International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 3 Article 4

March 2022

A Comprehensive Study on Security in Wireless Sensor Networks(WSNs)

Sucheta Panda
SIKSHA O ANUSANDHAN DEEMED TO BE UNIVERSITY, bimalabibhuprada@gmail.com

Sushree Bibhuprada B. Priyadarshini
SIKSHA O ANUSANDHAN DEEMED TO BE UNIVERSITY, bimalabibhuprada@gmail.com

A Comprehensive Study on Security in Wireless Sensor Networks(WSNs)

Cover Page Footnote

The authors are highly grateful to the Department of CSE and CS&IT of Siksha 'O' Anusandhan Deemed to be University for making this investigation successful.

A Comprehensive Study on Security in Wireless Sensor Networks(WSNs)

Sucheta Panda[a], Sushree Bibhuprada B. Priyadarshini [b]
[a] Siksha O' Anusandhan University, Bhubaneswar, India, suchetapanda10@gmail.com
[b] Siksha O' Anusandhan University, Bhubaneswar, India, sushreepriyadarshini@soa.ac.in

Abstract

Wireless Sensor Networks(WSNs) are an important component of today's ubiquitous and pervasive computing. Without WSNs, the applications aren't as clever as they could be. Almost every scenario involving WSNs necessitates a quick and precise localization process. Existing frameworks and algorithms, on the other hand suffer from a significant disadvantage when it comes to beacon node trust, which is a critical component in Wireless Sensor Network. For localization this has to be ensured.. This issue is addressed in our current solution. In the harsh environment of WSN operations, malicious nodes are inescapable. As a consequence, A technique has been proposed to find out the problem while simultaneously offering a safe trust based localization system. It focuses on the algorithm for assessing trust and the creation of blockchains. Every beacon node's truth value(trust value) are determined using various trust criteria with the corresponding weights being dynamically changed during localization process. After that the most reliable beacon nodes are chosen for mining. This two-step process ensures that the blockchain is kept up to current, and that beacon nodes have consistent T_{values}(Trust values). We conducted a series of simulations to test the suggested algorithm's performance and effectiveness. The accuracy of localization, harmful activity detection, the confusion matrixes are used to compare results.

Keywords
Beacon node, Block chain, Confusion matrix, Trust values

1. Introduction

WSN is a network of small inculcated devices called "motes" that is used for monitoring physical environment[1]. After that data is transferred to a sink node or base station at the designated location. The importance of WSN broadly used in industry, military, smart homes[2] and also in hospitals. Sensor node position information is crucial in various applications for assuring the correctness of the data collected.

WSN is an infrastructure free wireless network that monitors system, physical and environmental conditions by deploying a large number of wireless sensors adhoc. They're linked to the WSN System's processing unit, the Base Station. A WSN system's base station communicates with each other over the Internet.Fig.1. explains the scenario of a Wireless Sensor Network briefly.

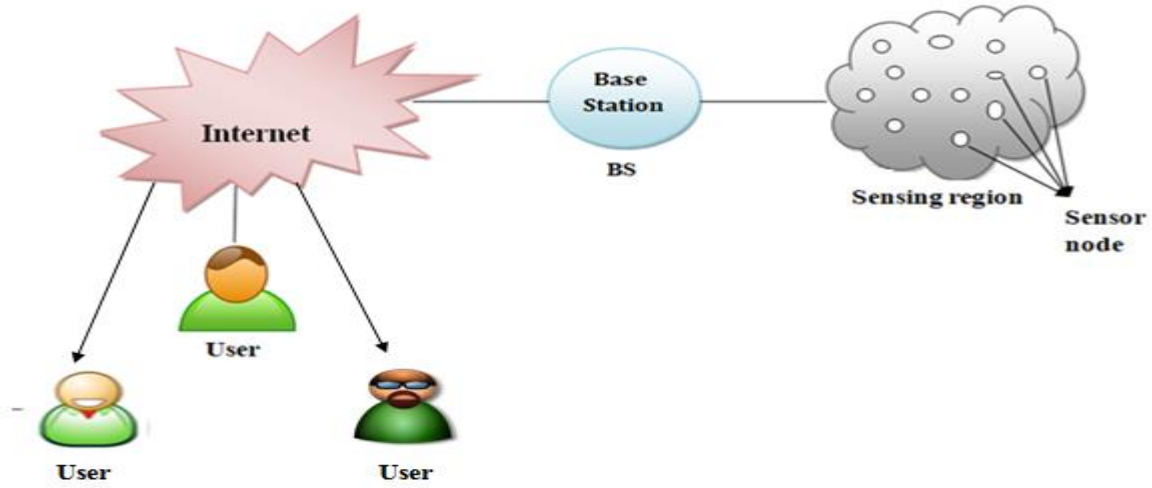

Fig. 1. A Scenario of Wireless Sensor Network

The process of determining the location of sensor nodes is referred to as localization. Because of the adverse environment in which WSN operate with random deployment and dynamics, the process of localization is sensitive to several attacks. WSNs are also vulnerable to various dangerous behaviours that could cause sensor node failure [4,5].Secure localization algorithms are available to protect against various harmful assaults. They are classified into 3 types:

i.location based on large amount of surveillance
ii.depending on the attacker's node separation
iii.confirmation of location

Limiting the distance between attacker nodes prevent them from interfering with the localization process in the first category. The attacker sensor nodes are separated barriers for observation in second strategy, which prevents false localization. An attacker node is isolated in the third form by combining a specified set of neighbour sensors with a scheduled deployed position. Though the aforementioned methods for safe localization are not without flaws, they do face a number of challenges[6].

