ASEAN Engineering Journal

Full Paper

TRAP BASED ANOMALY DETECTION MECHANISM FOR WIRELESS SENSOR NETWORK

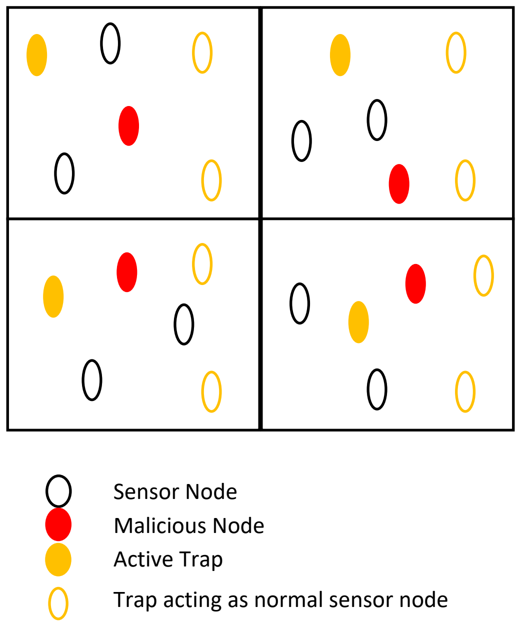
Deviprasad Mishra[a]*, Partha Roy[a], Anil Mishra[b]

[a]Computer Science & Engineering, BIT Durg, Chhattisgarh, India
[b]Electronics & Telecommunication Engineering, BIT Durg, Chhattisgarh, India

Article history
Received
20 August 2023
Received in revised form
13 December 2023
Accepted
14 December 2023
Published online
31 May 2024

*Deviprasad Mishra
dpmishra@bitdurg.ac.in

Graphical abstract



Abstract

A Wireless Sensor Network (WSN) comprises compact, resource-limited devices strategically placed for data collection and transmission, adapting seamlessly across diverse sectors and managing sensitive information. Security is pivotal in these applications, where compromised sensor nodes swiftly jeopardize network integrity, especially without robust security measures. Strategies addressing node compromise center on detecting false data from compromised nodes but often lack precision in tracing the exact source, hindering effective compromised node detection. This paper introduces an inventive anomaly-detection mechanism rooted in trap-based strategies, aiming to prevent sensor node compromise, ensure secure data aggregation, and sustain energy efficiency in WSNs. The trap system integrates deceptive nodes strategically to entice potential attackers, gathering essential attacker details and promptly alerting other network nodes. Consequently, the network excels in identifying attackers and thwarting node compromise, enhancing energy efficiency, network longevity, success rates, and data transmission. Additionally, this approach provides early warning mechanisms for swift attacker detection and attack-type identification, addressing vulnerabilities effectively. By deploying traps proactively, this innovative mechanism not only safeguards against compromises but also fortifies the network's resilience and performance. This proactive strategy aligns with energy efficiency goals in WSNs, elevating the network's security significantly while advancing efficiency across sensitive data domains in sensor network infrastructure.

Keywords: Security; Integrity; Attacker; type of attack; IDS.

1.0 INTRODUCTION

Wireless sensor nodes encompass essential components such as microcontrollers, transceivers, external memory, and battery power sources. These nodes are strategically deployed in specific terrains within a Sensor Network to sense and transmit diverse parameters to a central sink node[1]. The wireless sensor network serves various purposes, including agriculture, smart homes, automation, traffic management, environmental monitoring, disaster detection, and military applications. Each individual sensor node possesses the capability to sense, process, and communicate[2] desired information to an aggregator or the sink node

Data aggregation involves consolidating data from multiple sensors to eliminate redundancy and unnecessary information, thereby delivering cohesive insights to the Base Station (BS)[3]. During the transmission or communication process of nodes, there exists a potential for node compromise. We aim to introduce a trap node into the network, which can identify malicious activities or information from attackers and subsequently issue alerts to counteract node compromise. The proposed system does not provide a definitive solution but augments our understanding of hackers or attackers. This system, functioning as an early warning mechanism, enhances intrusion detection systems and aids in crafting improved security tools.

