INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Sinkhole Detection Using Probe Route Mechanism (SDPRM) For Internet of Things

C Linda Hepsiba[1]*, **R Jemima Priyadarsini**[2]

1 Assistant Professor, Department of Computer Science,, Bishop Heber College, Affiliated with Bharathidasan University, Trichy17, Tamilnadu, India
2 Associate Professor, Department of Computer Science, Bishop Heber College, Affiliated with Bharathidasan University, Trichy17, Tamilnadu, India

OPEN ACCESS

Received: 31-05-2022
Accepted: 01-09-2022
Published: 14-10-2022

Citation: Linda Hepsiba C, Priyadarsini RJ (2022) Sinkhole Detection Using Probe Route Mechanism (SDPRM) For Internet of Things. Indian Journal of Science and Technology 15(37): 1892-1899. https://doi.org/10.17485/IJST/v15i37.1156

* **Corresponding author**.

hepsi.linda@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: To propose an Intrusion Detection System, called SDPRM (Sinkhole Detection using Probe Route Mechanism), to distinguish sinkhole assaults on the steering administrations in IoT. **Methods:** SDPRM intends to moderate unfriendly impacts initiate in IDS which troubled the routine tasks. The proposed architecture has the node ranker, notoriety and trust systems for recognition of assailants by examining the way of behaving of gadgets. Probe routing mechanism along with cluster configuration of the IoT gadgets are used to detect the SH attack. The probability density function is used to detect the behaviour of the gadgets present in the IoT environment. To demonstrate the efficiency of the proposed work Cooja simulator is used for experimentation. **Findings:** The proposed SDPRM is compared with the existing INTI architecture and it shows good results for detection rate and packet delivery ratio parameters. The comparative analysis is performed for static and mobility scenario. **Novelty:** In the existing architecture, probe route protocol was not used to detect the sinkhole attack in IoT environment. The current research work uses FIB (Forwarding Information Base) based probe-routing mechanism is used for securing the communication channel. The proposed architecture outperforms than the existing INTI architecture in terms of detection rate and packet delivery ratio.

Keywords: Internet of Things; Network security; Sinkhole attack; Proberoute; Beta distribution

1 Introduction

Advances such as IEEE 802.15.4, 6LoWPAN, and RPL have led to the production of genuine applications related to IoT [(1)]. However, due to the proliferation of smart gadgets and the high demand for these, there are likely to be weaknesses in the IoT environment. Most IoT gadgets have limited computing properties such as low power, limited range handling, capacity, loss of connections and various other features. Such restrictions make the IoT vulnerable to direct attack, which is one of the most damaging steering attacks [(2)].

Linda et. al.[3] have discussed the categories of routing attacks in the IoT. The authors specified that sinkhole attack is one of the major problems in IoT[4]. A sinkhole (SH) attacker wants to get the best traffic in a given area, which affects the collection of information at the classified point. As a result, it compromises the consistent quality and integrity of the information sent by gadgets (hubs). Overall, there are several options for measuring the impact of SH attacks on networks such as MANETs, WSNs and VANETs. In the IoT environment, a sinkhole attack is a vulnerable attack where intruders attempt to compromise a neighbouring node and cause damage in the IoT environment. Considerable research is being done on sinkhole attack detection in the IoT environment. A sinkhole attacker causes packet delivery losses, end-to-end latency, and reduced throughput. Grey hole and black hole attacks are some other threatening factors in the IoT environment. In a research work, the authors used PASR (prevention of an active sinkhole routing attack)[5] technique to detect the presence of sinkhole intruders in the IoT environment. The proposed method was compared with various environments with different attacks such as black hole and gray hole.

Edge computing based IoT deployment attracts researchers and industrialists to minimize the invasion of network attackers. In a recent study[6], the authors proposed a sinkhole attack detection algorithm using edge-based computing for the IoT environment. The proposed work used ranking mechanism to categorise the nodes and raise the false alarm. A technique based on rich resourced edge (RRE) nodes[7] is proposed to detect sinkhole in IoT. The proposed model is implemented in the NS2 simulator. RRE shown 0.37 % of improvement in the false rate prediction when compared with the previous research.