The secure localization techniques discussed above contain vulnerabilities, and WSNs are working on fixes. As a result trust is critical during the localization process. When sensor node trust is maintained, the position estimation process can be improved[7,8]. Fig.1. express a scenario of Wireless Sensor Network.

Some secure localization approaches employ location verification to mitigate the impact of incorrect or faulty data[9].Therefore employing blockchain technology to evaluate a trust evaluation based secure localization appears to be intriguing. By increasing localization accuracy, we can approximate the position of nodes under difficult scenarios.

• For WSNs, a blockchain-based trust evaluation-based localization technique is described, which allows every beacon nodes to decentralized the updating of their trust values.

• The beacon node can now add the trustworthy block to the blockchain thanks to a Proof-of-Stake consensus.

1. 1. Motivation

There are various applications of WSN. Those are:-

a. Process Management:WSNs are often used to monitor large areas. The WSN is used to monitor a specific event through out a region. The uses of sensors for identifying enemy penetration is the military example of and Geo-fencing of gas or oil-pipelines is the civilian example.Air surveillance is the most critical component.

b. Healthcare monitoring: Wearable or implantable medical uses are possible. The user's skin is covered with wearable electronics and our bodies are surgically implanted with implantable medical devices.Body posture assessment and monitoring as well as general patient monitoring in hospitals and at home, are some of the other applications.

c. Environmental/Earth sensing: Environmental monitoring is useful for a variety of reasons, some of which are given below. They discuss any additional challenges brought on by the harsh weather and lack of power.

d. Polluting of the environment monitoring: In many cities WSNs have been developed to track the power of dangerous compounds for residents(Stockholm, London and Brisbane).These can use ad hoc wireless connections instead of cable connections.

e. Forest fire detection:A collection of sensor nodes is usually created in a forest to detect when a fire has started.For measuring temperature, humidity and gases produced by fire in trees or crops, sensor nodes are used. Fire brigade can recognize when a fire starts and spreads thanks to Wireless Sensor Networks.

f. Landslide detection:A wireless sensor network is used in a landslide detection system to detect small soil movements and charges in a variety of factors that occur in the time of landslide or prior to it. Based on information acquired, it might be feasible for prediction when landslides may occur.

g. Monitoring of water quality: Dams, rivers, lakes and seas as well as underground water reserves, all have their water quality monitored.Without the requirement for human data retrieval, a large number of wireless dispersed sensors can be used for creating an exact map of water state and permanently deploy monitoring stations in difficult-to-reach areas.

h. Natural disaster prevention: Floods can be mitigated via wireless sensor networks. In rivers where realtime monitoring of water levels is essential, wireless nodes have been effectively used.

i.Industrial monitoring:

- **Machine health monitoring:**WSN have been increased for condition based maintenance in machinery due to the huge cost savings and new possibilities they provide.The cost of wiring in wired systems is typically linked to the number of sensors deployed.
- **Data logging:**WSNs are frequently used to collect web data for environmental monitoring; this can include everything from monitoring the temperature of a refrigerator to the quantity of water in overflow tanks at nuclear power plant.The statistical data will subsequently be used to show how well the systems have performed. The ability to receive "live" data flow is the key advantage of WSNs, over traditional loggers.

Though there are various applications of WSN, still there are some challenges.

Some major challenges are listed below:-

a) **Resource Constraints**

The sensor network's main constraint is the sensor node's battery power. The power source has a direct impact on the sensor node's effective timeline. Therefore, the power source has an impact on the sensor network's lifespan. The physical layer decisions made by a sensor node have an impact on the device's total energy consumption and the design of higher level protocols. So, the protocol's prime priority is energy consumption. Another stumbling point is the amount of data that can be stored in individual sensor nodes because to limited computing power and memory size. As a result, the protocol should be easy to understand

b) Security

A wide number of WSNs collect private information. Sensors that are operated remotely and without supervision are more vulnerable to hostile intrusions and attacks. Wireless connections can make listening in on sensor transmission easy for an enemy. A denial-of –service attack, which aims to prevent a sensor network from functioning properly, is one of the most dangerous security threats. While there are different distributed systems tactics and solution that can prevent assault or restrict the breadth and damage of attacks, many of them have enormous computation, networking and storage requirements that resource-constrained sensor nodes can not meet.As a result, unique mechanisms for key generation and distribution, node authentication and secrecy will be required in sensor networks.

c) Quality of Service

Some real time sensor applications are very time-sensitive, requiring data to be delivered within a specified period of time after it is perceived, or else data will be useless. Therefore for some applications this will require a QOS configuration. The RAP protocol for example introduces a new policy known as velocity monotonic scheduling.A package will include a deadline as well as a travel distance. Packages are scheduled for transmission based on the highest velocity need of any packet at this node, and these attributes are utilised to establish a package's average velocity requirements.There are no guarantees with this protocol, which handles real-time.

SPEED is a routing protocol that is based on real-time data. Feedback control is used in this protocol to ensure that packets transiting a node have an average latency. Due to transient behaviour, message loss, congestion , noise and other factors, these guarantees are limited.Data fusion, data transfer, target and event detection, categorization and query processing are some of the functions that must meet real time requirement.

d) Heterogeneity and Complexity

The more variety a network has, the more powerful and generic it becomes.However it involves the adoption of more sophisticated and robust routing and communication protocols.

e) Fault-Tolerance

A sensor node may fail in a hostile environment owing to physical injury or a lack of energy(power). When some node fails, the currently used protocols must adapt to the new network configuration. For example, find acceptable paths or aggregation locations in the event of routing or aggregation protocol failures.

f) Scalability

The bulk of applications are required, and hundreds of thousands, if not millions, of sensor nodes must be installed. To respond and function with a high number of sensor nodes, protocols must be scalable.