In a sensor network, the aggregator or sink node queries the sensor nodes to collect sensed data. Generally, each sensor node transmits its collected data to an intermediate node, which, in turn, forwards the data to the sink node for processing. Data aggregation aims to extend the network's lifespan by reducing the resource consumption of sensor nodes. Designing a well-structured data aggregation protocol[4] to ensure data accuracy, fault tolerance, latency, communication efficiency, and overhead proves to be a complex task. To achieve successful and effective data aggregation, the network must prevent node compromise, as compromised nodes could inject false data into the network, leading to significant challenges in maintaining secure data aggregation

1.1 Trap-based anomaly detection specific work

The approach encompasses two integral components: a distributed system and a centralized system. The distributed system operates on each node within a Wireless Sensor Network (WSN), with each sensor node hosting a version of this component. This component includes sensor applications, routing protocols, and more. Concurrently, a centralized system operates on the base station[5], which serves as a higher-level entity, enhancing the accuracy of compromise assessments and minimizing errors.

The network as a whole is partitioned into clusters[6], with each cluster housing a Low Interaction Trap. This Trap detects potential attackers and captures their activities. Subsequently, the Low Interaction Trap forwards the attacker's information to a High Interaction Trap functioning as a Remote Gateway. This gateway serves as a pivotal hub for collating all malicious activities[7]. Upon detection of an attack by the Low Interaction Trap, it can activate a trigger on the High Interaction Trap. This High Interaction Trap comprehensively investigates the attacker's actions and records them in log files.

In the context of the Roaming Trap technique, the location of the Trap remains concealed from potential attackers. Within the Sensor Network, the Roaming Trap employs unpredictability, constantly changing its location and adopting disguises. The network is subdivided into smaller virtual grid-like partitioned zones, with each zone hosting a single Trap. These Mobile Traps[8] must possess knowledge of their positions facilitated through a positioning system.

1.2 The Advantages Of The Trap-Based Mechanism Include:

- Fidelity: The mechanism deals with compact, valuable data sets.
- Innovative Tools and Strategies: It introduces novel approaches and techniques.
- Efficient Resource Usage: The mechanism does not demand significant resource allocation.
- Simplicity: It is characterized by its straightforward and uncomplicated nature.

1.3 Drawbacks of the Trap System:

- Risk Factors: The system carries inherent risks.
- Construction Complexity: The process of building and implementing the system can be intricate.
- Requirement for Expertise: Effective deployment necessitates a certain level of skill and expertise.
- Limited Perspective: The system's view or scope might be constrained.
- Indirect Vulnerable System Protection: It does not provide direct safeguarding for vulnerable systems.

2.0 METHODOLOGY

Our primary focus lies in the modeling of a regulation-centered, immensely interactive system as depicted in Figure 1. This system employs trap-based anomaly detection grounded in rule sets. We incorporate a mechanism for recognizing trap rotation variances utilizing roaming traps [9]. In contrast to the existing web spider-based defense mechanism, which exhibits reduced interactivity potentially leading to communication delays, our proposed technique employs highly interactive traps to expedite communication processes. When a trap sensor detects a relationship, it shortly suspends interactions with the impostor while concurrently updating the Central Authority (CA). Afterward, the Central Authority collects the data from the fraudulent node and activates the Anomaly Detection Module (ADM).

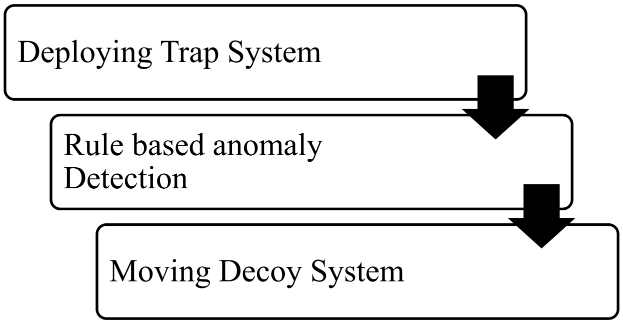


Figure 1 Implementation of Anomaly Detection with Traps Using Rule-Based Approach

2.1 Traps in Wireless Sensor Networks

Here, we delineate the process of utilizing wandering traps to identify malicious nodes[10] within a wireless sensor network. A trap, functioning as a vigilant monitoring tool, offers early insights to a system administrator concerning potentially malevolent activities occurring within the WSN. Notably, these traps exhibit heightened activity levels, facilitating quicker communication compared to existing methodologies. The radio range attributed to a trap mirrors that of other sensor nodes, as the standard sensor nodes periodically assume the role of traps. Employing wireless traps serves the purpose of amassing information about an imposter present within a WSN and generating various performance metrics for WSN.