Machine learning plays significant role in predicting intruders in the IoT environment. Recently, considerable amount of research work is being published in the field of machine learning (ML) and deep learning (DL) for intrusion detection. The research article[8] reviewed the previous studies of forecasting intrusion detection by using ML and DL based techniques. The authors[8] proposed random forest based classifier to detect sinkhole attack in RPL-based IoT.HCODESSA[9] (Hop Count-Based Detection Scheme for Sinkhole Attack) was proposed to mitigate the sinkhole attack in wireless sensor cognitive radio networks. The proposed method was experimented in Matlab software.

In the wireless sensor networks (WSN), various studies have been done in cluster head allocation. In the article[10], hybrid optimal modal was proposed to optimize the WSN. Harmony search algorithm was improved using simulated annealing and it was combined with differential evolution optimization method to identify the cluster heads. The proposed work improved the lifetime of cluster and member nodes in WSN environment. In a recent research work[11] knowledge-based specification rule was proposed to detect sinkhole attacks in IoT. The proposed work was experimented and compared with the INTI architecture.

The authors[12] have proposed a new mechanism for Content-Centric Networking using probe-based routing technique. The probe-based technique is an alternative for the traditional internet protocol based routing method. FIB (Forwarding Information Based) probe routing method was experimented and results shown an efficient routing. The probe-based technique reduced the network congestion and increased the FIB accuracy.

From the above study, the application of probe route mechanism-based intrusion detection system in the IoT environment is less focused. In the proposed research work, probe router is used to filter the intruder in the network environment. In the existing INTI architecture, the reputation of the node was checked with the probability density function. To fill the research gap, the proposed research work provides a SDPRM framework to detect the presence of sinkhole attacks in IoT environment using probe route mechanism. In the current research, the node ranker is used along with the probability density function to filter the compromised nodes. SDPRM architecture works to prevent, identify and disconnect the impacts of the sinkhole attack in motion, while preventing adverse impacts. It combines route monitoring, reputation and confidence techniques to find attackers by dividing the behaviour of each node. The experiment results show that proposed SDPRM has 92% of identification speeds with standard gadgets.

This article is integrated as follows: Section I provided the introduction and background study of SH detection. The proposed work is discussed in the Section II. The outcome of the proposed work is given in the section III. Section IV concludes with the results of proposed SDPRM.

2 Methodology

2.1 IOT Environment

The assumed attack and communication models of the IoT environment is described in this section. Generally, the communication model in the IoT environment contains two levels for healthier communication between the physical networks is as follows:

i. Intercluster communication: It forms communication within groups (i.e., among various groups).
ii. Intracluster communication: It form communication inside the group (i.e., single group).

In the IoT environment, the physical network model is defined by the following expression 1.

$$\{s_1, s_2, s_3, \ldots, s_n\}, \; where \; s_n \in P \qquad (1)$$

Where s is the list of devices (i.e., gadgets/nodes/hubs) that are belongs to the physical network P.

The individual device has its own identification number which is identified by its unique physical address. In the IoT environment, a broadcasting node is created through wired or wireless environment with asynchronous-channel may contains information loss due to the noisy information and mobility of nodes. Usually, nodes are comprised by various properties such as memory size and battery. The data transmission range for nodes in the physical network has same values and it travels to diverse directions.

In the proposed work, the components of the IoT environment and their connections are represented in the Figure 1. The network devices in the IoT environment are classified as follows:

i. Base station: It is the main hub of the connected devices. It receives all the information from the nodes in the IoT environment.

ii. Moving nodes: It does not belong to cluster nodes and it may move within the provided environment.

iii. Head nodes: This node receives information from the member nodes in the cluster environment and passes the information to base station. The head node is acting as the sink node. It is placed in the IoT environment to identify the fake sink node. It has infinite energy and no downtime. This node contains separate encryption function and private key to encrypt the received data.

iv. Fixed nodes: These nodes are not movable and placed fixed. It helps to pass the information between the clusters.

v. Member cluster nodes: These are the normal nodes that are inside the cluster environment.

