International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6620
***Article Received**: 28 February 2023 **Revised**: 09 April 2023 **Accepted**: 30 April 2023*

Sinkhole Detection in IOT using Elliptic Curve Digital Signature

C. Linda Hepsiba[1], Dr. R. Jemima Priyadarsini[2]
[1]Assistant Professor, Department of Computer Science,Bishop Heber College,
Affiliated with Bharathidasan University,
Trichy17,Tamilnadu,India
hepsi.linda@gmail.com
[2]Associate Professor, Department of Computer Science,Bishop Heber College,
Affiliated with Bharathidasan University,
Trichy-17,Tamilnadu,India
jemititus@gmail.com

Abstract— A variety of smart applications, including homes, transportation, health, and robots in industries, are starting to gain interest due to the fast expansion of Internet of Things (IoT). Smart devices are made up of sensors and actuators that actively involved in monitoring, prediction, security, and information sharing in the IoT ecosystem. These state-of-the-art (SOTA) technologies enable people to monitor and manage their unified milieu in real-time. IoT devices are nevertheless regularly used in hostile situations, where attackers try to grab and penetrate them to take over the entire network. Due to the possibility of selective forwarding, sinkhole, blackhole, and wormhole attacks on IoT networks is a serious security risk. This research offers an effective method using a digital signature to detect and mitigate sinkhole attacks on IoT networks to resolve this problem. By doing a thorough security study of this suggested system, it shows how safe it is and how resistant it is to secure sinkhole attack detection. In this study, elliptic curve digital signature algorithm is used along with the node ranker to detect the sinkhole attack in IoT environment. According to the performance analysis and experimental findings compared to other research, the suggested system offers good detection accuracy and greatly lowers the overhead associated with computing, communication, and storage.

Keywords- Iot; sinkhole detection; digital signature; elliptic curve cryptography;

I. INTRODUCTION

IoT has been attracting the attention of hackers at a higher rate than ever before due to its phenomenal growth rate [1]. This has been supported by the increasing frequency of cyberattacks on devices connected to the smart ecosystem and intermediary communication media. Attacks on the smart ecosystem can result in significant financial loss if it goes undiscovered for an extended period of time and cause major service interruption. Additionally, it poses the risk of identity protection being compromised. It is necessary to be able to detect intrusions on devices connected to the smart ecosystem in real time in order to make the smart devices-enabled services safe and gainful [2].

IoT devices are often installed in unsafe areas where adversaries try to capture and penetrate them to control the network. An intruder can physically capture IoT devices, collect important information, replicate them, and intelligently deploy them in desired areas to conduct various attacks. IoT networks are vulnerable to selective forwarding, sinkhole, blackhole, and warmhole assaults from device cloning attacks [3]. Sinkhole attack is one of the dangerous attacks in the IoT environment [4].

One of the ways for identifying sinkhole attacks in the Internet of Things is called INTI [5] [6]. The rules for the intrusion detection process in the INTI architecture were created by applying specification-based approaches. This was done during the attack detection process. Every node in the network possesses its own unique set of knowledge-based rules. In order to carry out each rule, an inference engine that supports forward chaining is utilised. Utilizing this method has resulted in an increase in the number of sinkhole attacks discovered. Several studies [7] [8] related to cyber-attacks were specified that the sinkhole detection system is the most vulnerable attack in the IoT environment [9] [10].

The Sinkhole networking exploit ruins the RPL protocol topology by rerouting all IoT network traffic. The authors [11] [12] reviewed sinkhole attacks in IoT and proposes strategies for mitigating and detecting them in low-power IoT networks. Ahmad et. al. [13] have proposed modified SVELTE Intrusion Detection System (IDS). It specifically improved the SVELTE IDS rank inconsistency detection technique.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6620
***Article Received**: 28 February 2023 **Revised**: 09 April 2023 **Accepted**: 30 April 2023*

Awagen [2] have introduced a Deep Learning (DL) based IoT intrusion detection solution. This intelligent solution detects fraudulent traffic that may harm IoT devices using a DL architecture. The suggested communication protocol-independent solution reduces deployment complexity. Experimental performance study shown that the suggested system outperformed well for simulated and real intrusions. It detected Blackhole, DDoS, Sinkhole, and Wormhole attacks. The attack detection rate was 93%. Sadhu et. al [14] have classified vulnerabilities based on the intruder characters. This article described each attack type and its countermeasures. IoT security case studies are highlighted. Security technologies such as blockchain and secret key-based cryptographic systems were discussed in this article.