1.2.Security Attacks

Due to the nature of transmission medium, two types of assaults are common in wireless sensor networks.

i. Active attacks
ii. Passive attacks

Passive attackers just aim to carryoff critical information like passwords and personal information, whereas active attackers want to find and destroy information. For communicating securely between sensor nodes in a wireless network, individuals and organizations need to aware of these dangers.The active attack scenario in a WSN is shown in fig.2 and Fig.3. describes about passive attack scenario. In Fig.4. clearly explains about types of attacks occurs in WSNs.

1.2.1. Active Attack

- Active attacks occur when the attacker tries to manipulate or change the content of messages. Active attack poses integrity and availability.
- Active attacks always cause damage to the system, and the resources of the system can be changed.
- The fact that the victim was told of the attack while it was still happening is crucial.

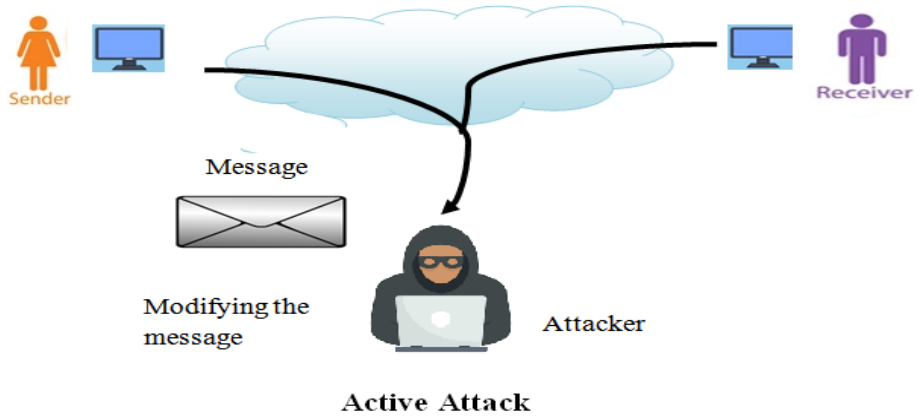

Fig. 2. Active attack scenario

1.2.2. Passive Attack

- The attacker can view or copy the contents of messages in passive assaults.
- Passive attacks are a concern in this attack because secrecy is at risk. Passive attack does not cause any damage to a system.
- The key element of passive attack is that the victim is fully unaware of the attack.