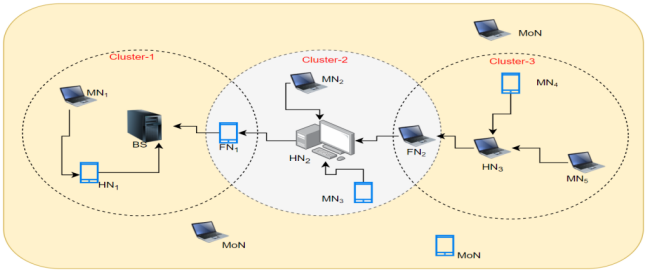

Fig 1. IOT Environment with Connected Devices (MN – Member nodes, FN – Fixed nodes, BS – Base Station, MoN – Moving Nodes, HN - Head Nodes)

2.2 Communication Model

In the IoT environment, the connected gadgets use the RPL protocol with its own limitations. However, as RPL deals with standard gadgets and terms[4], a protocol based on the RPL and it considers both the versatility and group organization of gadgets. The probe route tunnel is established within the IoT environment to monitor the intruders. Probe router is a device that is installed near the gateway for monitoring the nodes in the environment.

2.3 Attack Model

Since each node is an authority for forwarding and receiving information packets. The fake sink node may try to attract the normal nodes at a given time as the role of a chosen node (i.e., head node, cluster node, member node or base node). SH attack is considered to be the most devastating of all direct attacks on remote companies. During this type of attack, the attacker informs the neighbours that it knows the abbreviated route for an ideal purpose. It expects to draw a rush hour gridlock in a particular region to dispose of packets and damage the IoT environment.

2.4 Proposed SDPRM Architecture

The proposed SDPRM (Sinkhole Detection using Probe Route Mechanism) architecture is given in the Figure 2. The proposed SDPRM system comprises of the various mobility devices in the environment. Hence, there is a probability of chances that intruders can play any roles in the IoT environment that is discussed in the following sub-section. Proposed SDPRM runs

on the following four modules that are discussed below. The proposed SDPRM uses 'Probe-Route' [12] based mechanism to transfer the data within the IoT environment. The nodes (i.e., smart devices or sensors) enter the IoT environment through the device gateway. Then the probe-route channel is established for forwarding and receiving the messages between the nodes and the base stations. In this research work, FIB (Forwarding Information Base) based probe-route mechanism is applied for securing the communication channel. The probe name and data name are stored in the FIB data packet. The data packet contains the following information, name, signature, data, probe and probe response. The probe name is the content name. The probe can be arbitrarily assigned. After establishing the cluster configuration, the behaviour of the node is assigned based on the probability density function which is given in the following subsection. Proposed SDPRM architecture comprises the following four components that are discussed in the below subsections:

i. Cluster Configuration
ii. Route Monitoring
iii. Sinkhole Detection
iv. Sinkhole Isolation

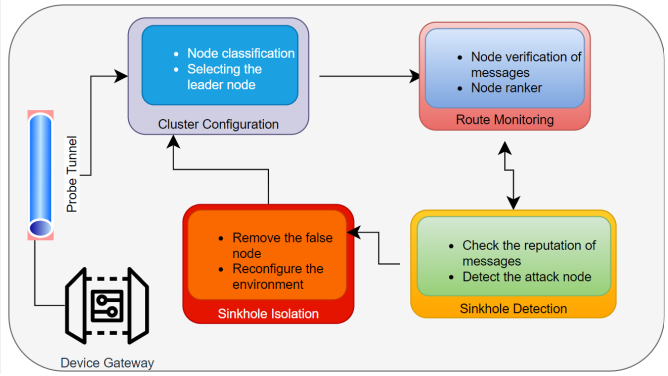

Fig 2. Proposed SDPRM Architecture

2.4.1 Cluster Configuration

This module characterizes a hierarchical based clustering that sets the hub cluster to guarantee the device scalability and enhance the life-time of the IoT environment. Hubs are individuals who rely on their network capabilities as members, fixed nodes, heads and moving nodes. Due to the versatility or attacking environment of the network, the work of each hub may change over a period of time due to fluctuations in the environment configuration.

First all the nodes in the network environment play as normal member nodes, to collect and transmit the control information. The role of member nodes may vary based on the necessary of the communication flow. Nodes send information in between them through probe-route communication tunnel (i.e., broadcast) to establish the request and response. This message empowers the nodes to measure how close they are to select the head nodes. The moving nodes can be categorized as the head node if they have continuous relationship (edges) between the nearest node (i.e., neighbouring nodes). After the appointment of the head nodes, the group is classified. At this point, the head nodes expect to form a team with one of their neighbours' choices (member nodes) head nodes. When setting up groups, head nodes look to see if one of their cluster nodes has received more than one message from different head nodes.

