**The secure channel setup technique to isolate misdirection attacks on the Internet of Things**

1. **Introduction**

The concept of the Internet of Things (IoT) enables us to consider the possibility that it could soon be able to use the internet to connect to every type of gadget that is in the nearby environment. This can make it possible for us to interact or engage with any gadget around us, regardless of its type, from any location in the world [1]. The development of IoT was inevitably influenced by several well-known and essential technologies of the present day, including Wireless Sensor Networks (WSN), Miniaturization, and Nanotech. In all kinds of IoT applications, WSN is always the most critical component [2].

WSN is the type of technology whose development is accelerating at an alarming rate, and the field of study surrounding them is often regarded as the most fascinating and rapidly expanding [3]. WSN is a component of many important applications that are used today i.e., the management and monitoring of combat zones, the evaluation and monitoring of weather forecasts, monitoring in healthcare facilities, and supply management [4]. Additionally, the computational power, power efficiency, and memory abilities of small computers or sensing devices have enhanced while their dimensions have radically dropped. This is although their numbers of transistors have remained unchanged [5].

The dangers and intrusions on the safety or privacy of a product or an individual have dramatically increased due to the above-mentioned pros [6]. IoT security is an ongoing study topic that is receiving a growing amount of attention in research conducted not just by academic institutions but also by private industry and the government [7]. Figure 1 demonstrated a systematic approach to IoT security.

![Diagram

Description automatically generated]()

Figure 1: Systematic approach for IoT security [8].

Connected devices are expected to enhance the quantity of personal information that can be collected and stored by IoT. As a result, hackers and other cyber criminals are drawn to this information [9]. There are numerous ways an IoT system might be attacked, including blocking network availability, sending incorrect information into the network, and gaining access to user data [10].

1. **Misdirection attacks on the IoT and WSN**

WSN and IoT are vulnerable to Denial of Service (DoS), Sybil, black holes, and misdirection attacks. These attacks impede WSN performance by inflicting information loss and high energy use [11]. The Misdirection threat is the main type of DoS attack. Under this attack, data packets are sent to far-away nodes by blunder, which slows down the network and reduces its throughput [12]. Misdirection attacks can be performed in the following ways:

* The data packets are directed to a node that is close to the intended one. It get there by pursuing a route that was not intended for them, it nevertheless managed to get there in the end. Due to pursuing the wrong path the data packets are delayed and the throughput is reduced [13].
* The data packets are sent to a location that is infinitely far from the user and it never delivered to their destination. This leads to an infinite delay, and overall throughput is zero [14].

Chart, bubble chart

Description automatically generatedFigure 2 demonstrated that the reasonable route should go from 1 to 4, but a malicious attacker (M) changed it so that it goes to 6.

Figure 2: Misdirection attack; (a) normal route; (b) misdirection route [15]

1. **IoT Security**

A picture containing graphical user interface

Description automatically generatedIoT security must be handled to protect the IoT system's hardware and networks [16]. As of now, all recommended methodologies and security solutions are based on traditional network security procedures. IoT systems, make it more difficult to implement security measures [17]. Figure 3 demonstrated IoT security using various security techniques.

Figure 3: IoT security using various security techniques [18]

The field of study known as IoT security focuses on protecting linked gadgets inside an IoT ecosystem. The IoT makes it possible to enhance a wide variety of applications across many different industries. Nevertheless, the implementation of limited IoT devices and technologies in such critical applications leads to the emergence of new security issues [19]. The IoT necessarily requires the implementation of security precautions across all three layers such as the physical layer for data collection, the network layer for information routing and communication, and the application layer to preserve privacy, verification, and integrity [20].