Several research articles and theses have proposed numerous data authentication systems based on system architecture and solutions to security breaches caused by defects and weak points in previous schemes. Ali E. Takieldeen, and Fahmi Khalifa [15] have reviewed lightweight elliptic curve cryptography (ECC) for IoT authentication. ECC outperforms other cryptosystems. Most IoT devices, particularly resource-constrained ones, should integrate it. Exploring approaches with clear explanations helped guide future IoT lightweight authentication researchers. To uncover lightweight ECC scheme design considerations, the study proposals were compared.

Authentication and session key agreement are the foundations of secure communication using custom security protocols. These protocols govern communication and cryptography. In the paper [16] reviewed the newest communication methods for IoT authentication and session key agreement. The authors have examined the protocols' security, vulnerability, computational, and communication costs.

Elliptic Curve Digital Signature Algorithm (ECDSA) is a lightweight intrusion detection system discussed by Jaspreet and Gangadeep [17]. By viewing and modifying header information, intruders can launch DDoS, sinkhole, blackhole, ransomware, and other assaults. HTTP, TCP, IP, UDP, TLS, and IPsec are included in this header information. Attackers can simply observe and exploit this information.

Distributed ledgers and blockchains emerged alongside IoT. Blockchains improve security, anonymity, capacity, and peer-to-peer capabilities. Blockchain technology can solve IoT problems, but integrating it is difficult. Later, we present this study's findings, which show how blockchain technology and IoT can be used to address privacy and security issues. We then categorise applications based on their primary information, objective, development level, target application, type of blockchain and platform, consensus algorithm, evaluation environment, and more. [18]

In a study suggested by Rakesh [19] Innovative Authentication and Secure Trust-based RPL Routing in Mobile sink-supported IoT (SecRPL-MS). All IoT nodes in the network register with SecRPL-MS. Mobile sink reduced the loss of IoT node. The member nodes must be authenticated to send data to the head node. Sailfish optimization technique was used for secure routing. Genetic algorithm based optimization was used to detect the sinkhole attack in IoT ecosystems [20].

Moshen et. al. [21] have introduced the Dropped Destination Advertisement Object (DDAO) attack and a new Intrusion Detection System (IDS) for RPL protocol. DDAO attack prevents downward routes by not delivering DAO messages. It was achieved by sending duplicate DAO-ACK messages to the DAO source. The authors have proposed a lightweight IDS to detect and counter DDAO attacks by monitoring parent behaviour against passed DAO messages.

A smart device that protects against sinkhole attacks, which are among the most damaging kinds of attacks that might occur in the IoT is discussed. Sinkhole attack detection strategies are typically utilised in ad hoc networks and WSNs; however, it might be difficult to adapt these strategies to the IoT because of the varying ambient conditions. Inside the scope of this research contribution, an innovative architecture for detecting and mitigating sinkhole attacks within an Internet of Things environment is provided. The reputation of messages transmitted in the IoT environment is transferred through the elliptic curve cryptography (ECC) mechanisms. The asymmetric key-based mechanism is used to transfer secure messages between the nodes. Along with the cryptosystem, the node ranker technique is used to isolate the compromised node in the IoT system.

The following is the structure of this article: followed by the introduction, the proposed mechanism is explained with a neat diagram in the section 2. The results and discussion are given in the section 3 and the article is concluded in the section 4.

II. HYBRID SIDE ARCHITECTURE

The proposed Hybrid SIDE (Hybrid Sinkhole Detection for IoT) architecture is given in the figure 1. The proposed Hybrid SIDE system comprises of the various mobility devices whereas there is a probability of chances that intruders can play any roles in the IoT environment that is discussed in the following section. The nodes (i.e., smart devices or sensors) enter the IoT environment through the device gateway. The architecture of the proposed work is given in the figure 1. The proposed architecture has three modules that are as follows: (i)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6620
***Article Received**: 28 February 2023 **Revised**: 09 April 2023 **Accepted**: 30 April 2023*

Cluster configuration, (ii) route monitoring and (iii) sinkhole isolation.