To identify the associated node, SDPRM checks the node which are receiving more than one messages. In simple term, if a node receives many messages from other nodes in a cluster, then it would be an associated node. The associated node helps to create links between other nodes. If there are two individual nodes in the same area, it is considered to be the corresponding node, which is the most significant energy content (HE): Total energy received refers to the total energy dependent on the same node and the total energy consumed. Total energy consumed Hub. The proposed beta uses the probability density function, i.e., which reveals the possibility of estimating the status of each hub behaviour, taking into accounts the previous effects of a hub. N = $(n_1, n_2, n_3, \ldots, n_i\}$ Where N is the total number of nodes.The leader node is identified by, if the node has contact with various member nodes from different clusters. The leader node is elected by the equation (2). The node communicates with different node and having more remaining energy.

$$HE_i = \frac{ER_i}{EC_i} \qquad (2)$$

where HE_I is the i^{th} node having highest energy, ER_i is the energy remaining and $EC_i$is the node consumed energy.

The cluster will be formed based on the radius of the connected devices. There will be a fixed node in each cluster and it acts as the associated node between the clusters. The fixed node has the FIB information and it helps to monitor the sink node (i.e., head node of the cluster).

2.4.2 Route Monitoring

A validation block is proposed for computing the transmission number and characterizing the information decision made by the responsive node for sending messages. For this purpose, the "monitor" node shows the number of transactions made by the "Head" Node, which is responsive to sending its messages. A head node is considered as top node since it has the lower rank among the nodes in the clusters. It evaluate show many sources of information and the results of the transaction are worked. Fundamentally, the health of node is calculated based on the input and output streams. The number of input transactions must be equal to the number of output streams. However, it is accepted that any deviations from the normal function will occur.

The factors such as HE and probe response are being monitor by the route monitoring. The changes in the behaviour will be updated and monitored. The PDF (probability density function) of Beta distribution is estimated based on the historical behaviour of the nodes and it is evaluated by the equation (3).

$$PDF = \frac{x^{\alpha-1}(1-x)^{\beta-1}}{P(\alpha,\beta)} \tag{3}$$

$P(\alpha,\beta) = \frac{\gamma(\alpha)\gamma(\beta)}{\gamma(\alpha+\beta)}$ where γ is the traditional gamma functiongiven in the equation (4).

$$\gamma(z) = \int_0^\infty x^{z-1}e^{-x}dx \tag{4}$$

The probability thickness and its measurable inference depend on the beta capacity. It is characterized by essential properties: It determines the function of a node in storing and sending messages to variable node. This value takes into account the probability of future expectation E(p), which is determined by the thickness capacity of the beta.

2.4.3 Sinkhole Detection

Proposed work can easily differentiate the behaviour of the compromised node that goes behind the sink node. The sinkhole detection component identifies the compromised node with probe-route mechanism and detect the sinkhole attacker in the IoT environment. The reputation of messages is identified with help of probe-tunnel. It is a conviction where nodes established between them. Notoriety of nodes are estimated based on the node's integrity. SDPRM uses the following parameters vulnerability (v), conviction (c) and suspicion (s). The above-mentioned parameters are evaluated using the beta distribution function. It is known that the $Beta(\alpha,\beta)$ is lies between [0,1]. The calculations of parameters v, c, s is denoted with the following equation 5

$$v+c+s=1 \tag{5}$$

Therefore, the conviction can be calculated using the equation (6)

$$c = 1-(v+s) \tag{6}$$

The vulnerability is a variance that occurred in the message transmission. In statistical term, variance is an error deviation that can be occurred in the population. Based on the principle of beta distribution, the variance of vulnerability is calculated using the following equation (7)

$$v = \frac{\alpha\beta}{(\alpha+\beta)^2*(\alpha+\beta+1)} \tag{7}$$

The average confidence of the reputation of nodes can be calculated using the equation (8).The confidence level is the mean of the beta distribution function. It resembles the reputation of convicted nodes. The value of c is greater than 0.75. The threshold value for confidence is set to 0.75 for this experiment.