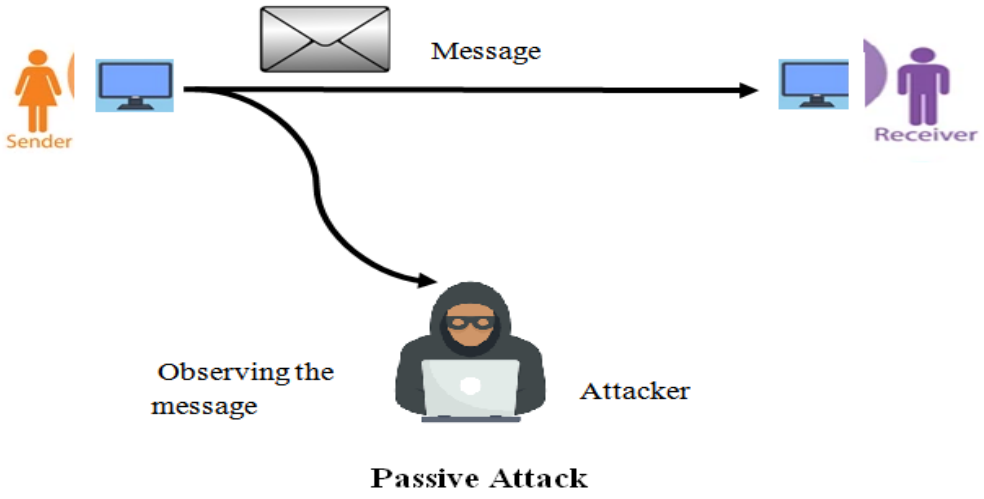

Fig. 3.Passive attack scenario

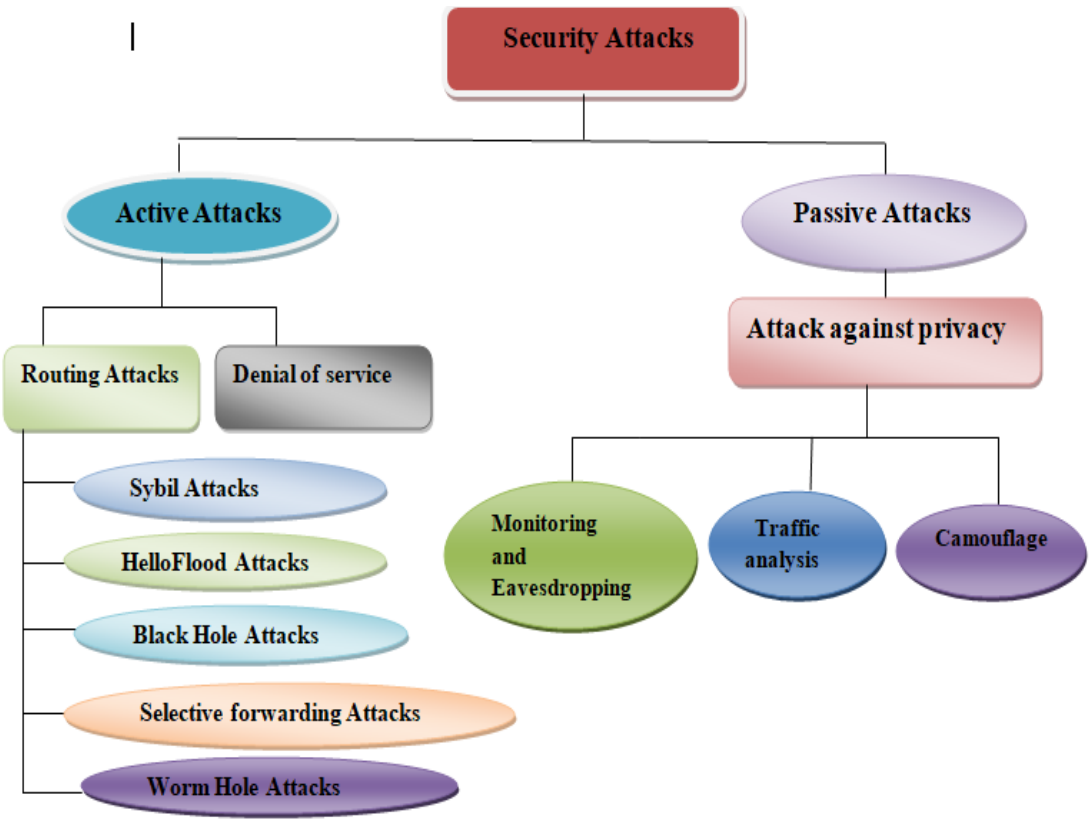

Fig. 4. Types of Attacks

1.2.1.1. Denial of Service(DoS)

In WSNs, DoS attacks are very common. The physical layer is attacked by spreading a signal that interferes with the sensor's network's radio frequencies. Continuous jamming can be performed by set of node devices or a strong device. Based upon the jamming process

is carried out, the attacker can disable the sensor network in many ways.From the datalink layer, DoS attacks can be initiated. The attacker either destroy or redirect the infrastructure configuration of the sensor network[10].The routing protocol is the target of network layer DoS attacks. A DoS attack at the transport layer is also conceivable, although it is highly dependent on network's transport layer protocol.

1.2.2.2. Routing Attacks

WSN routing protocols are the target of numerous assaults, all of which are insider attacks, as is the case with virtually all networks.

- **Selective forwarding Attack**

  In this attack, a node plays the role of router and here malicious nodes may deny to forward messages and simply drop them. However such an attacker runs the risk that neighbouring nodes will conclude that this node has failed and decides to seek another route.Fig.5 narrates about the framework of selective forwarding attack.

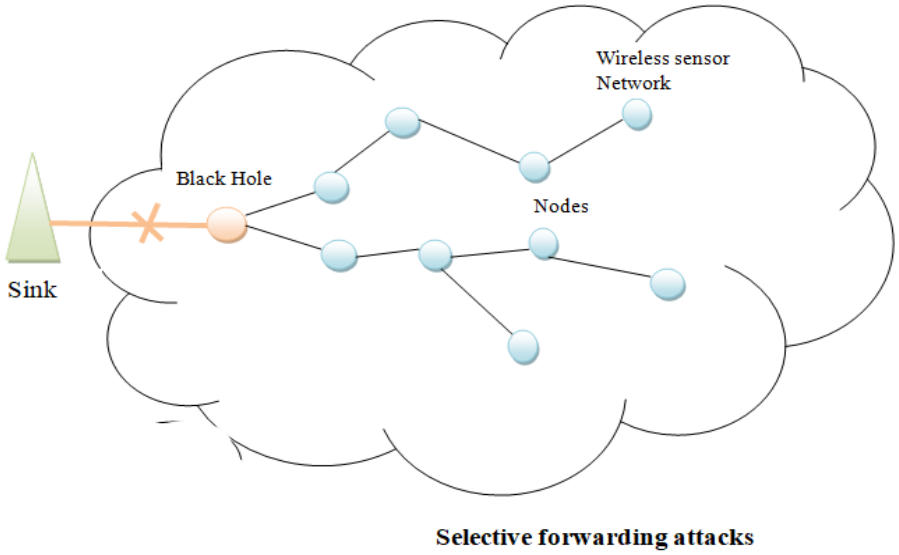

Fig. 5.Framework of Selective forwarding attack

- **Sybil Attack**

  A single malicious node is used in a Sybil attack to assume several identities. This one node can impair fault tolerant systems like topology maintenance, multipath routing , distributed storage etc. The structure of Sybil attack has been described clearly in Fig.6.

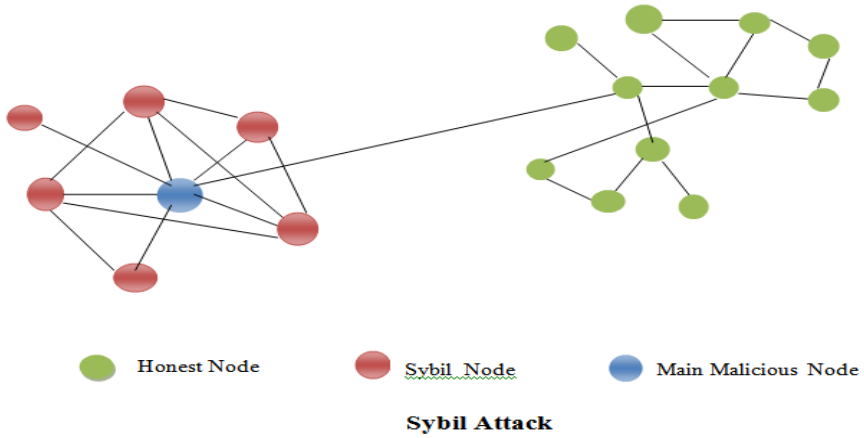

Fig. 6.Framework of Sybil attack

- **Wormhole attack**

  When the rouge node receives a packet, it send it to another sensor network site over second a low-latency channel. This type of attack can be launched without the knowledge of the network. Here delay in packet delivery occurs and it fails to findout the valid routes.The concept of Wormhole attack occurs in WSN has been discussed in Fig.7.

