PROTECTION ISSUES IN WORMHOLE ATTACK

Akhilesh Soni, Prof. Abhilasha Vyas, Mr. Upendra Singh

Patel College of Science and Technology
Indore

***Abstract* : Sensor hubs, when sent to shape Wireless sensor arrange working under control of focal expert i.e. Base station are equipped for displaying intriguing applications because of their capacity to be conveyed universally in threatening and unavoidable conditions. Be that as it may, because of same reason security is turning into a noteworthy worry for these systems. Remote sensor systems are helpless against different sorts of outer and inward assaults being restricted by calculation assets, littler memory limit, constrained battery life, preparing power and absence of alter safe bundling. This study paper is an endeavor to examine dangers to Wireless sensor arranges and to report different research endeavors in contemplating assortment of directing assaults which focus on the system layer. Especially crushing assault is Wormhole assault Denial of Service assaults, where assailants make a low-inactivity connect between two focuses in the system. With concentrate on study of existing strategies for recognizing Wormhole assaults, scientists are in procedure to distinguish and separate the key research challenges for discovery of Wormhole assaults in system layer.**

***KEYWORDS*: Denial of Service, Mobile Adhoc network, Security, Wireless sensor network, Wormhole attacks.**

I. INTRODUCTION

Remote sensor arranges as a piece of MANET comprises of an extensive number of little sensor hubs that consistently screens ecological conditions. Sensor hubs perform different noteworthy errands as flag preparing, calculation, and system self-arrangement to extend organize scope and reinforce its versatility. The sensors all together give worldwide situation of the conditions that offer more data than those given by freely working sensors. They are additionally in charge of detecting condition and transmission data. Generally the transmission undertaking is basic as there is tremendous measure of information and sensors gadgets are confined. As sensor gadgets are constrained the system is presented to assortment of assaults. Conventional security instruments are not pertinent for WSNs as they are typically substantial and hubs are restricted. Additionally these instruments don't dispense with danger of different assaults. WSNs are helpful in different basic areas, for example, condition, industry, military, medicinal services, security and numerous others. For an occurrence, in a military operation, a remote sensor organize screens a few exercises. On the off chance that an occasion is distinguished, these sensor hubs sense it and report the data to the base station (called sink) by speaking with different hubs. To gather information from WSNs, base stations are by and large utilized. They as a rule have more assets (e.g. calculation power and vitality) than typical sensor hubs which have pretty much such limitations. Accumulation focuses assemble information from neighboring sensor hubs incorporate the information and forward them to base stations, where the information are additionally handled or sent to a preparing focus. Along these lines, vitality can be saved in WSNs and system life time is in this way drawn out.

WSNs have some unique attributes that recognize them from different systems, for example, MANET. The qualities, are recorded as takes after, that can prompt the utilization of WSNs in this present reality:

Sensor hubs have to a great degree constrained assets, for example, battery life, memory space and handling ability. Steering conventions and calculations are wanted to accomplish longer sensor life.
WSNs are self arranging and self sorting out remote systems.
The topology of sensor system changes quickly and haphazardly. Sensor hubs are ceaselessly included and erased from the system.
WSNs have brought together approach as far as system control. Information streams from sensor hubs towards a couple conglomeration focuses which additionally forward the information to base stations. Additionally base stations could communicate question/control data to sensor hubs [1].

Among the plans of WSNs, security is one of the huge viewpoints that merit incredible consideration, considering the enormous application openings. Therefore remembering security limitations this paper introduces a concise audit of existing procedures for wormhole assault recognition in system layer.

Subsequently, the overview paper concentrates on different ways to deal with recognize wormhole assaults. Segment 2 depicts the difficulties of sensor systems; area 3 presents assaults on sensor systems; segment 4 considers foundation and hugeness of wormhole assault; segment 5 portrays wormhole assault display; segment 6 presents sorts of wormhole assault; segment 7 depicts countermeasures to wormhole assaults and segment 8 taken after by future research challenges. Segment 9 portrays the conclusion.

II. CHALLENGES OF SENSOR NETWORKS

A remote sensor system is an extraordinary system which has numerous limitation contrasted with a customary PC organize Security in remote sensor systems has pulled in a great deal of consideration in the current years. Larger part of asset imperatives makes PC security all the more difficult undertaking for these frameworks. The different difficulties are examined as takes after.

