	140	240
12000	85	120	190
14000	72	95	151
16000	57	57	131

Table 9. Residual Energy of 100, 200, and 300 nodes in 16000 rounds for 15 intruders detection.

Total Intruder =15			
	No. of Nodes		
	100	200	300
Rounds	Residu Energy	Residual Energy	Residual Energy
2000	179	365	557
4000	161	330	477
6000	145	271	390
8000	109	230	290
10000	90	160	215
12000	78	125	195
14000	64	87	175
16000	50	56	122

6. Conclusion

In WSN, the proposed protocol detects the intruder without the addition of any monitoring nodes. The legal nodes show their identity to the BS by sending an acknowledgement. The simulation for 5, 10, and 15 intruders in areas of $(100 \times 100)\,\mathrm{m}^2$, for 100, 200, and 300 nodes, respectively, show the number of rounds required to detect intruders. In the overall process, the residual energy is optimized by detecting and deactivating the network intruders. As a result, creating a network with the different densities of nodes can also reduce energy usage and increase network longevity. The simulation results show that using various node densities might boost intruder detection. CH plays a vital role in detecting intruders to protect data confidentiality and integrity. In the future, the simulation experiment on mobile sensor nodes will be performed, and different parameters like communication quality of node, sleep, and awake concept will be included.

References

Acharya, R. and Karuppayil, A. (2009) ‘Data integrity and intrusion detection in Wireless Sensor Networks’, in, pp. 1–5. Available at: https://doi.org/10.1109/ICON.2008.4772642.

Ammari, H.M. and Das, S.K. (2006) ‘Coverage, connectivity, and fault tolerance measures of wireless sensor networks’, in *Symposium on Self-Stabilizing Systems*, pp. 35–49.

Boni, K. R. C. *et al.* (2020) ‘A Security Concept Based on Scaler Distribution of a Novel Intrusion Detection Device for Wireless Sensor Networks in a Smart Environment’, *Sensors* (*Basel*, *Switzerland*), 20.

Cardei, M. and Du, D.-Z. (2005) ‘Improving Wireless Sensor Network Lifetime through Power Aware Organization’, *Wireless Networks*, 11, pp. 333–340. Available at: https://doi.org/10.1007/s11276-005-6615-6.

REFERENCES

Chaturvedi, Pooja and Daniel, A.K. (2020) 'Energy Efficient Communication Framework for Target Coverage using Trust Concepts', *International Journal of Engineering and Advanced Technology (IJEAT)*, pp. 247–257.

Chaturvedi, P. and Daniel, A. K. (2017) 'Trust aware node scheduling protocol for target coverage using rough set theory', in 2017 *International Conference on Intelligent Computing, Instrumentation and Control Technologies* (*ICICICT*), pp. 511–514. Available at: https://doi.org/10.1109/ICICICT1.2017.8342615.

Chellaian, G. (2015) 'Detection of SYBIL Attack using Neighbour Nodes in Static WSN', *International Journal on Recent and Innovation Trends in Computing and Communication*, 3, pp. 2428–2432. Available at: https://doi.org/10.17762/ijritcc2321-8169.1504140.

Chen, H. *et al.* (2007) 'Lightweight Anomaly Intrusion Detection in Wireless Sensor Networks', in *PAISI*, pp. 105–116. Available at: https://doi.org/10.1007/978-3-540-71549-8_9.

Commuri, S. and Watfa, M.K. (2006) 'Coverage strategies in wireless sensor networks', *International Journal of Distributed Sensor Networks*, 2(4), pp. 333–353.

Culpepper, B. J. and Tseng, H. C. (2004) 'Sinkhole intrusion indicators in DSR MANETs', in *First International Conference on Broadband Networks*, pp. 681–688. Available at: https://doi.org/10.1109/BROADNETS.2004.77.

Dwivedi, R. and Kumar, R. (2020) 'An Energy and Fault Aware Mechanism of Wireless Sensor Networks Using Multiple Mobile Agents', *International Journal of Distributed Systems and Technologies*, 11, pp. 22–41. Available at: https://doi.org/10.4018/IJDST.2020070102.

Guan, S. *et al.* (2018) 'Intrusion detection for wireless sensor networks: A multi-criteria game approach', in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6. Available at: https://doi.org/10.1109/WCNC.2018.8377427.

Jisha, R. C., Ramesh, M. V and Lekshmi, G. S. (2010) 'Intruder tracking using wireless sensor network', in 2010 *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1–5. Available at: https://doi.org/10.1109/ICCIC.2010.5705799.

Kharat, P. and Kharat, J. (2014) 'Wireless Intrusion Detection System Using Wireless Sensor Network: A Conceptual Framework', *International Journal of Electronics and Electrical Engineering*, pp. 80–84.

Kim, Y. *et al.* (2010) 'Lifetime maximization considering connectivity and overlapped targets in wireless sensor networks', in 2010 2*nd International Conference on Information Technology Convergence and Services*, pp. 1–6.

Li, L., Sun, L. and Wang, G. (2018) 'An Intrusion Detection Model Based on Danger Theory for Wireless Sensor Networks.', *International Journal of Online Engineering*, 14(9).