A. 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.

In this phase, the cluster of nodes in the IoT 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).

The role of member nodes may vary based on the necessary of the communication flow. Nodes send information in between them through 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 (free nodes) head nodes. When setting up groups, head nodes check to see if any of their cluster nodes have received multiple messages from multiple other head nodes. If it does, then consider that node to be a member of more than one group. If a single area node is found to have received several messages, it will be determined to be connected. This will result in the formation of connections between the various groups. In the event that there are two distinct nodes located in the same region, the one that is regarded to have the most substantial amount of energy content is the associated node. The term "total energy received" refers to both the total amount of energy that is dependent on the same node as well as the total amount of energy that is used. 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 denotes the available nodes in the environment.

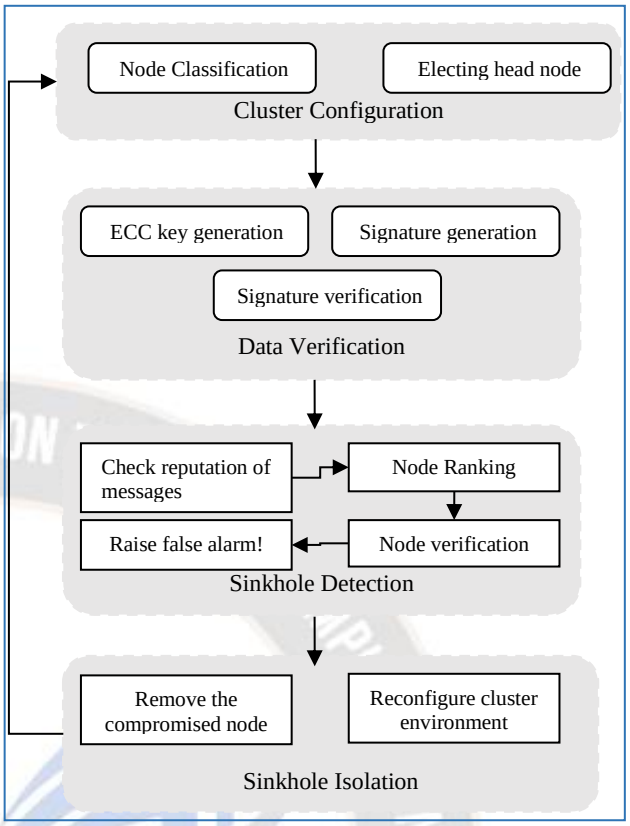

Figure 1. Proposed Architecture

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 (1). The node communicates with different node and having more remaining energy.

$$HE_i = \frac{ER_i}{EC_i} \qquad (1)$$

Notations used:

HN = head node

MN = member node

d = data

nn = node ID

HF = hash function

o = Prime field F_o Order

EC(a,b) = Elliptic Curve defined over the F_o

PT = non-zero random base point in EC(F_o)

x = ordinal value of PT (basically it is a prime number)

f = cofactor = $\frac{|EC(Fo)|}{x}$

Pub_k = public key

Pri_k = private key

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6620
Article Received: 28 February 2023 Revised: 09 April 2023 Accepted: 30 April 2023

C = coordinates(x,y)

t = signature

R_{HN} = Rank of head node

R_{MN} = Rank of member node

Algorithm: Data Verification

Input: Data, Domain parameters (o, EC, PT, x, f)