2.1. Wireless nature of communication: The open way of remote medium is characteristically less secure and in this manner makes it defenseless against different sorts of vindictive assaults. These assaults can be either uninvolved or dynamic assaults. Inactive assault expects to take data and to listen in on correspondence inside the system In dynamic assaults, assailant changes and infuses parcels into the system. This calculate ought to be taken thought so that execution of the framework is not fundamentally influenced.

2.2. Ad-Hoc Deployment : Sensor hubs are conveyed haphazardly and don't have any settled topology. The specially appointed nature of sensor systems implies no consistent structure can be characterized. Because of high portability of hubs system topology is constantly subject to changes. Subsequently security instruments must have the capacity to work inside this dynamic condition.

2.3. Hostile Environment : Antagonistic condition in which sensor hubs are conveyed is another testing component. Because of the communicate way of the transmission medium, remote sensor systems are helpless against different security assaults. Additionally hubs are set in a risky or unguarded condition where they are not physically ensured. Assailants may catch a hub, physically alter it, and concentrate significant data from it. The very unfriendly condition speaks to testing approach for security analysts.

2.4. Resource Limitation : Satisfactory measure of assets are obligatory for the usage of all security approaches. counting memory, data transmission, and vitality to control the sensor. Be that as it may, as of now these assets are extremely restricted in a little remote sensor which postures significant difficulties to asset hungry security systems.

2.4.1 Limited Memory and Storage Capacity:

Sensor hub is a minor gadget with little measure of memory and storage room for the code. It is important to confine the code size of the security calculation with a specific end goal to build up a compelling security component.

2.4.2 Power Limitation: The utilization of remote sensor systems is expanding step by step and since every hub relies on upon vitality for its exercises, this has turned into a greatest limitation and essential necessity in remote sensor systems. The disappointment of one hub can obliterate the whole framework. Consequently, a few components must be intended to ration vitality asset.

2.5. Scalability : Versatility is a main consideration in remote sensor systems. A system topology is dynamic, it changes relying on the client necessities. Every one of the hubs in the system zone must be versatile to adjust with changing system topology.

2.6. Unreliable Communication : Absolutely, temperamental nature of correspondence channel is another testing issue to sensor security. The security of the system depends vigorously on a characterized convention, which thusly relies on upon correspondence.

2.6.1 Unreliable Transmission: Sensor organize takes after bundle based steering approach for correspondence. Subsequently transmission is connectionless and along these lines naturally inconsistent.

2.6.2 Conflicts: In spite of the fact that the channel is solid, the correspondence may at present be untrustworthy in view of clog of information parcels. This is because of the communicate way of the remote sensor organize.

2.6.3 Latency: Inactivity is characterized by how much time a hub takes to screen, or sense and convey the movement. Sensor hubs assemble data, handle it and send it to the base station. Inactivity in a system is figured in view of these exercises and in addition how much time a sensor hub takes to forward the information in substantial system movement or in a low thickness arrange.

2.7. Unattended Operation : In specific cases, the sensor hubs are not worked and henceforth are left unattended for drawn out stretches of time. There are three principle motivations to unattended sensor hubs.

2.7.1 High risk of Physical Attacks: After arrangement, sensors are typically left unattended and simple to be physically traded off. An enemy can catch at least one hubs, infuses some malignant code into them to cause dangers or gets data from the system. Likewise, an enemy can without much of a stretch spy the transmission or dispatch genuine assaults. Along these lines, it is not shocking that sensor systems are defenseless against numerous security assaults.

2.7.2 Managed Remotely: Remote administration of a sensor organize makes it hard to identify physical altering and physical support issues.

2.7.3 Lack of Central Coordinator: A sensor system ought to be a circulated arrange. Every sensor hub ought to work self-sufficiently with no essential issue of control in the system. On the off chance that if composed erroneously, it will make the system association troublesome, wasteful, and frail. A sensor hub left unattended for longer time will probably be traded off by an enemy [2].