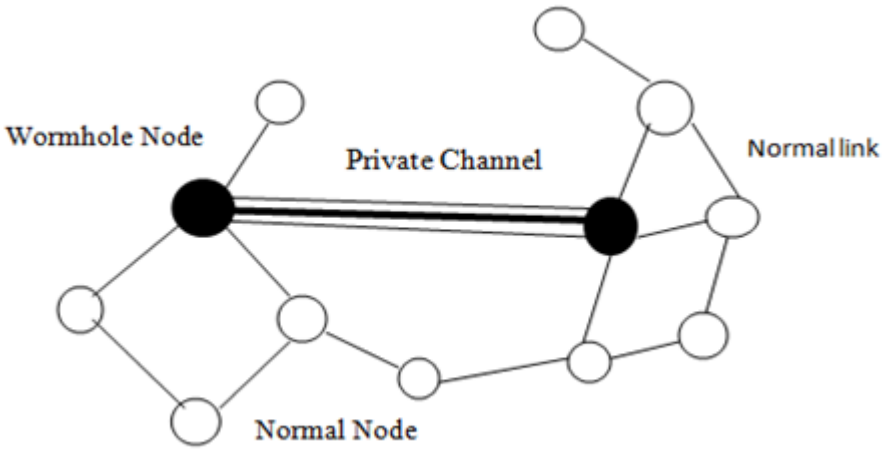

Fig. 7.Framework of Wormhole attack

- **Sinkhole Attack**

  In this attack attacker node takes the position of sink node and it behaves like its base station, so everyone starts sending data by believing that it is the base station. The sink node consumes all information from various nodes and does not work properly. So we think that our working is processing, which is our wrong assumption. The concept of Sinkhole attack in WSN has been described clearly in Fig.8.

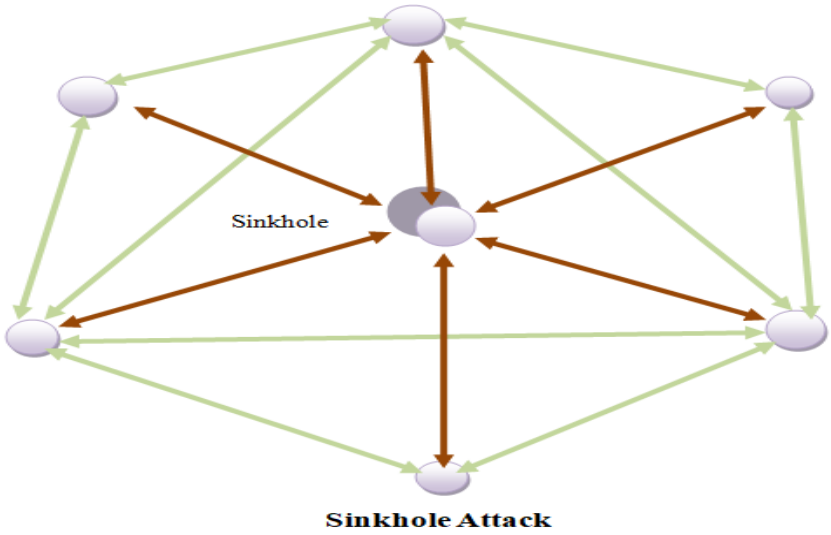

Fig. 8.Structure Sinkhole Attack

Attack against privacy

- **Monitoring and eavesdropping:-**

Attacks on network integrity are unaffected by eavesdropping. The attackers eavesdrop on the data to find out the communication channel and breach the network security[11].It's the most typical data-privacy breach.

- **Traffic analysis:-**

  The attacker examines the communication patterns in this form of assault. Through any active attack, the attacker provides the structure to the opponent in order to harm and help damage to WSN. To prevent this assault, the network is continually monitored.

- **Camouflage:-**

  The attacker impersonates a regular node in WSN and hides required number of nodes, causing packets to be misrouted to alternative communication channels.

There are some security solutions also available. Different types of existing solutions with its pros and cons are described in Table.1.

- 802.15.4
- Zigbee
- Bluetooth
- TinySec
- MiniSec
- Spins
- SecureSense
- AMSecure
- Sizzle

Table .1. Existing solutions

Type of Solutions	Advantages	Disadvantages
802.15.4	data encryption, frame integrity and sequential freshness , High Security	Problems with the feasibility of supporting different keying model
Zigbee	Verylong battery life, more reliable ,less complex than bluetooth.	It is not secure like wifi based secure system, low data speed, low complexity
Bluetooth	providing authentication, confidentiality and authorization.	Number of attacks present bluesnarfing , bluebugging and bluejacking.
TinySec	Ease of use and transperancy	no key exchange mechanisms are included, limited platform support.
MiniSec	authenticated encryption using OCB(Offset code book) mode, strong replay protection without the transmission overhead	limit the length of the 802.15.4 packets by overloading the length field
Spins	data confidentiality, two party authentication and data freshness, efficient broadcast authentication.	Not include any key management mechanisms for exchanging, updating or revoking keys.
Secure Sense	Improves overall operational efficiency , reduce risk across all platforms	difficult to determine if it is a practical solution, not provides any real energy saving
AM Secure	message confidentiality, authentication, integrity, replay protection and semantic security.	AM Secure lies in its lack of portability, difficult to port to a platform that uses a different radio chip.
Sizzle	very impressive code size, memory usage and speed for the services it provides	In terms of energy consumption, cannot be considered a suitable benchmark.