Output: Accept or Reject Data and detect malicious head node

1. Data from SN
2. While cluster is exists:
3. If HN is not malicious:
4. If data is True:
5. Generate key along with data
6. Choose PT of order x for EC(F_o), PT ϵ EC(F_o)
7. Generate Pri_k for Pri_k is some positive integers of (1, x-1)
8. Compute $Pub_k = Pri_k * PT$
9. End step 4
10. Generate signature with d, Pri_k, HF, PT
11. Select random number q for some q between 1 and x-1
12. Compute C = q*PT
13. If nn != 0:
14. Compute nn = x
15. End step 13
16. Elif nn == 0:
17. Goto step 11
18. End step 16
19. Compute HF(d) using md5 and store it as integer i
20. Compute $s = q^{-1} (i + (Pri_k * nn))$
21. If s == 0:
22. Goto step 11
23. End step 21
24. Check signature verification with Pub_k and signature (nn, t)
25. Let nn and s are numbers between 1, x-1
26. Compute HF(d) using md5 and store it as integer i
27. Compute $\gamma = t^{-1} \, mod \, x$
28. Compute $v_1 = (i * \gamma) \, mod \, x$ and $v_2 = (nn * \gamma) \, mod \, x$
29. Compute $C = (v_1 * PT) + (v_2 * Pub_k)$
30. If C == None:
31. Reject signature
32. Goto step 37
33. End step 30
34. If nn = $v_1 \, mod \, x$:
35. Accept signature
36. End step 33
37. Elif HN == malicious:
38. Check R_{HN}
39. Remove HN
40. Elif MN == malicious:
41. Check R_{MN}
42. Remove MN
43. End step 3
44. End step 2
45. Reconfigure cluster.

B. Route Monitoring

ECC is used to obtain the keys which is the form of a digital signature algorithm. A branch of public-key cryptography called elliptic curve cryptography (ECC) is centred on elliptic curves generated from algebraic structure over finite fields. The ECC, which requires fewer keys to achieve identical security, makes it more effective and robust even if it performs comparably to other signature algorithms like DSA and RSA. Using basic ECC has been demonstrated to be effective in improving the overall performance and robustness. The ECC approach is a lightweight key generation mechanism as well as it increases computational speed and decrease the dependability of key size. Elliptic curve digital signature and verification algorithm (ECDSVA) is a variant of ECC that computes and validates signatures faster than ECC, is also being considered.

Instead of certifying each digital signature one at a time, you may validate numerous digital signatures at once using a process known as batch verification. In this method, the signer node interacts with the verifier node to create ‘t’ signatures.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6620
***Article Received**: 28 February 2023 **Revised**: 09 April 2023 **Accepted**: 30 April 2023*

The verifier simultaneously verifies each of these 't' signatures. ECDSVA is a popular digital signature method on the Internet of Things (IoT) because it employs lower key sizes, provides the same degree of security as public-key cryptography, and maintains the reliability of devices and data transmission between them. In order to validate the location proof signatures generated by IoT devices, the proposed work focused on ECDSVA signatures. A variation of ECDSVA signatures provide 40% greater efficiency in verification without sacrificing security. It is necessary to implement the suggested algorithm for key creation, signature generation, and signature verification in order to use the ECDSVA, just as it is necessary to do with the ECC. The subsequent sections detail both the practical application of these algorithms as well as their respective explanations.

The step 5 to 9 shows how to generate both public and private keys for ECDSVA. A public and private key pair is created by the key generation algorithm and used in the signing and verification procedures.

The signing procedure is carried out to produce the real digital signature using the step 10. The ECDSVA Signature Generation process is demonstrated by Algorithm 1 in the step 10 to 23. It takes as inputs the message m, the hash function HF, and domain parameters like PT, and generates the signature (nn, t) for each participant. For instance, on the Internet of Things, each unique signature is produced for each device for verification. This algorithm starts the signature creation process by choosing a random number between 1 and n-1 for the q parameters. The random number q is then multiplied with the random point PT to provide the coordinates C. The message m is sent to the hash function HF (in this example, MD-5) which generates a digest string value as a hash value, which is then transformed to an integer 'i'. The result of adding the sum of the integer 'i' and the private key 'Prik' is multiplied by 'nn', and the result is the signature value 't'. A pair, such as, is the product of the IECDSA signature generating process (nn, t).

The steps from 24 to 36 in the algorithm is used to validate signatures that have been submitted using the signer's public key. The length of the signature affects the verification procedure; the longer the signature, the longer the verification process will take. Because of the variation in signature size, the techniques used to verify signatures are slightly different.

The inputs needed for this procedure are a public key 'Pubk' and a signature value (nn, t) that must be verified. However, the outcome of the signature verification is a binary choice, such as accept or refuse. Checking if the signature values nn and t are inside the range [1, x-1] is the first step in the signature verification procedure. The hash HF function compares m's hash value. The hash value is transformed into an integer 'i,' just like the technique for creating signatures. An integer value is produced by calculating the modulus of the signature's inverse value. The next step is to multiply the numbers 'i' and 'nn' by the value of to produce the two coordinates v1 and v2. Combine the product of PT and Pubk by the determined coordinates (v1,v2) from the preceding step yields an C value. The signature will not be accepted if C = empty; instead, it will only be accepted if value of nn is correct. The flowchart of elliptic curve digital signature is given in the figure 2.