III. ATTACKS ON WIRELESS SENSOR NETWORKS

Remote sensor systems are vulnerable to extensive variety of security assaults due to the multi-jump nature of the transmission medium. Likewise, remote sensor systems have an extra powerlessness since hubs are by and large conveyed in a threatening or unprotected condition. Despite the fact that there is no standard layered design of the correspondence convention for remote sensor organize, henceforth there is have to compress the conceivable assaults and security arrangement in various layers as for ISO-OSI display as follows[3]:

Layer	Attacks	Security approaches
Physical Layer	Denial of Service Tampering	Priority Messages Tamper Proofing Hiding, Encryption [4].
Data Link Layer	Jamming Collision Traffic manipulation	Use Error Correcting Codes Use spread spectrum techniques
Network Layer	Sybil attack Wormhole attack Sinkhole Flooding	Authentication Authorization Identity certificates
Transport Layer	Resynchronization Packet injection attack	Packet Authentication
Application Layer	Aggregation based attacks Attacks on reliability	Cryptographic approach

3.1. Definitions, Strategies and Effects of Network Layer Attacks on WSN

WSNs are organized in layered form. This layered architecture makes these networks vulnerable and lead to damage against various kinds of attacks. For each layer, various attacks and their defensive mechanisms are defined. Thus, WSNs are vulnerable to different network layer attacks, such as black hole, gray hole, wormhole, sinkhole, selective forwarding, hello flood, acknowledgement spoofing, false routing, packet replication and other attacks to network layer protocols [3].

Now, the following table shows network layer attacks on WSNs, its classification and comparison based on their strategies and effects.

Table 2 Classification of Network layer attacks on WSN

Attack Criteria	Attack Definition	Attack Effects
Black Hole	In a black hole attack, the attacker swallows (i.e. receives but does not forward) all the messages he receives, Just as a black hole absorbing everything passing by.	• It can disrupt the communication between the base station and the rest of the WSN, and hence prevent the WSN from serving its purposes. • Throughput of a subset of nodes, around the attacker and with traffic through it, is decreased [1]
Worm hole	A wormhole attack requires two or more adversaries. These adversaries have better communication resources (e.g. Power, memory) than normal nodes and can establish better communication channels (called "tunnels") between then [1].	• False/forged routing information. • Change the network topology. • Packet destruction/alteration by wormhole nodes. • Changing normal messages stream.

Sybil	In Sybil attack, a malicious node attacks network traffic by representing multiple identities to the network [6].	• Confusion and WSN disruption. • Enable other attacks. • Exploiting the routing race condition.
Sink Hole	Sink hole is a more complex attack compared with black hole attack [1].	• Attacks almost all the traffic. • Triggering other attacks, such as eavesdropping trivial selective forwarding, black hole and worm hole. • Change the base station position.
Selective Forwarding	In selective forwarding attack attacker refuses to forward packets or selectively drop then and act as a black hole [7].	• Message modification. • Information fabrication and packet dropping. • Suppressed messages in a certain area. • Routing information modification. • Exhausting of resources.
Hello Flood	In Hello Flood Attack, attacker broadcast hello message with strong transmission power to the networks and acts as a fake sink [7].	• Creates an illusion to base station of being a neighbor to many nodes in the networks. • Confuse the network routing badly [2].
Acknowledge Spoofing	An adversary can spoof Network layer Acknowledgements (ACKs) of overhead packets.	• False view/information of the WSN. • Launch selective forwarding attack. • Packet loss corruption.
False Routine (Misdirection Attack)	Attacker routes the packets to false destination, creates the loops in networks [8].	• False and misleading message generated. • Resource exhaustion. • Degrade the WSN performance.

IV. BACKGROUND AND SIGNIFICANCE OF WORMHOLE ATTACK

Shortage of different assets makes remote sensor organize helpless against a few sorts of security assaults. Assailant having adequately substantial measure of memory space, control supply, preparing capacities and limit with respect to high power radio transmission, brings about era of a few malevolent assaults in the system. Wormhole assault is a sort of Denial of Service assault that misdirects steering operations even without the learning of the encryptions strategies not at all like different sorts of assaults. This trademark makes it vital to distinguish and to safeguard against it [9].

Wormhole assault is a serious kind of assault on Wireless sensor arrange steering where at least two assailants are associated by fast off-channel connect called wormhole interface [10].

Wormhole assaults exists in two distinct modes, in particular "covered up" and "uncovered" mode, contingent upon whether assailants put their personality into parcel headers while burrowing and replaying bundles [11].