1. **Review of Literature**

The research described the secure channel setup technique to isolate misdirection attacks on the Internet of Things. Several researchers provided the following descriptions of their findings:

**Hameed et al., (2022) [21]** demonstrated that the IoT is a new and viable network framework comprised of an enormous number of gadgets that allow people and things the ability to connect, interact, and exchange information for a variety of reasons. The IoT-based vehicular network makes it possible for vehicles currently in transit to connect and communicate in a two-way manner with other moving vehicles as well as road infrastructure to facilitate vital communications and activities. IoT devices have been subject to a large number of attacks, varying from security attacks to privacy issues, due to the restrictions of their functional skills. Attackers can easily breach IoT device authentication since they are non-tempered and adaptable. Clone node attacks on WSNs and IoT networks are hard to detect. To accelerate the verification procedure, an improved Elliptic Curve Digital Signature (ECDS) technique should be combined with a location-proof mechanism. In the end, it concluded that ECDS offers a reliable and significant attack detection rate for clone node attacks on IoT networks while simultaneously decreasing the amount of computing, memory, transmission, and energy costs.

**Kuzlu et al., (2021) [22]** investigated that the IoT is difficult to characterize since it has been developing and transforming since yet, it is possible to comprehend a system of digital and analog computer devices and machinery. IoT devices are susceptible to cyberattacks due to the various attack surfaces present in them. AI technologies like decision trees, machine learning (ML), Support Vector Machines (SVM), and neural networks have been used to keep the IoT safe. Cyber-attacks on industrial IoT systems can be detected, estimated, and compensated for using an AI-based control strategy. The Man-in-the-Middle (MITM) attack is one of the most common IoT assaults. A MITM attack permits the intruder to act as a middleman among two nodes and eavesdrop on their conversations. MITM attacks can be carried out across a wide range of networks. Finally, it was decided that the models mentioned are effective and could develop common intrusion recognition systems in the next several years.

**Ang and Seng (2021) [23]** revealed that in recent years, the IoT has been becoming increasingly significant and pervasive because of rapid advancements in detecting, computing, and platform technologies that run on the cloud. The IoT makes it possible to connect intelligent gadgets and items to massive networks so that they can be accessed from any location in the world via the internet. The use of various forms of biometric identification for verification in consumer-focused products and gadgets is quickly expanding. The rapid expansion of biometrics based IoT led to many difficulties. Hardware limitations mean that IoT devices are unable to support resource-intensive cryptography protocols. Due to the variety of biometric characteristics, biometrics equipment generates visual data. The IoT framework necessitates the incorporation of extra capabilities into previous architectures and deployments to address the Challenges of biometric identification. For IoT devices to function properly, it must be secured. Any IoT device that is connected does not have adequate security, making it vulnerable to various dangers. In the end, it concluded that the incorporation of biometric technology into linked devices for the IoT can take place within the next several years. This sector is continuing to expand as organizations seek solutions to the possible security risks posed by unsecured IoT devices that are connected to their networks.

**Huanan and Jiannan (2021) [24]** examined that the WSN is sight, with the sensor as its principal instrument. The utilization of detectors can successfully perceive the surrounding area, and then, with the assistance of wireless networks for the transfer of information, user requirements could be satisfied. As a factor of WSN's high technical depth and complicated structure, its security must be carefully considered. Otherwise, the implications of a security breach would be frightening. The utilization of WSN can encompass all aspects of a situation since it can be utilized to collect all sorts of knowledge and facts and to cope with all sorts of complex situations. The features that are shared by the WSN include liberty of organization, uncertainty regarding the topology of the network, the mechanism of control is not centralized, and the level of safety is low. In the investigation of WSN technology, security has been a major focus. WSNs are vulnerable to a variety of attacks because of their features. Security Optimization Technology (SOT), which is based on a ternary key distribution technique, was introduced in this analysis to improve the security of WSNs. According to this, it concluded that a SOT could solve the topology design and help to reduce network attacks.