Within a WSN context, a fraudulent node [11] can be simulated by a sensor node, which, in response to an intrusion, furnishes counterfeit data. This approach serves the purpose of both detecting the intruder and alerting the network administrator regarding the network's status.

The concept of luring intruders[12] has several applications based on sensor networks. The incorporation of a trap within a WSN has been proven feasible, as evidenced by its implementation in existing endeavors. Figure 2 offers a visual representation of a WSN, featuring several nodes alongside a limited number of traps. The observable scope of the trap, instrumental in detecting anomalies[13], is also depicted. Within this network, the traps are deliberately scattered.

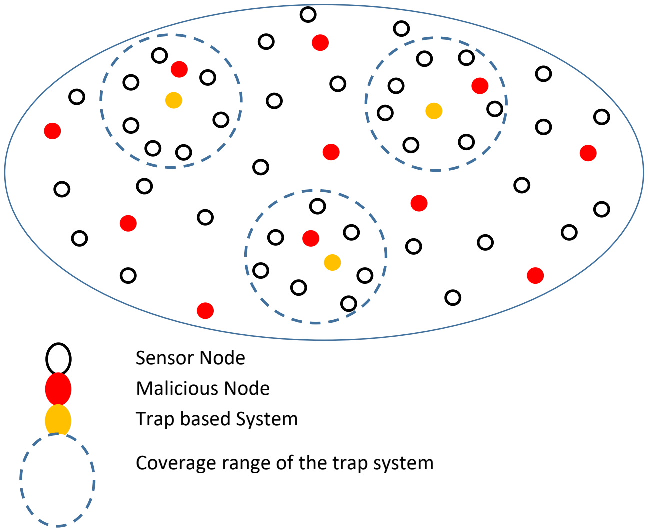


Figure 2 Deployment of Wireless Sensor Network (WSN) with Traps and Malicious Nodes

2.2 Deployment of Traps:

The subsequent algorithm outlines the procedure for deploying traps.

2.2.1 Algorithm 1

```
P1, P2, …,Pk Virtual Partition
T1, T2, …,Tk Traps
Ndi Node density of each Partition Pi.
Avg{Ndi}  Average density of nodes in all Partition.
Step 1. Virtually split sensor n/w in k smaller parts P1, P2,..Pk
Step 2. Deploy each trap Ti into each Pi, i = 1, 2, …, k.
Step 3. Ti estimates Ndi of Pi
Step 4. Check  Ndi> average {Ndi}, then
Step 5. Ti will be made active
Step 6. Otherwise
Step 7. Find Gj=Gi U Gi+1
Step 8. Check Ndj> Avg {Ndi}, then
Step 9. Ti will be made active
Step 10. otherwise
Step 11. i = i + 1
Step 12. Repeat Step 7
Step 13. End
```

At this stage, the entire sensor network is partitioned into smaller, parts or zones[14] to enhance manageability, with each zone hosting a single trap. Every trap calculates the node count within its designated region. Among the traps, those situated adjacent to the fewest nodes will function as regular nodes, while the remaining traps will assume dynamic roles. The determination of whether a trap operates as a trap or a standard node hinges on two factors: the zone with the typically lowest and the highest node density zones.

If the node density within a particular region surpasses the predefined threshold, the trap within that region will assume a dynamic role. Conversely, if the density falls below the threshold, the trap in that region will function as a standard node.

Before transitioning from functioning as a trap to assuming the role of a standard node, the trap must first cease fulfilling its current obligations of aiding malicious nodes[15]. The division of a WSN into regions is depicted in Figure 2. Each of these regions can be referred to as a grouping or cluster, and every sensor node enveloped by the cluster falls within the capture range of the corresponding trap. Consequently, whenever an imposter or a novel connection infiltrates a cluster, the trap verifies the intrusion.

Traps that transform into standard sensor nodes based on the expiry of the timer value are depicted in Table 2. The process of anomaly detection depends on predefined rules that classify data instances as anomalies or normal occurrences. During network observation, these rules are judiciously selected and applied to the incoming data packets. The delineation of rules for anomaly detection is presented in Table 1.

The recognition of anomalies executed within a cluster is established via the cluster formation protocol. Following this, a cluster head and coordinator are elected through a designated method[16]. The cluster head's responsibilities are allocated by the Anomaly[13] Detection and Localization Unit (ADLU). The procedure for detecting anomalies within new connections is outlined in Algorithm 2.