In wormhole assault, a couple of assailants structures "passages" to exchange the information parcels and replays them into the system. This assault tremendously affects remote systems, particularly against directing conventions. Directing components can be befuddled and upset when steering control messages are burrowed. The passage shaped between the two intriguing assailants is alluded as wormhole. Figure 1 demonstrates the wormhole assault. Bundles gotten by hub X is replayed through hub Y and the other way around.

Typically it take a few jumps for a bundle to cross from an area close X to an area close Y, parcels transmitted close X going through the wormhole will touch base at Y before parcels going through different bounces in the system. The aggressor can make An and B trust that they are neighbors by sending directing messages, and afterward specifically drop information messages to disturb correspondence amongst An and B [12].

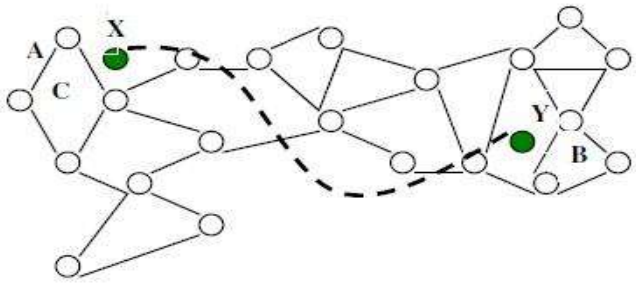

Figure 1: Wormhole Attack [13]

V. WORMHOLE ATTACK MODEL

Wormhole assault is one of the Denial-of-Service assaults that can influence the system even without the information of cryptographic strategies actualized. This is the motivation behind why it is exceptionally hard to identify. It might be propelled by one, two or more number of hubs. In two finished wormhole, bundles are burrowed through wormhole connect from source to goal hub. On getting parcels, goal hub replays them to the next end.

Outlining anticipation and identification techniques for Wormhole assault requires the grouping of Wormhole assaults. Figure 2 represents the three models of wormhole assault.

Contingent upon whether the assailants are noticeable on the course, bundle sending conduct of wormhole hubs and also their inclination to cover up or demonstrate the personalities, wormholes is arranged into three sorts: shut, half open, and open. In the accompanying cases S and D are the source and goal hubs separately. Hubs M1 and M2 are noxious hubs.

5.1. Open Wormhole

Source(S) and goal (D) hubs and wormhole closes M1 and M2 are unmistakable. Hubs An and B on the navigated way are kept covered up. In this mode, the assailants incorporate themselves in the bundle header taking after the course disclosure methodology. Hubs in system know about the nearness of vindictive hubs on the way yet they would copy that the malevolent hubs are immediate neighbors.

5.2. Half-Open Wormhole

Vindictive hub M1 close to the source (S) is unmistakable, while second end M2 is set covered up. This prompts way S-M1-D for the bundles sent by S for D. The aggressors don't alter the substance of the parcel. Rather, they essentially burrow the parcel shape one side of wormhole to another side and it rebroadcasts the bundle

5.3 . Close Wormhol

Personalities of all the middle of the road hubs (M1, A, B, M2) on way from S to D are kept covered up. In this situation both source and goal feel themselves only one-bounce far from each other. Along these lines fake neighbors are made.

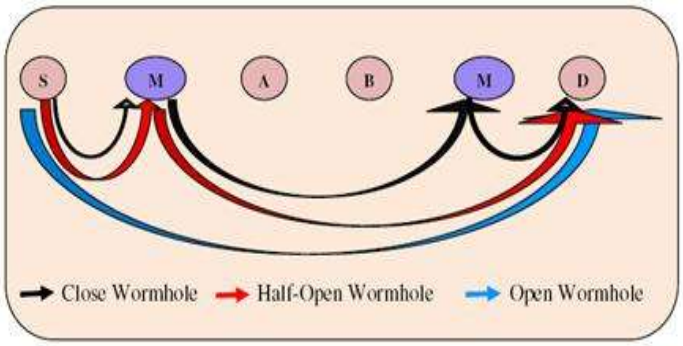

Fig 2: Representation of Open, Half-Open and Closed Wormhole [14]

VI. TYPES OF WORMHOLE ATTACK

In this segment, we characterize the wormhole assault in view of the methods utilized for propelling it. Number of hubs required in setting up wormhole and the best approach to build up it arranges wormhole into the accompanying sorts:

6.1 . Wormhole using Packet Encapsulation

Here a few hubs exist between two pernicious hubs and information parcels are typified between the noxious hubs. Subsequently it keeps hubs on path from increasing jump tallies. The bundle is changed over into unique shape by the second end point. This method of wormhole assault is not hard to dispatch since the two finishes of wormhole don't need any cryptographic data, or extraordinary prerequisite, for example, high-control source or high transmission capacity channel.