**Sajwan et al., (2020) [25]** reported that the IoT is being used in a significant way in a variety of different scenarios. The IoT design is itself creating a method in which detector nodes sense data and transfer it to the base terminal. The connection is formed between the network of linked objects and the connected PCs. The Low-energy Adaptive Clustering Hierarchy (LEACH) is an extremely efficient technique that can divide an overall structure into groups of a constant size. Recognition layers are created using these groups. Data protection is one of the security requirements. clients must be assured that their information is protected and that no one can use it without the required access consent. This enables the device in question to validate and verify the credibility of the individual with whom it is collaborating using the aforementioned resource. IoT devices are becoming increasingly vulnerable to attacks, which can legitimately affect the IoT device when it is in the IoT stage, thus security is the major concern about these devices. According to the postulated and current methods, the LEACH technique performs well in terms of residual vitality and the number of dead hubs.

**Meneghello et al., (2019) [26]** indicated that the number of IoT gadgets has expanded significantly in recent years, with an estimate of around 50 billion products linked to the web in 2020. For many of these complex and personalized smart services, customers are needed to give some of their personal information to use them. The design of IoT devices and services should therefore emphasize security and privacy as a top priority. Media coverage of security assaults on industrial IoT devices has helped improve public awareness of the dangers of this emerging technology. Security should be considered while designing business IoT gadgets to be more resistant to cyber-attacks. Many IoT devices have severe restrictions in respect of energy, connectivity, computing, and storage capacities. To keep the connection secure, encryption is the first major step. Encryption ensures that a potential eavesdropper can only read the ciphertext but cannot decipher the message's content. Symmetric or asymmetric encryption can be used. In the end, it concluded that it is viable to load a modified version of the firmware to disable all of the safety features.

**Benzarti et al., (2017) [27]** indicated that the analysis of the cybersecurity of IoT has gained numerous affection from investigators. Transforming the society to be a superior environment and developing a city of aspirations which is termed a smart society is a trending subject of investigation. In this sense, everything is linked to the internet so that it can communicate with one another and make the world a more developed place. The IoT is susceptible because of the wide diversity of connections being built. Intelligent services such as those offered by the IoT, the Smart Grid (SG), smart transportation, and others enhance the lifestyles better by saving us time and energy. Several threats can disrupt the performance of every network. This research provided a taxonomy of threats coming from the many different networks that are a part of the IoT. This categorization differentiates between widespread and targeted attacks on each network by using characteristics such as the security features, the level of throughput, and the extent of disruption. It required more intricate protocols and more recent techniques to ensure the integrity of IoT networks. Several of the present methods are not sufficient to prevent an assault. The security demands for protecting the IoT are also exposed by presenting several current security methods in depth. In the end, it was determined that certain researchers are proposing the use of cryptographic methods to encrypt information that is being transmitted over an IoT network.

**Alaba et al., (2017) [28]** indicated that the IoT has lately emerged as an essential issue for exploration. Since it enables a variety of detectors and objects to connect openly with one another without the involvement of a person. The demands for the widespread deployment of the IoT are fast expanding, however, there is a huge issue over security. IoT privacy concerns and vulnerabilities are examined in this research by doing a detailed review of the information on IoT security. There is a classification of current threats to privacy in the domains of program, design, and transmission. For reasons of safety and protection, IoT devices make use of lightweight encryption technique, which involves Lightweight Cryptographic Algorithms (LCA). This analysis also evaluates potential security risks posed by the IoT. It explored the IoT privacy situation and present an evaluation of the probable threats. IoT security investigation and deployment difficulties are also discussed. IoT security risks and flaws in the diverse IoT ecosystem are documented and viable solutions for strengthening the IoT safety design can be proposed in this study.

1. **Comparison of the reviewed literature**

Table 1 shows the comparison of reviewed literature of different authors which has given below.