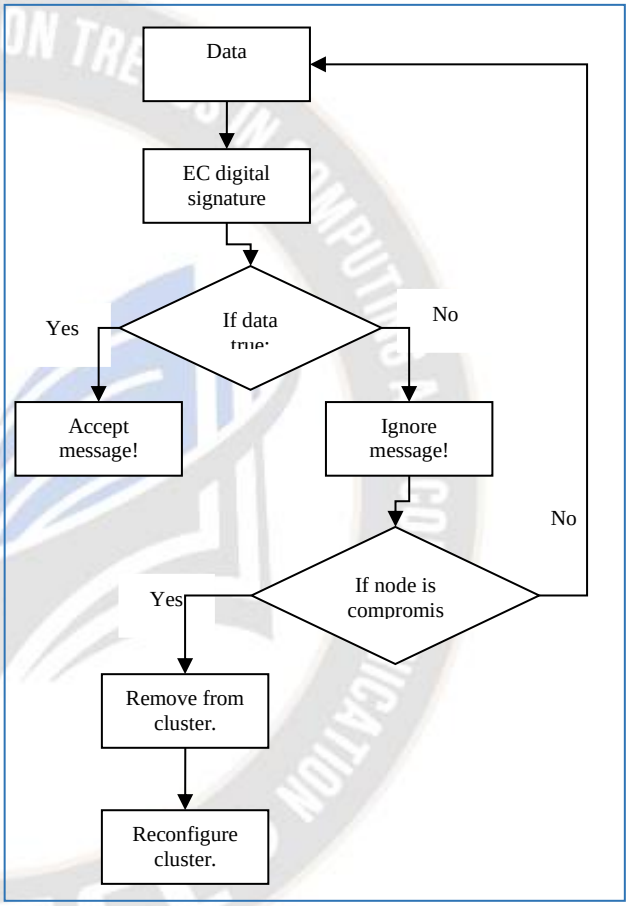

Figure 2. Flowchart of Elliptic curve digital signature phase.

C. Sinkhole Isolation

Following the process of the route monitoring, this block serves to differentiate it by isolate the compromised node or attacker node. To achieve this goal, the node that identifies the SH attack generates and transmits a warning message to other nodes in the vicinity. In addition to this, the node advances by communicating in a particular way to its neighbours the detachment of the occupier of the node. The node rankings are an example of the fundamental information generated by the restructuring clusters. These rankings make it possible for nodes to refocus when they remain in the same position.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6620
***Article Received**: 28 February 2023 **Revised**: 09 April 2023 **Accepted**: 30 April 2023*

There are three distinct parts to a sinkhole, and they are as follows: (I) When a sinkhole hub is only a partial hub, its own leader will divide such a node; (ii) when the SH Hub is pioneering, if the area nodes divide the SH Hub or assume that there is a corresponding hub on the other hand, it will disconnect the occupier; and (iii) when the SH Hub moves to the corresponding node, it is controlled by the pioneer node, which is the highest level, which then interrupts correspondence with the attacker. It is also extremely important to make certain that the cluster is contained and that all other relevant nodes are located at the lowest level possible, in order for messages to be directed to the node that is intended to receive them. In the event that this does not occur, the pioneer will spread the message of redemption in an effort to convince its people to join the nearby clusters.

When a node falls flat, leaves the board, or is hit by a single hole attack, clusters are rebuilt according to the criteria listed above. When a pioneer node is hit by one of these problems, one of two things may take place: either a new head is appointed to the cluster, or the nodes in the affected area may be dragged into neighbouring groups. Because the corresponding node is located within the normal area, it is possible that the other area will be selected even if it is the one that is affected. On the other hand, presuming that the two cluster precursors are at the same transfer interval, the group combination makes it possible for each cluster to contain a greater number of area nodes. It is anticipated that there will be a lower total number of head nodes.