6.2 . Wormhole utilizing Out-of-Band Channel

This sort of wormhole approach has just a single vindictive hub with much high transmission capacity in the system that pulls in the bundles to take after way going from it. The odds of malevolent hubs exhibit in the courses set up amongst sender and beneficiary increments for this situation. Likewise this sort is alluded as "dark gap assault" in the writing.

6.3 . Wormhole utilizing Packet Relay

At least one noxious hubs can dispatch bundle transfer based wormhole assaults. In this sort of assault vindictive hub replays information parcels between two far hubs and along these lines fake neighbors are made. This sort of assault is likewise called as "replay-based assault" in the writing.

6.4 . Wormhole using Protocol Distortion

In this method of wormhole assault, single vindictive hub tries to pull in system activity by mutilating the steering convention. This mode does not influence the system directing much and thus is safe. Additionally it is known as "surging assault" in the writing.

The accompanying Table IV compresses distinctive methods of the wormhole assault alongside the related prerequisites are given [15].

Name of Mode	Minimum no. of adversary nodes	Requirements
Packet Encapsulation	Two	None
Out -of -band Channel	Two	High speed wire line link
High power Transmission Capability	One	High power source
Packet relay	One	None
Protocol Distortions	One	None

VII. COUNTERMEASURES TO WORMHOLE ATTACK

A few Researchers have dealt with location and avoidance of wormhole assaults in Wireless Sensor Networks. This segment will depict the essential wormhole assault location systems.

7.1.1 Location Information based method : Hu, Perrig and Johnson characterized the wormhole assaults in adhoc systems [16]. Afterward, they proposed a system, called parcel chains, which keeps bundles from voyaging more remote than transmission go. This component depicts two sorts of rope: Geographical and Temporal. In Geographical Leashes, every hub knows its exact area and all hubs have approximately synchronized timekeepers to decide the neighbor connection. Before sending a parcel, hub attaches its present position and transmission time to it. On accepting bundle, getting hub processes the separation as for the sender and the time required by the parcel to navigate the way. The recipient can utilize this separation data to conclude whether the got parcel gone through a wormhole or not. In Temporal Leashes, each hub keeps up a firmly synchronized clock however does not rely on upon GPS data [11].

Both instruments utilize lightweight hash chains to verify the hubs [9]. The Message Authentication Code (MAC) can be computed progressively. One advantage of parcel rope is the low calculation overhead.

7.1.2 Statistical Analysis strategy : Melody et al. propose a wormhole revelation component in view of factual investigation of multipath steering. Melody watches that a passage made by a wormhole is exceptionally appealing as far as steering, and will be chosen and asked for with unnaturally high recurrence as it just uses directing information officially accessible to a hub. These components empowers for simple combination of this technique into interruption identification frameworks just to directing conventions that are both on-request and multipath [16].

7.1.3 Hardware based technique : Hu and Evans proposed the strategy for directional reception apparatuses [17]. It depends on the way that in specially appointed systems with no wormhole connect, on the off chance that one hub sends parcels in a provided guidance, at that point its neighbor will get that bundle from the other way. Just when the bearings are coordinating in sets, the neighboring connection is affirmed. It is vital that every hub requires an exceptional equipment i.e. directional radio wire.

7.1.4 Visualization based strategy : Bhargava [11] to recognize wormhole assaults in static WSNs. In this approach utilizing the got flag quality, each hub measures the separation to its neighbor. In light of these estimations, base station computes the system's physical topology. It is watched that the system with malevolent hubs has diverse perception from that with ordinary hubs. Without wormholes, topology ought to be pretty much level, where as in their nearness "string" pulling diverse finishes of system are seen. It recreates the design of the sensors utilizing multi-dimensional scaling plan. The irregularities, which are presented by the fake associations through the wormhole, will twist the reproduced surface to pull the sensors that are far away to each other. Thusly, MDS-VOW could find the wormhole associations. In MDS-VOW, all sensor hubs are required to send their neighbor records to the base station.