$$c = \frac{\alpha}{(\alpha+\beta)} \tag{8}$$

The suspicion nodes can be calculated with the equation (9).

$$s = 1 - \left(\frac{\alpha\beta}{(\alpha+\beta)^2 * (\alpha+\beta+1)} + \frac{\alpha}{(\alpha+\beta)} \right) \quad (9)$$

The reputation of node is calculated based on the status evaluated with the (v, c, d) parameters. The value will be presented between 0 and 1. Bayesian probability function is performed based on the subjective probabilistic reasoning. Dempster-Shafer Theory (DST)was developed based on the Bayesian networks. It can be applied for the malformed probability distributions. In this research work, the node can be estimated under any of the three parameters (v, c, d). Among three 'v' and 'd' are malformed nodes. The value for DST is limit to [0,1]. As it is mentioned in the above discussion, the threshold value to identify the reputation of a node is set to 0.75. The following equation (10) is used to calculate the trust-relationship between two nodes. The value obtains from equation 11 is updated constantly. If the value is less than 0.75 then it is identified as vulnerable node. Expected mean of beta distribution for calculating the confidence of two communication nodes is denoted by the equation 10.

Confidence = $E(Beta(\gamma, \delta)) = \frac{\gamma}{(\gamma+\delta)}$ (10)

whereγ *and* δ are value of two communicating nodes.

2.4.4 Sinkhole Isolation

This final component separates the SH node after its invention. To this end, the node that recognizes a SH attack, it generates and amplifies a warning message on the broadcast to alert nearby nodes. Besides, the node is advancing by conveying the detachment of the occupier to its neighbours in a specific way. The information loss can be occurred to the intruder in the network. This phase is designed to rebuild the cluster after remove the false node from the environment. The cluster rank is revaluated with the cluster configuration components. In the proposed SDPRM architecture, three types of nodes are used to form the inter-cluster communication that are as follows: Member node (MN), fixed nodes (FN) and head nodes (HN). The following are the different cases used to separate the sinkhole node from the environment.

- Case – 1 (MN is SH): The HN isolate the compromised MN from the cluster.
- Case – 2 (FN is SH): The HN isolate the compromised FN from the cluster.
- Case – 3 (HN is SH): The FN isolate the compromised HN from the cluster. In this case the node ranker helps to identify the compromised head node in the environment. The associated node can identify the sinkhole node based on the rank that is updated constantly via the probe-information. The election of new head node will be conducted based on the behaviour of other nodes in the cluster. The HE is calculated to select the head node and reform the cluster.

Restoration of the clusters occurs based on the following criteria:

- If a node falls flat
- If a node exits the environment
- If node is compromised by the sinkhole attack.

3 Results and Discussion

The probe-route mechanism helps to maintain the information of nodes updated throughout the communication channel in the IoT environment. In the existing INTI architecture, the PDF was used to identify the reputation of nodes. In the proposed SDPRM architecture, the messages communicating between nodes are transmitted through the probe-route tunnel. This helps to verify the information and signature of the nodes. The threshold value of sinkhole detection was set to 0.5 in the existing INTI architecture, whereas, 0.75 is set as new threshold value to select the good node. The node which contains value less than 0.75 is isolated as sinkhole node.

Based on the fact that the INTI[12] architecture is additionally carried out on a similar test system, the proposed SDPRM architecture was implemented on a cooja simulator. The proposed ones are rated with INTI and are compared with sufficient quantity and effectiveness to mitigate SH attacks. There are fifty nodes in the rating scenario, some are standard and others are versatile, which refers to the regular number of public users traveling on a road. These public users have remote gadgets, for example, mobile phones, PDAs, workstations and travel in the connected area. This situation includes the practical metropolitan climate of a road, where there are a wide variety of products and gadgets. These customers can be walkers, pedestrians, cyclists and vehicles traveling at speeds ranging from 0 m / s to 6.94 m / s (10mk / h).