Table 1. Summarized table of reviewed literature

|  |  |  |
| --- | --- | --- |
| **Authors Name** | **Technique used** | **Outcomes** |
| **Hameed et al., (2022) [21]** | ECDS | ECDS reduces compute, storage, communication, and energy overhead for clone node attacks on IoT networks. |
| **Kuzlu et al., (2021) [22]** | SVM and decision tree | The models mentioned are promising, and within a few years, they could be common assault detection systems. |
| **Ang and Seng (2021) [23]** | Biometric Technology | Over the next few years, biometric technologies can be integrated into IoT-connected devices. |
| **Huanan and Jiannan (2021) [24]** | SOT | SOT has the potential to increase WSN anti-attack efficiency by simplifying the topology design of nodes. |
| **Sajwan et al., (2020) [25]** | LEACH | In terms of residual vitality and the number of dead hubs, the LEACH approach performs admirably. |
| **Meneghello et al., (2019) [26]** | Symmetric encryption Technique | With the use of a conventional encryption mechanism, it is feasible to update a modified software version and deactivate all protection features. |
| **Benzarti et al., (2017) [27]** | Cryptographic method | Making safe IoT gadgets required adapting cryptography technologies to the IoT context. |
| **Alaba et al., (2017) [28]** | LCA | It describes IoT security threats and weaknesses and gives solutions for strengthening IoT security architecture. |

1. **Background Study**

Many sensors are already being used in military and commercial applications to create WSNs. Sensor networks in remote and unsupervised situations are arranged in a variety of ways. Sensors are positioned in an unsecured area and communicate wirelessly. WSNs are susceptible to a variety of security risks, including black holes, Sybil attacks, sinkholes, wormholes, forwarding, and grey hole attacks. As the number of attacks on vital infrastructures handled by networked systems continues to rise, the development of strong intrusion detection systems is becoming more important for securing sensitive information. A safe intrusion detection system is developed using a decision tree classification model and machine learning. A decision tree IDS found a high success rate in detecting suspicious patterns using Matrix Laboratory (MATLAB) and the NSL-KDD dataset. It was tested using the NSL-KDD dataset to compare detection metrics for various types of attacks [29].

1. **Problem Formation**

WSNs are very vulnerable to assaults since systems are often unattended and lack tamper-resistant networks. Assuring the data's integrity and the reputation of sensor nodes was thus critical for WSN. For secure data transfer without any hampering, a network was required that enables efficient data transmission. The explained technique works for the enhancement of the network by making Inspector Nodes (IN) act as the cluster-head (CH) at the time when the malicious activity was being detected in the network. The current work focused on detecting malicious activities and the resolution of the same during the current transmission by giving the alternative path that was evaluated from the k-fold technique.

1. **Research Methodology**

CH and IN nodes were selected by calculating the Composite Reputation Value (CRV) value for each node. To determine the CH and IN nodes, the highest and second highest CRV values were used. The IN notify both the source node and the destination node about suspicious nodes, which was reliable and efficient (base station). It was necessary to maintain a routing table that includes information such as source, destination and time, and energy consumption. After creating the k fold path, IN performs a check for the malicious node. Unless IN detects a malicious node, the data-sharing process, and routing table were completed and updated, respectively.

* 1. **Research Technique**
* **Clustering with Residual Energy and Neighbors (CREN) Technique**

A hierarchical clustering method called CREN was presented it was based on a node's number of neighbors and its residual energy was calculated. It was based on these characteristics that selected a cluster head. A node with sufficient power and many neighbors should be prioritized as a CH in these algorithms for collecting data from the neighbors. Probability was used to select CHs. Using a set of neighboring nodes, residual energy, and several clusters in a network, each node determined whether it could be the CH only if its random number were less than a threshold value. Sensor Nodes are always energy constrained since it controlled by a battery, and it is challenging to charge the power supply of SNs because of their random deployment. Figure 4 demonstrated the cluster formation using the CREN technique.

Chart

Description automatically generated

Figure 4: Cluster formation [30]

WSNs can last longer if the following things are done:

* By ensuring that the CH is properly selected during the initial setup phase.
* By using a backup CH for the main CH in case the main CH dies.
* By using the zone routing protocol, WSNs can spread out the load.
* By displaying excellent performance, particularly when the level of mobility is high

1. **Proposed methodology**

As shown in Figure 5 below, the methodology used in this study was to verify the transfer of a packet of data from one location to another.

Diagram

Description automatically generated

Figure 5: Structural design of Proposed Methodology.