III. RESULTS AND DISCUSSIONS

The suggested architecture known as Hybrid SIDE is being evaluated by the well-known operating system for the internet of things known as Contiki OS. The Cooja simulator is utilised in order to do testing on the RPL implementation. The main purpose of the Hybrid SIDE is to identify and stop routing assaults, especially the sinkhole attack. The RPL implementation in the Contiki operating system is used by the Hybrid SIDE mechanism to create the detection modules for the RPL network. Except for the border router, which is not a constrained node, all of the nodes in the RPL network are resource restricted. The root node has been implemented with the suggested approach, Hybrid SIDE. The modules can use the substantiation phase to validate and verify the node's behaviour.

The suggested ECC-based intrusion detection system is commonly used in order to monitor the behaviour of the nodes that make up the Internet of Things. The RPL implementation of the Hybrid SIDE mechanism is used for network routing. This means that each node is responsible for keeping track of all of its own control messages. In addition, the Hybrid SIDE defends the RPL network against attacks such as sinkholes, blackholes, and selective forwarding.

The analysis is based on the properties of the network. The properties such as the amount of energy that is spent, the amount of time that is required to determine whether or not an attacker is present, and the length of time that is required for the network to converge. In the testing conducted by Contiki, using the Cooja network simulator, it was discovered that accurate results could be obtained. On the Cooja simulator, the code for deployable Contiki is put through its paces.

The ones that have been offered are evaluated using INTI, and their quantity and efficiency in warding off SH vulnerabilities are weighed against one another. For simulation, fifty nodes are used. In that, some of the nodes are fixed and other nodes are movable. A standard node refers to the typical number of members of the public who travel on a route. These members of the public utilise remote devices, such as mobile phones, personal digital assistants (PDAs), and workstations, and they move around in the linked area. This scenario encompasses the bustling urban environment of a road, which features a diverse assortment of goods and devices available for purchase. These clients might be walkers, pedestrians, bikers, or cars moving at speeds ranging from 0 metres per second up to 7 metres per second.

The size of the SH range anywhere from 20% and 30% of each node being distributed individually. Following the paradigm and operational model Random Waypoint created in the 80x80m and 100×100m remoteness, each node makes use of a remote correspondence mode. In order to facilitate grouping, the RPL employs the conference's extension in the capacity of a redirect conference. They make use of the UDP protocol, and the hub range is anywhere from 30 to 40 metres in length. The time for the experiment is one minute and five hundred seconds. The results are based on an average of twenty-five different simulations, and the confidence interval is set at ninety-five percent. Detection rate and packet delivery rate are two of the measures that are utilised in the process of evaluating the proposed Hybrid SIDE and INTI architecture when subjected to SH vulnerabilities.

In static scenario, the comparative study of detection rates is depicted in Figure 3. The proposed Hybrid SIDE shown an improvement of 3% compared with the INTI architecture. The comparison is made with the sinkhole attack in the 10 nodes and 15 nodes environment. The mobility scenario of the SH attack detection rate is shown in Figure 4. The proposed work shown an 5% improvement of detection rate in the mobility scenario when compared with the existing INTI architecture. From the results, it is observed that the detection rate is decreasing for the nodes moving fast in the IoT ecosystem.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6620
***Article Received**: 28 February 2023 **Revised**: 09 April 2023 **Accepted**: 30 April 2023*