Anomaly Detection and Localization: The anomaly detection[14] mechanism employs pre-established rules to distinguish between data instances categorized as anomalies and those conforming to normal patterns. During network monitoring, these rules are judiciously selected and applied to the incoming data packets. The rules governing anomaly detection are presented in Table 1.

Table 1 Rules for Detecting Anomaly

Rules	Factor of Detection	Identified Intrusions
The tally (counter) is increased when a packet that requires forwarding is not forwarded for any given reason. An alarm is activated once the counter value exceeds a predetermined threshold.	Packet lost or dropped ratio	Selective forwarding and black hole attacks are subjects of concern.
An alarm is initiated when a packet originates from a node situated beyond the radio range of a single hop.	The source address of the packet	Hello flood, sinkhole as well as Sybil attack
An alarm is triggered when the distance measurements between multiple nodes coincide.	The factor for distance matching	Sybil attack

Detection of anomalies occurs within a cluster, formed through the cluster development protocol. Subsequently, the selection of a cluster head and coordinator is carried out via an election process. The allocation of responsibilities for the cluster head[15] is managed by the Anomaly Detection and Localization Unit (ADLU)[16]. The procedure for recognizing variances in novel associations is outlined in the algorithmic framework in algorithm 2

2.2.2 Algorithm 2 for Detecting Variance in Novel Associations

Step 1: In the Wireless Sensor Network (WSN), a limited number of counterfeit sensor nodes, often with inadequate protection, are randomly positioned to act as traps for potential malicious nodes.

Step 2: The cluster formation protocol is utilized to establish groups of nodes within the network, guaranteeing the presence of at least one trap in each cluster. As a result, every node in the network is enclosed by at least one trap.
Step 3: The trap in the network actively disseminates fabricated data to all additional nodes within the network.

Step 4: Whenever a trap identifies multiple intruders or a specific connection, it promptly updates the Centralized Administrator (CA) with the relevant information.

Step 5: When a correlation request is received, the trap deliberately adds a delay to its response. This delay provides the network administrator with sufficient time to track the recent connection and collect relevant details about it.

Step 6: An Anomaly Detection Module (ADM) is recommended to validate the legitimacy of the new association.

Step 7: Upon receipt of a data packet from a novel correlation, the packet undergoes initial validation against predefined anomaly rules.

Step 8: If the data packet conforms to the rules characterizing an anomaly, the novel correlation is confirmed as an anomaly, triggering an alarm.

Step 9: Subsequently, the CA validates whether a user is a fraudulent entity or an invader, and takes appropriate action accordingly.

Step 10: Following an examination of the data packet stemming from the new correlation, and considering the varying rules, if the data packet adheres sufficiently to the rules defining a standard node, the CA designates it as a standard node.

2.3 Trap Rotation Mechanism

Each trap sensor is equipped with a timer schedule and can communicate with other trap sensors. The timer values for the traps within the network are outlined in Table 2. These timers determine the duration during which each sensor functions as a trap. Once the timer elapses, the sensor transitions to operating as a standard node, and a new node is designated as a trap. A Central Authority (CA) is established to communicate with the traps. The rotation pattern[17] of trap sensors is randomized for each cycle, effectively preventing intruders from predicting or detecting the presence of a trap sensor.

Table 2 Timer value of the Traps

Trap number	Time
1	30 s
2	20 s
3	15 s
4	5 s
5	10 s

3.0 RESULTS AND DISCUSSION

This study is executed within the Network Simulator 2.32 environment. Sensor nodes are distributed randomly across a 50 x 50 m^2 area of interest. All sensor nodes are uniformly equipped with identical hardware and transmission power. To demonstrate the effectiveness of the TBADT (Trap-Based Anomaly Detection Technique), the simulation results of the suggested protocol are compared side by side with those from the protocols known as the Web Spider-Based Defense Technique (WSBDT) and the Segment-Based Anomaly Detection Technique (SBDAT) [18].

Results drawn from a range of network scenarios conclusively demonstrate the superior performance of the RBADT algorithm in terms of latency, overhead, accuracy, and residual energy. The simulation data is analyzed by varying the number of rounds between 100 and 500. These outcomes are verified across diverse simulation topologies. The parameters employed in the simulation are systematically summarized in the following table.