**Step 1: Display the IoT-based WSN network**

CH, because of its critical role in the IoT-based WSN, was frequently subjected to a variety of attacks from both within and outside the network. One of the most common attacks was selective forwarding, in which an attacker compromises a CH and drops all or part of the data packets that are sent to the CH in question. A self-generated dataset has been taken from https://mcfp.felk.cvut.cz/publicDatasets/IoT-23-Dataset/iot\_23\_datasets\_small.tar.gz

**Step 2: Clustering of nodes using the CREN technique**

CREN was a hierarchical clustering technique for WSN. It was based on two fundamental parameters, such as the figure of neighbors a node had and the amount of residual energy it had. CREN rotates the cluster head among the sensor nodes to maintain an even distribution of energy consumption.

**Step 3: Cluster head and inspector node selection based on RSSI value**

This network's IN and CH values were determined by their Received Signal Strength Indicator (RSSI) values, with the highest RSSI value acting as the cluster head and the next node with the second highest RSSI value acting as the inspector node, and the computation was dependent on the energy level, forwarding rate, and other characteristics of the nodes.

The original energy level of the network is 1, and the excess energy of the nodes was . The CRV for the node was , and was the forwarding rate for the given node.

(1)

Where Val is the CRV value of the particular node a and b were specified constants with values ranging from 0<a, b<1, and a+b=1.

**Step 4: Generate K-Fold path from source to destination**

Networks employ this to determine the best secure and quickest routing path possible, and it was generated by using the k-fold path routing strategy. This function was used to compute the Round Trip-Time (RTT) that was applied to each path in a network.

**Step 5: Inspector Node training via machine learning**

The IN was trained to determine whether the Member Nodes (MN) or CH were malicious or not and to respond appropriately based on certain criteria and established parameters, as appropriate.

**Step 6: Training of Malicious Act**

Next, if the entire path is efficient according to the routing table, IN checks for malicious activity. The next best path was chosen if any malicious activity was detected by IN, which then marks CH as a malicious node. Otherwise, finish the transmission of data and update the routing table if necessary.

**Step 7: IN Communication**

If RTT was greater than Threshold (TH), then IN gathers the complete communication and replaces the stocking nodes with them.

1. **Conclusion and Future scope**

**References**

Kaur, Bhavkanwal, and Puspendra Kumar Pateriya. "A Security Framework for Detection and Prevention of Misdirection Attack in Wireless Sensor Networks for IoT." environment 12, no. 13: 14.

Malik, Chirag, and Vikas Sindhu. "Analysis of Energy Efficient Techniques for Wireless Sensor Networks." (2019).

Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions, and future directions." In 2016 49th Hawaii International Conference on System Sciences (HICSS), pp. 5772-5781. IEEE, 2016.

Abie, Habtamu. "Adaptive security and trust management for autonomic message-oriented middleware." In 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, pp. 810-817. IEEE, 2009.

Mosenia, Arsalan, and Niraj K. Jha. "A comprehensive study of security of internet-of-things." IEEE Transactions on emerging topics in computing 5, no. 4 (2016): 586-602.

Khan, Zeeshan Ali, and Peter Herrmann. "Recent advancements in intrusion detection systems for the internet of things." Security and Communication Networks 2019 (2019).

Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an analysis of security issues, challenges, and open problems on the internet of things." In 2015 IEEE world congress on services, pp. 21-28. IEEE, 2015.

Riahi, Arbia, Yacine Challal, Enrico Natalizio, Zied Chtourou, and Abdelmadjid Bouabdallah. "A systemic approach for IoT security." In 2013 IEEE international conference on distributed computing in sensor systems, pp. 351-355. IEEE, 2013.

Chandrakanth, S., K. Venkatesh, J. Uma Mahesh, and K. V. Naganjaneyulu. "Internet of things." International Journal of Innovations & Advancement in Computer Science 3, no. 8 (2014): 16-20.

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29, no. 7 (2013): 1645-1660.