SH hubs range in size from 10 and 15, with 20% and 30% in all nodes separately. Each node uses a remote correspondence mode, following the model (Medium Unit Disk Graph (UDGM)) and operating model Random Waypoint generated in the 80 x 80 m and 100 x 100 m districts. The RPL uses the extension of the conference as a redirect conference to allow grouping. The

hub range varies from 30 to 40 m and they use UDP convention. The experimental time is 1500 seconds. Results are taken from the average of 25 simulations with confidence interval of ninety-five percentage. Four scales are used to evaluate the proposed and INTI architecture under SH attacks: detection rate and packet delivery rate. Figure 3 depicts the comparative analysis of detection rate for SH hubs range in size from ten and fifteen, with twenty percentage and thirty percentage in all nodes separately. Figure 4 depicts the mobility scenario of the SH attack detection rate. Figures 5 and 6 represents the packet delivery ratio for static and mobility scenario respectively.

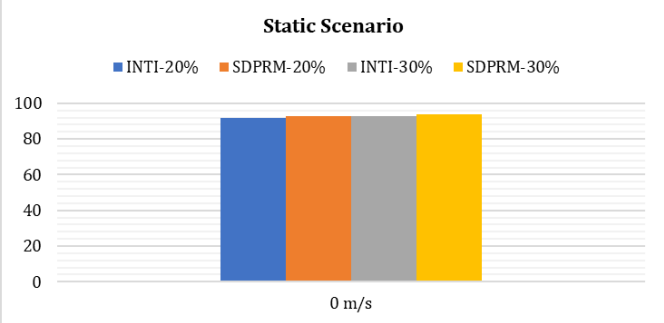

Fig 3. Comparative analysis detection rate – Static Scenario

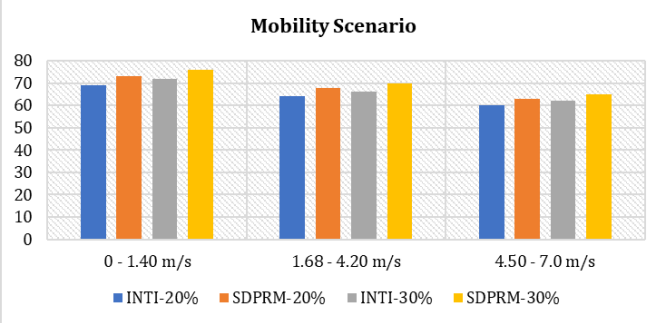

Fig 4. Comparative analysis detection rate – MobilityScenario

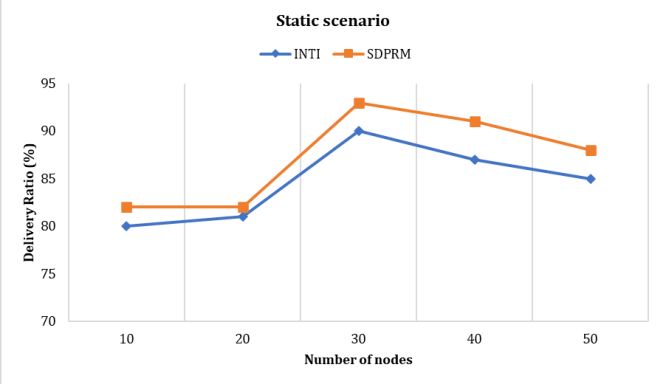

Fig 5. Comparative analysis of Packet Delivery Ratio –Static Scenario

In previous research works, the study has been done using the INTI architecture with traditional internet protocol-based routing system. The proposed SDPRM uses the probe-based routing mechanism. The proposed work increases the detection rate and decreases the network traffic congestion. This results an improvement in the packet delivery ratio.