Table 3 Simulation Parameters Configuration

Parameter	Value
Number of nodes	25,50,100,150 and 200
Area of deployment (m^2)	50 X 50
Simulation Time (s)	60
The initial energy of each node (J)	10 J
Data Rate (Kbps)	50
Traffic Source	CBR
Propagation Model	Two Ray Round
Amount of energy needed to transmit one bit of information (nJ/bit)	60
Amount of energy spent for Amplification in Free Space Propagation (pJ/bit/m^2)	10
Amount of energy spent for Amplification in Multi-Path Propagation (pJ/bit/m^4)	0.0013
Energy consumption for data aggregation (nJ/bit/signal)	5

3.1 Comparative Algorithm Performance Assessment

In this section, the performance outcomes of the developed TBADT protocol are juxtaposed with those of several other existing protocols, including WSBDT and SBDAT. These comparisons are drawn from simulation results. The evaluation metrics encompass recognition latency, recognition accuracy ratio, transparency of recognition, counterfeit positive rate, and average residual power[18]. The Web Spider-Based Defense Technique (WSBDT) is one of the protocols used for comparison. This technique is inspired by the predatory behavior of web spiders when capturing prey.

3.2 Discussion on Results Interpretation

The experimentation involves varying node counts at 25, 50, 100, 150, 200, 250, and 300 nodes while employing Constant Bit Rate (CBR) traffic. Within these node counts, 10% are designated as malicious nodes. The metrics under consideration include recognition latency, recognition accuracy ratio, transparency of recognition, counterfeit positive rate, and average residual power.

The measurement of detection accuracy [19] involves calculating the proportion of identified attacks relative to the sum of both identified and unnoticed attacks. Communication overhead is quantified as the proportion of the total communication overhead within a system utilizing the detection algorithm, in contrast to the system operating independently. Detection latency gauges the temporal gap experienced between the conclusion of computation and the effective detection of termination.

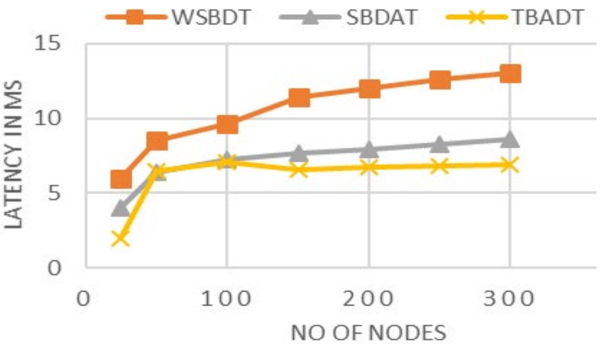


Figure 3 Comparison of TBADT with WSBDT & SBDAT

4.0 CONCLUSION

This study presents an enhanced approach for Wireless Sensor Networks (WSNs) through the integration of rotational traps. The initial step involves strategically deploying traps to ensure that each node within the network is enveloped by at least one trap's coverage. These traps then scrutinize incoming novel associations by engaging a centralized administrator. This administrator collects comprehensive information about these novel associations by suspending interactions among the involved nodes. Subsequently, predefined rules are applied to assess whether an incoming novel node conforms to an anomaly or follows regular patterns. The timing mechanism incorporated within each trap signifies when the trap's function as a detector concludes, at which point another sensor node is designated as a trap, and the previously active trap resumes operation as a standard sensor node.

The dynamic rotation of traps throughout the network renders it challenging for potential intruders to track these traps and subsequently disrupt the network's integrity. This method effectively manages the recognition of anomalies within a WSN.

For future research, the integration of various Quality of Service(QoS)[20]metrics could enhance performance analysis. Additionally, conducting comparative assessments with existing studies may yield more robust and insightful results.

Acknowledgement

The authors express sincere gratitude to Dr. Ramesh Kumar for his invaluable cooperation and insights, which significantly enhanced the execution of this study. His support played a pivotal role in the study's success, enriching its findings and contribution.

References

[1] F. S. Cohen, J. C. De Oliveira, and E. Taslidere.2006., “Locating hot nodes and data routing for efficient decision fusion in sensor networks,” *Ad Hoc Networks*, 4(3): 416–430, doi: 10.1016/j.adhoc.2004.11.001.

[2] D. P. Mishra and R. Kumar, 2015.,“A Vision of Hybrid Security Framework for Wireless Sensor Network Engineering,” *Indian Journal of applied Research*, 167(1): 2249–555.