Mustafa, Iqra, Sheraz Aslam, Muhammad Bilal Qureshi, Nouman Ashraf, Shahzad Aslam, Syed Muhammad Mohsin, and Hasnain Mustafa. "RL-MADP: Reinforcement learning-based misdirection attack prevention technique for WSN." In 2020 international wireless communications and mobile computing (IWCMC), pp. 721-726. IEEE, 2020.

Sachan, Roshan Singh, Mohammad Wazid, Dhirendra Pratap Singh, and R. H. Goudar. "A cluster-based intrusion detection and prevention technique for misdirection attack inside WSN." In 2013 International Conference on Communication and Signal Processing, pp. 795-801. IEEE, 2013.

Dhulkar, Ruchita, Ajit Pokharkar, and Ms. Rohini Pise. "Survey on different attacks in Wireless Sensor Networks and their prevention system." (2015).

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54, no. 15 (2010): 2787-2805.

Yang, Guang, Lie Dai, and Zhiqiang Wei. "Challenges, threats, security issues and latest trends of underwater wireless sensor networks." Sensors 18, no. 11 (2018): 3907.

Hassan, Wan Haslina. "Current research on the Internet of Things (IoT) security: A survey." Computer networks 148 (2019): 283-294.

Zhang, Zhi-Kai, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. "IoT security: ongoing challenges and research opportunities." In 2014 IEEE 7th international conference on service-oriented computing and applications, pp. 230-234. IEEE, 2014.

Hassija, Vikas, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

Jurcut, Anca D., Pasika Ranaweera, and Lina Xu. "Introduction to IoT security." IoT security: Advances in authentication (2020): 27-64.

Mahmoud, Rwan, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. "Internet of things (IoT) security: Current status, challenges, and prospective measures." In 2015 10th international conference for internet technology and secured transactions (ICITST), pp. 336-341. IEEE, 2015.

Hameed, Khizar, Saurabh Garg, Muhammad Bilal Amin, Byeong Kang, and Abid Khan. "A context-aware information-based clone node attack detection scheme in the Internet of Things." Journal of Network and Computer Applications 197 (2022): 103271.

Kuzlu, Murat, Corinne Fair, and Ozgur Guler. "Role of artificial intelligence on the Internet of Things (IoT) cybersecurity." Discover the Internet of things 1, no. 1 (2021): 1-14.

Kuang, Boyu, Anmin Fu, Willy Susilo, Shui Yu, and Yansong Gao. "A survey of remote attestation in the Internet of Things: Attacks, countermeasures, and prospects." Computers & Security 112 (2022): 102498.

Huanan, Zhang, Xing Suping, and Wang Jiannan. "Security and application of wireless sensor network." Procedia Computer Science 183 (2021): 486-492.

SAJWAN, MRS MANISHA PUNDIR, MR PRAMOD SAJWAN, and MR ANUJ CHANDILA. "IN INTERNET OF THINGS IMPERATIVENESS EFFICIENT TECHNIQUE FOR DATA AGGREGATION." (2020).

Meneghello, Francesca, Matteo Calore, Daniel Zucchetto, Michele Polese, and Andrea Zanella. "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices." IEEE Internet of Things Journal 6, no. 5 (2019): 8182-8201.

Benzarti, Sana, Bayrem Triki, and Ouajdi Korbaa. "A survey on attacks in the Internet of Things based networks." In 2017 International conference on engineering & MIS (ICEMIS), pp. 1-7. IEEE, 2017.

Alaba, Fadele Ayotunde, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. "Internet of Things security: A survey." Journal of Network and Computer Applications 88 (2017): 10-28.

Gebremariam, Gebrekiros Gebreyesus, J. Panda, and S. Indu. "Secure Intrusion Detection System for Hierarchically Distributed Wireless Sensor Networks." In 2021 International Conference on Industrial Electronics Research and Applications (ICIERA), pp. 1-6. IEEE, 2021

John, Aniji, and K. Vinoth Babu. "Two phases dynamic method for cluster head selection in a wireless sensor network for Internet of Things applications." In 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1228-1232. IEEE, 2017