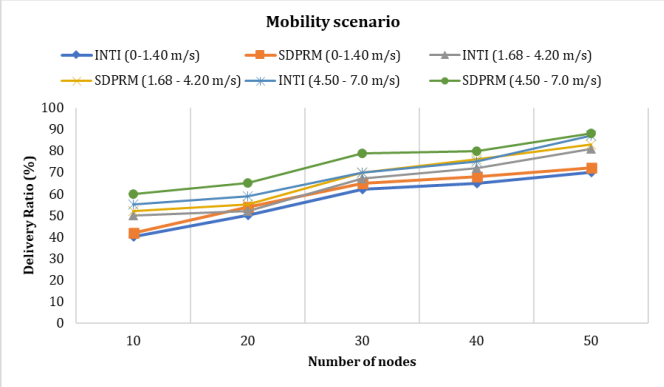

Fig 6. Comparative analysis of Packet Delivery Ratio –Mobility Scenario

4 Conclusion

This study provides the SDPRM framework for locating and isolating sinkhole attacks in IoT. The proposed technique is evaluated using the probe-route mechanism and compared with the INTI architecture. SDPRM sets up a unique concept to facilitate IoT communication and monitor the behavior of moveable hubs during transmission. Further, SH attack doesn't think about the effect of gadget portability, which in fundamental in metropolitan situations, similar to savvy urban communities. The way of behavior of suspicious hubs is identified by reputation and probability-based functions. The experiment results show that SDPRM fulfils a sinkhole detection rate of 92% in static conditions for having 30 nodes. SDPRM achieves 76% of detection rate for mobility scenario for 30% of nodes, which is 4% higher than the traditional INTI architecture. It is clearly evident that, increasing number of head nodes (i.e., number of clusters), results in increase of packet delivery ratio. As future work, we will evaluate SDPRM functionality to differentiate between different types of attacks in IoT.

References

1) Hepsiba CL, Priyadarsini DR, Dr S, Titus. A Comprehensive Study on Routing Attacks with Countermeasures in Internet of Things. 2020;63:7993–7999. Available from: http://solidstatetechnology.us/index.php/JSST/article/view/8339.
2) Suresh SDBA, Priyadarsini J. ETSET: Enhanced Tiny Symmetric Encryption Techniques to Secure Data Transmission among IoT Devices. *Turkish Journal of Computer and Mathematics Education*. 2021;12(10):1094–1099. Available from: https://doi.org/10.17762/turcomat.v12i10.4294.
3) Mathew J, Priyadarsini R. A Review on DoS Attacks in IoT, Solid State Technology. *Solid State Technology*. 2020;63(4):8000–8009. Available from: http://solidstatetechnology.us/index.php/JSST/article/view/8340.
4) Suresh SA, Priyadarsini RJ. A Comprehensive Study on Sybil Attacks and Its Defence Mechanisms in Internet of Things. *Solid State Technology*. 2020;63:7966–7974. Available from: http://solidstatetechnology.us/index.php/JSST/article/view/8337.
5) Tahir S, Bakhsh ST, Alsemmeari RA. An intrusion detection system for the prevention of an active sinkhole routing attack in Internet of things. *International Journal of Distributed Sensor Networks*. 2019;15(11):155014771988990–155014771988990. Available from: https://doi.org/10.1177/1550147719889901.
6) Pundir S, Wazid M, Singh DP, Das AK, Rodrigues JJPCJPC, Park Y. Designing Efficient Sinkhole Attack Detection Mechanism in Edge-Based IoT Deployment. *Sensors*. 1300;20(5):1300–1300. Available from: https://doi.org/10.3390/s20051300.
7) Bilal A, Hasany SMN, Pitafi AH. Effective modelling of sinkhole detection algorithm for edge-based Internet of Things (IoT) sensing devices. *IET Communications*. 2022;16(8):845–855. Available from: https://doi.org/10.1049/cmu2.12385.
8) Prathapchandran K, Janani T. A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST. *Computer Networks*. 2021;198:108413–108413. Available from: https://doi.org/10.1016/j.comnet.2021.108413.
9) Sejaphala LC, Velempini M. The Design of a Defense Mechanism to Mitigate Sinkhole Attack in Software Defined Wireless Sensor Cognitive Radio Networks. *Wireless Personal Communications*. 2020;113(2):977–993. Available from: https://doi.org/10.1007/s11277-020-07263-9.
10) An TGH, Cho H. Improving Sinkhole Attack Detection Rate through Knowledge-Based Specification Rule for a Sinkhole Attack Intrusion Detection Technique of IoT. *International Journal of Computer Networks and Applications (IJCNA)*. 2022;9(2):169–178. Available from: https://doi.org/0.22247/ijcna/2022/212333.
11) Umashankar ML. An efficient hybrid model for cluster head selection to optimize wireless sensor network using simulated annealing algorithm. *Indian Journal of Science and Technology*. 2021;14(3):270–288. Available from: https://doi.org/10.17485/IJST/v14i3.2318.
12) Tsai PH, Zhang JB, Tsai MH. An Efficient Probe-Based Routing for Content-Centric Networking. *Sensors*;22(1):341–341. Available from: https://doi.org/10.3390/s22010341.