1.3. Frame Model

a) Network model:-

For sensing we use a 2-D environment to set beacon and unknown nodes. By definition all beacon and unknown nodes are static. Then resources available to beacon nodes are more than those available to non-beacon nodes.

$$N = M + u$$

M- beacon nodes

u- unknown nodes

• Both applicants and validators can use the beacon nodes.

• The packets are initially transmitted by the beacon nodes to their neighbouring beacon nodes. Fig.9. clearly discuss about the formation of packet and the parameters used in it. The following are the representation of broadcast packets:

$$packet_i = \left\{Id_i, location_i^c, timestamp, E_{residual}^i\right\}$$

$$Id_i = address\ of\ ith\ beacon\ node$$
$$location_i^c = represnts\ the\ measured\ position$$
$$E_{residual}^i = residual\ enegy\ of\ beacon\ node$$

Fig.9 .Representation of broadcast packet

• All beacon nodes can find their true location and there are no localization errors.
• The beacon node reports its position, which is similar to $location^c(location_{true})$.

b) Attack model

The algorithm's operation can be disrupted by assaulting it at many stages, including gathering location data, calculating distance between nodes and validating the projected position.

External as well as internal nodes can carry out these assaults. A sensor node can be compromised, and the identities of legitimate nodes can be tampered with. The adversary's goal is to figure out where the node is located and create true uniqueness for nodes.

An attacker can use benign nodes to carry out the following actions:

• $Malicious_i$refers to the sum of attacker nodes, where maliciousnodes are defined as(1,2,3,4……K<<M).

• As seen below, compromised beacon nodes can intentionally send out false location packets to their neighbours:

$packet^{false}{}_i$={Id_i, $location^c{}_i$, timestamp, $Ei_{residual}$},
where,$location^c{}_i \neq location_{true}$.

The suggested algorithm is split into two sections:
a) beacon node assessment of trust
b) The creation of block chain

Using Direct trust(D_{trust}) and Indirect trust(I_{trust}) trust value of beacon node is calculated. Then blockchain creation process starts using most reliable beacon node.

2. Trust value evaluation

Each beacon node's trust value($Trust_v$) is initially taken 0.5,demonstrating that each network node is trustworthy from the start. Information integrity(m1), node reputation(m2), and residual energy(m3) are used to calculate $Trust_v$, which is then used to provide $Trust_v$ for I_{trust}(m4).D_{trust} is calculated using these metrics.With two counters, each beacon node counts the number of observations.i.e. Pcount and Ncount, which are initially set to 0[12].

2.1. Direct trust evaluation

By emitting $packet_i$ to its surrounding beacon nodes, beacon nodes forward information. The estimated distance is calculated by each of the beacon nodes.

Estimated distance $D^{est}_{ij,}$ using speed and Co-ordinated distance D^{co}_{ij}using coordinates of the nodes respectively.

In the model, the received power is calculated as follows:

$$P_R = P_T \times G_T \times G_R \times \frac{(\lambda)^2}{(4 \times \pi \times D)^2}$$

Where,

P_R : Received power at beacon node's receiver antenna.

P_T : Transmitting power

G_T, **G_R** : Gain (Transmitter)antenna and Gain (Receiver) antenna

λ : Wavelength

D : Distance

$D_{ij}^{est} = \frac{k}{\sqrt{P_R}}$Where,

k - Constant

D^{est}_{ij} - Sensor nodes I and j are separated by estimated distance.

The following equation is used by all beacon nodes to compute the reputation of their neighbours:

$$R_{t+1}^{Bij} = \alpha \times R_t^{Bij} + (1 - \alpha)$$

Where,

R_{t+1}^{Bij} and R_t^{Bij} : The Beacon node Bi's reputation by Bj in the time't' and 't+1' respectively. At first ,$R_t^{Bij}$is set as 0.5, V beacon nodes.

α : The following is how the weight for reputation value is calculated:

$$\alpha = \frac{\left|D_{ij}^{CO} - D_{ij}^{est}\right|}{D_{ij}^{CO} + D_{ij}^{est}} \quad , \; E_{residual} \geq E_{Thresold}$$

Where, $E_{\text{Threshold}}$ represents the threshold energy.

The computation of D_{trust} is executed with two components:

- weight computation ($weight_{mi}$)
- expectation computation

The value of (**$weight_{mi}$**) indicates the importance of a specific trust metric and is calculated as follows:

$$weight_{mi} = \frac{P_{count(mi)}}{\sum_{i=1} 4 \; P_{count}(mi)}$$

The **$Expectation_{(mi)}$**is a statistic that measures how important beacon nodes are in meeting the requirements of the trust metric m_i.

$$Expectation_{(mi)} = \frac{P_{count}(mi) + 1}{P_{count}(mi) + N_{count}(mi) + 2}$$

The following equation is used to calculate**D_{trust}**:

$$D_{Trust}(k) = \sum_{i=1} 4\ weight_{mi} \times Expectation_{mi}$$

2.2. Indirect trust evaluation

$$I_{trust}(k) = \sum_{(i=i)} 4 \frac{P'_{count}(mi)}{(P'_{count}(mi) + N'_{count}(mi))}$$

I_{trust} is used to express the indirect trust value of kth beacon node(k). $Trust_v$is calculated for each beacon node by combining D_{trust} and I_{trust} values and adding weights indicated by $w_{direct}$and $w_{indirect}$.