Liu, Y. *et al.* (2019) 'Nodes Deployment for Coverage in Rechargeable Wireless Sensor Networks', *IEEE Transactions on Vehicular Technology*, 68(6), pp. 6064–6073. Available at: https://doi.org/10.1109/TVT.2019.2912188.

Liu, Y. and Yu, F. (2008) 'Immunity-based intrusion detection for wireless sensor networks', in 2008 *IEEE International Joint Conference on Neural Networks* (*IEEE World Congress on Computational Intelligence*), pp. 439–444. Available at: https://doi.org/10.1109/IJCNN.2008.4633829.

M, V. and Malladi, S. (2021) 'Secure Intruder Information Sharing in Wireless Sensor Network for Attack Resilient Routing', *International Journal of Advanced Computer Science and Applications*, 12. Available at: https://doi.org/10.14569/IJACSA.2021.0120263.

Marti, S. *et al.* (2000) 'Mitigating Routing Misbehavior in Mobile Ad Hoc Networks', *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM* [Preprint]. Available at: https://doi.org/10.1145/345910.345955.

Mekelleche, F., Hafid and OuldBouamam, B. (2018) 'Monitoring of Wireless Sensor Networks: Analysis of Intrusion Detection Systems', in 2018 5*th International Conference on Control*, *Decision and Information Technologies* (*CoDIT*), pp. 421–426. Available at: https://doi.org/10.1109/CoDIT.2018.8394844.

Mishra, T. *et al.* (2015) 'Energy Efficient Coverage and Connectivity with Varying Energy Level in WSN', in 2015 *International Conference on Computational Intelligence and Networks*, pp. 86–91. Available at: https://doi.org/10.1109/CINE.2015.26.

Mourabit, Y. E. L. *et al.* (2014) 'Intrusion detection system in Wireless Sensor Network based on mobile agent', in 2014 *Second World Conference on Complex Systems* (*WCCS*), pp. 248–251.

Narayan, V. and Daniel, A. K. (2020) 'Multi-Tier Cluster Based Smart Farming Using Wireless Sensor Network', in 2020 5*th International Conference on Computing*, *Communication and Security* (*ICCCS*), pp. 1–5.

Narayan, V. and Daniel, A. K. (2021a) 'IOT Based Sensor Monitoring System for Smart Complex and Shopping Malls', in *International Conference on Mobile Networks and Management*, pp. 344–354.

Narayan, V. and Daniel, A. K. (2021b) 'RBCHS: Region-Based Cluster Head Selection Protocol in Wireless Sensor Network', in, pp. 863–869. doi: 10.1007/978-981-33-6307-6_89.

Narayan, V. and Daniel, A. K. (2022) 'CHHP: coverage optimization and hole healing protocol using sleep and wake-up concept for wireless sensor network', *International Journal of System Assurance Engineering and Management*. Springer, pp. 1–11.

Narayan, V. and Daniel, A. K. (2021) 'A novel approach for cluster head selection using trust function in WSN'.

REFERENCES

Onat, I. and Miri, A. (2005) 'An intrusion detection system for wireless sensor networks', in *WiMob*'2005), *IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005.*, pp. 253–259 Vol. 3. Available at: https://doi.org/10.1109/WIMOB.2005.1512911.

Pires, W. R. *et al.* (2004) 'Malicious node detection in wireless sensor networks', in 18*th International Parallel and Distributed Processing Symposium*, 2004*. Proceedings.*, pp. 24-. Available at: https://doi.org/10.1109/IPDPS.2004.1302934.

Rajesh, S. and Sangeetha, M. (2021) 'Intrusion Detection In Wsn Using Modified AODV Algorithm', in. EAI. Available at: https://doi.org/10.4108/eai.7-6-2021.2308629.

Roman, R., Zhou, J. and Lopez, J. (2006) 'Applying intrusion detection systems to wireless sensor networks', in *CCNC* 2006*.* 2006 3*rd IEEE Consumer Communications and Networking Conference*, 2006., pp. 640–644. Available at: https://doi.org/10.1109/CCNC.2006.1593102.

Sharma, D., Kumar, V. and Kumar, R. (2016) 'Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET', in, pp. 475–485. Available at: https://doi.org/10.1007/978-81-322-2731-1_45.

Silva, A. P. *et al.* (2005) 'Decentralized intrusion detection in wireless sensor networks', in, pp. 16–23. Available at: https://doi.org/10.1145/1089761.1089765.

Yu, B. and Xiao, B. (2006) 'Detecting selective forwarding attacks in wireless sensor networks', in *Proceedings* 20*th IEEE International Parallel Distributed Processing Symposium*, pp. 8 pp.-. Available at: https://doi.org/10.1109/IPDPS.2006.1639675.

Yu, Q., Luo, Z. and Min, P. (2015) 'Intrusion detection in wireless sensor networks for destructive intruders', in 2015 *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, pp. 68–75.

Zhang, R. and Xiao, X. (2019) 'Intrusion detection in wireless sensor networks with an improved NSA based on space division', *Journal of Sensors*, 2019.

Zishan, A. Al *et al.* (2018) 'Maximizing heterogeneous coverage in over and under provisioned visual sensor networks', *J. Netw. Comput. Appl.*, 124, pp. 44–62.