[3] R. Di Pietro, L. V. Mancini, and S. Jajodia,2003., “Providing secrecy in key management protocols for large wireless sensors networks,” *Ad Hoc Networks*, 1(4): 455–468, doi: 10.1016/S1570-8705(03)00046-5.

[4] P. Sharma and P. Bhadana,2010., “An Effective Approach for Providing Anonymity in Wireless Sensor Network: Detecting Attacks and Security Measures,” *International Journal of Computer Science Engineering*, 02(05): 1830–1835.

[5] M. Bohio and A. Miri,2004., “Efficient identity-based security schemes for ad hoc network routing protocols,” *Ad Hoc Networks*, 2(3): 309–317, doi: 10.1016/j.adhoc.2004.03.011.

[6] H. Qu,2017., “An Adaptive Intrusion Detection Method for Wireless Sensor Networks,” *International Journal of Advanced Computer Science and Applications*, 8(11): 27–36.

[7] K. Akkaya, M. Younis, and M. Bangad,2005 “Sink repositioning for enhanced performance in wireless sensor networks,” *Computer Networks*, 49(4):512-534, doi: 10.1016/j.comnet.2005.01.014.

[8] S. M. Mohamed, H. S. Hamza, and I. A. Saroit,2017., “Coverage in mobile wireless sensor networks (M-WSN): A survey,” *Computer Communication.*, 110:133–150, doi: 10.1016/j.comcom.2017.06.010.

[9] S. Shamsh,2013., “Roaming Honeypots along with IDS in Mobile Ad-Hoc Networks,” International Journal of Computer Applications, 69(23): 14–21.

[10] N. Marchang and R. Datta,2008., “Collaborative techniques for intrusion detection in mobile ad-hoc networks,” Ad Hoc Networks, 6: 508–523, doi: 10.1016/j.adhoc.2007.04.003.

[11] [11] Y. C. Hu, D. B. Johnson, and A. Perrig,2003., “SEAD: Secure efficient distance vector routing for mobile wireless ad-hoc networks,” *Ad Hoc Networks*, 1(1):175–192, doi: 10.1016/S1570-8705(03)00019-2.

[12] Y. Y. Li and L. E. Parker,2008, “Intruder detection using a wireless sensor network with an intelligent mobile robot response,” *Conference Proceedings - IEEE Southeastcon*, 37–42, doi: 10.1109/SECON.2008.4494250.

[13] Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, 2015, “A global hybrid intrusion detection system for Wireless Sensor Networks,” *Procedia Computer Science.*, 52(1):1047–1052, doi: 10.1016/j.procs.2015.05.108.

[14] S. Shakkottai, R. Srikant, and N. B. Shroff,2015 “Unreliable sensor grids: Coverage, connectivity and diameter,” *Ad Hoc Networks*, 3(6):702–716, doi: 10.1016/j.adhoc.2004.02.001.

[15] T. A. Zia and A. Y. Zoma Zia, Tanveer & Zomaya, 2011, "A Lightweight Security Framework for Wireless Sensor Networks," Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications., 2(3): 53–73.

[16] R. K. Ghosh, V. Garg, M. S. Meitei, S. Raman, A. Kumar, and N. Tewari,2006, “Dense cluster gateway based routing protocol for multi-hop mobile ad hoc networks,” *Ad Hoc Networks*, 4(2):168–185, doi: 10.1016/j.adhoc.2004.04.011.

[17] Y. Yi, M. Gerla, and K. Obraczka,2004, “Scalable team multicast in wireless ad hoc networks exploiting coordinated motion,” *Ad Hoc Networks*, 2(2):171–184, doi: 10.1016/S1570-8705(03)00053-2.

[18] D. P. Mishra and R. Kumar, 2019, “Hybrid Sink Repositioning Mechanism For Wireless Sensor Network,” *International Journal of Research in Advent Technology.*, 7(3): 1442–1447.

[19] C. Madhusudhanarao,2018, “Flow Sampling for Network Intrusion Detection – An Acceptance Sampling Approach,” International Journal of Applied Engineering Research, 13(13):11030–11033.

[20] M. Li, H. Zhu, and I. Chlamtac,2006, “End-to-end QoS framework for heterogeneous wired-cum-wireless networks,”, *Wireless Networks*, 12(4): 439–450, doi: 10.1007/s11276-006-6544-z.