$Trust_v$is evaluated as follows:

$$Trust_v(k) = w_{direct} \times D_{Trust}(k) + w_{indirect} \times I_{Trust}(k)$$

The blockchain is created using the trust values that have been evaluated.

2.3. Blockchain

Blockchain technology is a peer to peer network of nodes that maintain public transactional records, referred to as blocks, in several databases, referred to as "chain".This sort of storage is commonly referred to as "ledger".The owner's digital signature authenticates and protects every transaction in this ledger against tampering. So the digital ledger's data is incredible secure. Blockchain technology has a lot of promise to encourage decentralization and enable novel transaction patterns and interactions in the IoTs[13].A blockchain and reinforcement-based trusted routing approach was created to improve the security of WSNs even further. Node routing information is stored in the block chain to make tampering more difficult and more reliable routing links is selected by reinforcement learning[14].ForVANETs, researchers designed a decentralized trust management system with Blockchain-based Anonymous Reputation System(BARS)[15].Fig.10. explain about the structure of Blockchain technique in detail.

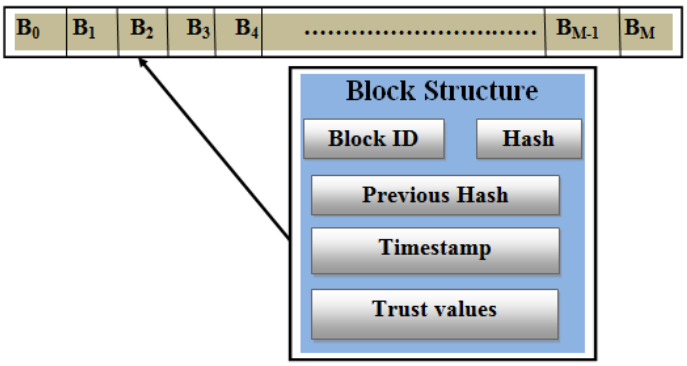

Fig.10. General structure of a block

Block chain is a new technique that has variety of advantages in this smart and digital era.

- **Highly Secure:**When digital signature technology is used to complete a fraud free transactions, it is quite problematic for other users to modify an individual's data without a unique digital signature.
- **Decentralized System:**Transactions are normally authorized by regulatory entities such as government or bank but in case of block chain technology transactions are done by userconsensus so that we get faster, smoother and secure and safer results**.**
- **Automation Capability :** It's adaptable, and if the trigger's conditions are met, it can initiate a series of actions, events and payments on its own.

2.4. Benefits of Blockchain technology with the proposed scheme

- **Decentralization:**Blockchain technology is built on a distributed system that is resistant to single points of failure and central authority is not needed.
- **Anonymity:**Members of blockchain network can converse anonymously.In the proposed system, instead of using a produced public address, they use a created public address for communication.
- **Auditability:**Because of transaction lists are linked, the current transaction must be related to previous one. As a result the series of transaction can be generated, each of which can be verified and recorded, assuring auditability and immutability.
- **Secure:**Hashing techniques are used to safeguard to the blockchain technology, ensuring that data on the ledger cannot be changed with and remains attestable.So, we can verify our suggested localization scheme.
- **Transparency:**A transaction should be able to be verified by anyone on network. The addition of a transaction in a new block may be seen by all nodes in the network, and all transactions are exposed to all members [17-20, 30-47].

3.Pros and Cons

3.1 Benefits of WSN

- It's scalable, so it can cope with any new nodes or devices that appear.
- Physical partitions are not an issue because it's adjustable.
- All WSN nodes can be accessed through a centralized monitoring system.
- Because it is wireless, it does not require any wires or cords.
- WSNs can be utilized in a variety of areas, including mines, healthcare, surveillance, agriculture and so on, on a large scale.
- It employs a number of security techniques that are compatible with the underlying wireless technology, resulting in a reliable network for consumers and users.

3.2. Drawbacks of WSN

WSN has the following disadvantages:

- It is vulnerable to hacking due to its wireless nature.
- Because it was designed for low speed purpose, it can not be used for high speed communication.

- Building network like this is expensive, not everyone can afford it.
- In a WSN there are numerous aspects to consider, including Energy conservation, restricted bandwidth, Cost of node, Paradigm of deployment, Design restriction in software and hardware and so on.
- Failure of a central node in a WSN with star topology leads the entire network to shut down.

4. Applications

WSN have a wide range of applications in a variety of industries:

- **Military Applications:** WSNs can be quickly deployed for monitoring and to offer battle field intelligence on chemical, biological and nuclear weapon's locations and detections.
- **Area Monitoring:** A symmetrical arrangement of sensor nodes is laid out across a display area. When the sensors detect an event(such as change in temperature and pressure), one of the base stations(BS) receives the information and takes action.
- **Transportation Applications:** WSNs gather real time traffic data to feed transportation models and alert drivers for impending road blocks and traffic problems. For traffic control and monitoring ,WSN is used.
- **Health monitoring:** There are various kinds of sensors which can measure blood pressure, body temperature and ECG. Body sensor network is special kind of sensor network that helps continuous and ambulatory health monitoring with real time update and medical records via internet.
- **Environmental Applications:** Environment Sensor networks(ESNs) has come to mean a wide range of WSN applications in environmental and earth science research. Oceans, seas, glaciers, the atmosphere, volcanoes and forests are only few of the things that make up the natural world. Several biosensors, on the other hand have been developed for agricultural and environmental applications. Monitoring and management of air pollution, forest fire detection, monitoring and control of green house gas(GH), and landslide detection are all critical challenges.
- **Industrial Applications:** WSNs make it possible economically to monitor the 'health' of machines and to ensure safe operation by collecting sensor nodes into machines.The amount of wiring required in wired categories frequently restricts the number of sensors that may be installed.
- **Agricultural Applications:** Farmers have noted that using WSNs helps them with a variety of tasks, including maintaining wiring in a challenging environment, implementing irrigation systems that help them use water more efficiently, and reducing waste.