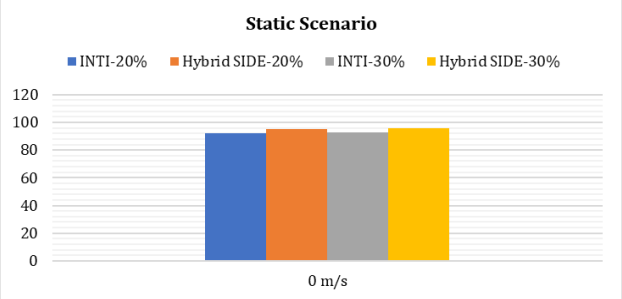

Figure 3. Detection rate – Static Scenario

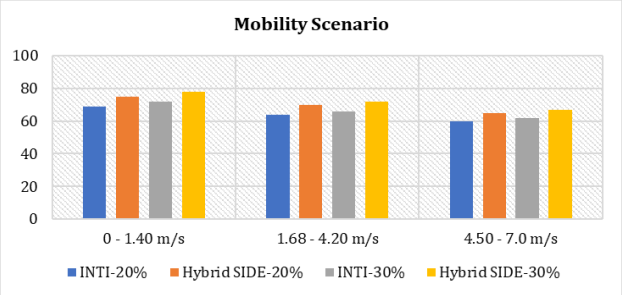

Figure 4. Detection rate – Mobility Scenario

Figures 5 and 6 illustrate the percentage of successfully delivered packets for the static and mobility scenarios, respectively. In the static scenario (fig. 5), the packet delivery ratio of proposed Hybrid SIDE architecture outperformed well than the existing INTI architecture for 30 nodes in the simulated IoT environment. Gradually it the delivery ratio is decreased for nodes between 30 to 50. Unlike, static scenario, the packet delivery ratio of the nodes in mobile scenario (fig. 6) shows little decrease in the accuracy between nodes 30 to 50. The packet delivery ratio is decreasing for the nodes moving fast from the IoT ecosystem.

The investigation has been carried out in prior research works utilising the INTI architecture in conjunction with the conventional internet protocol-based routing system. The work that is being proposed would boost the detection rate while also reducing the amount of network traffic congestion. This causes an increase in the percentage of successfully delivered packets. The packet delivery ratio for the static scenario is higher than the mobility scenario.

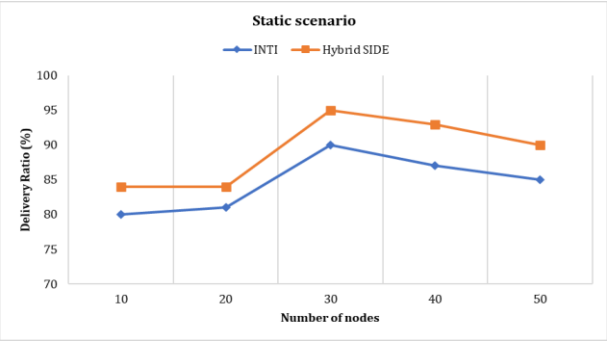

Figure 5. Packet Delivery Ratio – Static Scenario

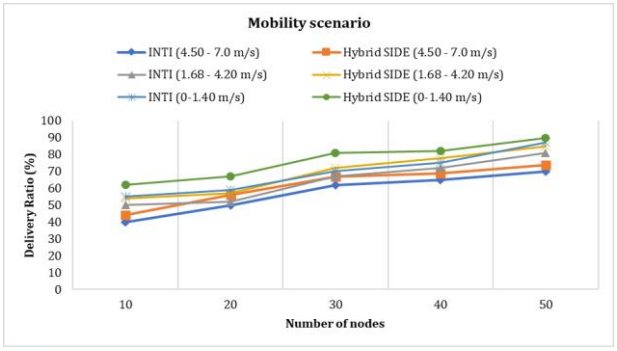

Figure 6. Packet Delivery Ratio – Mobility Scenario

IV. CONCLUSION

This paper provides the Hybrid SIDE architecture for locating and isolating sinkhole attacks in IoT. The proposed technique is evaluated using the ECC mechanism for verifying the nodes in the cluster environment. The proposed Hybrid SIDE is compared with the INTI architecture. Hybrid SIDE sets up a unique concept to facilitate IoT communication and monitor the behavior of moveable hubs during transmission. Furthermore, the SH attack detection includes the impact of smart devices mobility, which is critical in metropolitan circumstances, such as urban populations. The proposed work checks the reputation of messages using ECC mechanism and it used the node ranker technique to isolate the compromised nodes. The experiment results show that Hybrid SIDE fulfils a sinkhole detection rate of 96% in static conditions for having 30 nodes. Hybrid SIDE achieves 84% 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, it will evaluate Hybrid SIDE functionality to differentiate between different types of attacks in IoT.

REFERENCES

[1] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, S. W. Kim, "The future of healthcare internet of things: a survey of emerging technologies," IEEE Communications Surveys & Tutorials, 22 (2), pp. 1121–1167, 2020.

[2] Awajan, A. (February 2023). "A Novel Deep Learning-Based Intrusion Detection System for IoT Networks." Computers, vol. 12. Available: https://doi.org/10.3390/computers12020034.

[3] Khizar Hameeda, Saurabh Garga, Muhammad Bilal Amina, Byeong Kanga, Abid Khanb. "A Context-Aware Information-Based Clone Node Attack Detection Scheme in Internet of Things". Journal of Network and Computer Applications, vol. 197, January 2022

[4] Zaminkar, M. and Fotohi, R., SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism, Wireless Personal Communications, vol. 114(2), pp.1287-1312, 2020.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6620
***Article Received**: 28 February 2023 **Revised**: 09 April 2023 **Accepted**: 30 April 2023*

[5] 5. C. Cervantes, D. Poplade, M. Nogueira and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," in Proc. 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606-611, 2015.

[6] Ga Hyeon An, Tae Ho Cho. "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), vol. 9, 2022.

[7] S. Alexander Suresh SDB and Dr.Jemima Priyadarsini, ETSET: "Enhanced Tiny Symmetric Encryption Techniques to Secure Data Transmission among IoT Devices", Turkish Journal of Computer and Mathematics Education, vol.12 No.10: pp. 1094-1099, 2021.

[8] C. Linda Hepsiba, Dr. R. Jemima Priyadarsini, Dr. S. Titus, "A Comprehensive Study on Routing Attacks with Countermeasures in Internet of Things", Solid State Technology, vol. 63 No. 4: 7993-7999, 2020.

[9] Jeethu Mathew, Dr. R. Jemima Priyadarsini, "A Review on DoS Attacks in IoT," Solid State Technology, vol. 63 No. 4: pp. 8000-8009, 2020.

[10] Mr. S. Alexander Suresh, Dr. R. Jemima Priyadarsini, "A Comprehensive Study on Sybil Attacks and Its Defence Mechanisms in Internet of Things", Solid State Technology, vol. 63 No. 4: pp. 7966 – 7974, 2020.

[11] J. Rani, A. Dhingra and V. Sindhu, "A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network," in Proc. International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, pp. 1-6, 2022.

[12] Maung, Tay Zar Bhone, and Lunchakorn Wuttisittikulkij. "A Comprehensive Survey of Sinkhole Attack in Routing Protocol for Low-Power and Lossy Networks for IoT Devices." in Proc. The 14th Regional Conference on Electrical and Electronics Engineering (RC-EEE 2021), 2022.

[13] Ahmad Mujtaba, Dr. Ammar Rafiq, Salal Amjad, Asim Mubarik, Muhammad Usman Younas. "Enhancement of accuracy of the Rank Inconsistency Detection Algorithm", Pakistan journal of engineering and applied sciences, vol. 30, Jan 2022.

[14] Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, "A. Internet of Things: Security and Solutions, Survey", Sensors, vol. 22, 2022.

[15] Takieldeen, FK Ali E., and Fahmi Khalifa. "Authentication and Encryption of IoT Devices Based on Elliptic Curves: A survey." Journal of Intelligent Systems and Internet of Things (JISIoT), vol. 5 2021.

[16] Szymoniak, S.; Kesar, S. "Key Agreement and Authentication Protocols in the Internet of Things: A Survey". Appl. Sci., vol. 13, 2023.

[17] Kaur, Jaspreet, and Gagandeep Singh. "A Blockchain-Based Machine Learning Intrusion Detection System for Internet of Things." Principles and Practice of Blockchains. Springer, Cham, pp. 119-134, 2023.

[18] Zubaydi, H.D.; Varga, P.; Molnár, S. "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review." Sensors, vol. 23, 2023.

[19] Bandarupalli Rakesh and Parveen Sultana H. "Novel Authentication and Secure Trust based RPL Routing in Mobile sink supported Internet of Things," Cyber-Physical Systems, vol. 9, pp. 43-76, 2023.

[20] S. Velliangiri, Iwin Thanakumar Joseph, Shanthini Pandiaraj, P. Leela Jancy and Ch. Madhubabu. "An enhanced security framework for IoT environment using Jaya optimisation-based genetic algorithm." International Journal of Internet Technology and Secured Transactions, vol. 13, no. 1. November 2022.

[21] Mohsen Sheibani, Behrang Barekatain, Erfan Arvan. "A lightweight distributed detection algorithm for DDAO attack on RPL routing protocol in Internet of Things." Pervasive and Mobile Computing, vol. 80, February 2022.