5. Conclusion

To address numerous security problems of localization, a trust evaluation model based on block chain primitives is proposed in this work. When compared to a model without trust , the graph of unknown nodes versus localization error yielded an accuracy of 51.71%. Still there is significant amount of localization error which further needs to be reduced. So we aim to develop a model that can further reduce the

localization error.In the graph of number of beacon nodes versus Average localization error(ALE) ,we observe that number of beacon node increases, ALE of all the algorithms decreases effectively . So we aim to produce a model that can further reduce the ALE.In the graph number of beacon nodes versus probability of finding true locations of unknown nodes increases as the number of beacon node increases. We aim to design a model which will help to find out more accurate result than the result which has been shown here.In the graph no. of malicious nodes versus probability of finding true locations we observe that when the number of malicious nodes increases , the probability of discovering true locations reduces . we aim a model which will give better result than the proposed algorithm.In the graph of number of malicious node versus False Positive Rate(FPR) shows that when the number of malicious node increases FPR of all the algorithms increases . But the algorithm which has been proposed here has least percentage of FPR as compared to existing algorithm .We aim a model which gives better result as comparison to previous ones.

6. REFERENCES

[1] B. Rashid, M.H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey", J. Netw. Comput. Appl., vol. 60, pp.192–219, 2016.

[2] B. Mukherjee, D. Ghosal, Wireless sensor network survey, Comput. Netw. vol. 52 ,no.12, pp.2292–2330, 2008.

[3] D.I. Curiac, "Anchor node localization for wireless sensor net-works using video and compass information fusion, Sensors (Switzerland)" vol. 14, no. 34. pp. 211–4224,2014.

[4] P.R. Vamsi, K. Kant, "Trust and location-aware routing protocol for wireless sensor networks", IETE J. Res. vol.62 no-5, pp. 634–644, 2016.

[5] T.H. Kim, et al., "A novel trust evaluation process for secure localization using a decentralized block chain in wireless sensor networks", IEEE Access vol. 7, pp. 184133–184144, 2019.

[6] W.W. Chang, et al., , "A smart medication system using wireless sensor network technologies, Sensors Actuators" vol.172, no. 1, pp. 315–321,2011.

[7] M. Tang, M. Alazab, Y. Luo, Big data for cyber security: "Vulnerability disclosure trends and dependencies", IEEE Trans. Big Data, vol. 5, no. 03 , pp.317–329,2019.

[8] Vinaya kumar, MamounAlazab, Sriram Srinivasan, Quoc-Viet Pham, Soman Padannayil, Simran Ketha, "A visualized botnet detection system based deep learning for the internet of things networks of smart cities",IEEE,vol.56, issue:4,pp.4436 - 4456 ,2020.

[9] S. Čapkun, K.B. Rasmussen, M. Čagalj, M. Srivastava, Secure location veri-fication with hidden and mobile base stations, IEEE Trans. Mob. Comput. vol.7, no.4, pp. 470–483, 2008.

[10] L., Liu, Q., Shao, J., & Cheng, Y."Distributed Localization in Wireless Sensor Networks Under Denial-of-Service Attacks". IEEE Control Systems Letters. vol. 5, no. 2, pp. 493-498, 2021.

[11] D.L., Nguyen, T.K., Nguyen, T.V., Nguyen, T.N., Massacci, F. and Phung, P.H., "A convolutional transformation network for malware classification". 6th NAFOSTED conference on information and computer science (NICS) vol. 33, pp. 234-239 .,2019.

[12] R. Goyata, G.Kumarc, M. Alazabb, R.Sahac ”A secure localization scheme based on trust assessment for WSNs using block chain technology” , vol.125, pp. 221–231,2021.
[13] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of block chains in the internet of things: A comprehensive survey, IEEE Commun. Surv. Tutor.vol.21, no.2,pp.2347-2376 , 2018.
[14] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, “On block chain and its integration with IoT. Challenges and opportunities”, Fut. Gener. Comput. Syst. vol.88, pp.173–190, 2018.
[15] J. Yang, S. He, Y. Xu, L. Chen, J. Ren, “A trusted routing scheme using block chain and reinforcement learning for wireless sensor networks”, Sensors (Switzerland) vol.19 ,no.4 ,2019.
[16] M. Mazinani, M. Safari, “Secure localization approach in wireless sensor network”, Int. J. Mach. Learn. Comput. 5 no.6, pp.458–461, 2016.
[17] L. Zhang, H. Yang, Y. Yu, F. Peng, A three-dimensional node security localization method for WSN based on improved RSSI-LSSVR algorithm, in: Proceedings - 10th International Conference on Measuring Technology and Mechatronics Automation, vol. 2018–Janua, pp.182–186,2018.
[18] T.H. Kim, et al., “A novel trust evaluation process for secure localization using a decentralized block chain in wireless sensor networks”, IEEE Access vol. 7, pp. 184133–184144, 2019.