7.1.5 Graph hypothesis strategy : Lazos and Poovendran [11] built up a "diagram hypothetical" way to deal with wormhole assault avoidance in WSNs. As per it, constrained area mindful protect hubs (LAGNs) which are hubs with known area and start which can be obtained through GPS recipients are utilized. Between each one bounce neighbors, LAGNs utilize "nearby communicate keys". Keeping in mind the end goal to distinguish wormhole assault, it is impractical to decode a message encoded with a nearby key – scrambled with the match savvy key. Henceforth amid the key foundation, creators utilized hashed messages from LAGNs to distinguish wormholes. On the off chance that a wormhole is available, hub can identify certain irregularities in messages from various LAGNs. Without wormhole, a hub ought to be not able hear two LAGNs that are far from each other.

7.1.1 Hop including technique : The jump tally is the base number of hub to-hub transmissions. This technique utilizes convention Delay per Hop Indicator (Delphi) [16] proposed by Hon Sun Chiu and King-Shan Lui, can distinguish both covered up and uncovered wormhole assaults. In DelPHI, endeavors are made to decide each accessible disjoint course between a source and a goal. To distinguish wormhole, postpone time and length of each course are measured and the normal defer time per jump along each course is registered. As indicated by this, the course containing a wormhole connection will have a more prominent Delay for every Hop (DPH) esteem. This system can distinguish both methods of wormhole assault; notwithstanding, pinpoint the area of a wormhole can't be resolved.

7.1.2 Message Traveling time data based strategy : Message voyaging time data is measured as far as round outing time (RTT). One approach to forestall wormhole assault, as utilized by Tran et al. [11], Jane Zhen and Sampalli [16], is to gauge RTT of a message and its affirmation. The RTT is the time that reaches out from the Route Request (RREQ) message sending time of a hub A to Route Reply (RREP) message accepting time from a hub B. Hub A will ascertain the RTT amongst An and every one of its neighbors. Since the RTT between two fake neighbors is higher than between two genuine neighbors, hub A can recognize both the fake and genuine neighbors. In this instrument, every hub registers the RTT amongst itself and every one of its neighbors. No uncommon equipment is required in this mechanism[16].

7.1.3 Trust based strategies : Another noteworthy strategy for distinguishing and detaching malevolent hubs that make a wormhole in the system is Trust Based Method by Jain and Jain [16] .In this technique, trust levels are determined in neighboring hubs in view of their earnestness in execution of the directing convention. This determined trust is then used to impact the directing choices, which thusly control a hub to maintain a strategic distance from correspondence through the wormholes.

Accepting that wormholes drop every one of the bundles it gets, it ought to have slightest trust level and subsequently can be effortlessly killed. By utilizing Trust Based Model Packet Dropping is diminished by 15% without utilizing any cryptography component and throughput is expanded up to 7-8%.

VIII. OPEN RESEARCH CHALLENGES

In the past segments, we have concentrated different methodologies of system layer assaults, essentialness of wormhole assault and their countermeasures in Wireless sensor systems. This segment will recognize open research challenges here. In Table 3, synopsis of wormhole discovery method is introduced. The majority of the techniques utilize equipment which expands the assembling expense of a sensor hub. Later analysts concentrated on programming based wormhole location systems. Yet at the same time the location of wormhole assaults in sensor systems is a testing assignment for scientists.

Among programming based strategies, Multipath Hop tally examination, voyaging time instrument, trust based models are generally utilized as they are promising as far as recognizing wormhole assaults with no equipment prerequisites. According to these methods, it is expected that time or separation information utilized for wormhole recognition can't be changed. Since pernicious hubs can alter transmitted data, separate bouncing and time-based wormhole discovery procedures must be bolstered with cryptographic confirmation systems so that legitimacy of the data can be checked over the way.

Wormhole assaults are entirely identified with system layer conventions. As new directing conventions are proposed for WSNs, it is critical to distinguish conceivable deficiencies of these new steering conventions, measure the execution of new steering convention with wormhole assault and to examine the viability of the current wormhole identification systems on these conventions. Thus, there is a degree for further research as far as measuring execution of existing wormhole identification systems on new steering conventions. Future work here spotlights on extra security improvements for directing conventions in remote sensor systems.

In the ebb and flow wormhole recognition investigate typically static topology of WSNs are considered. Thus, wormhole location in a dynamic WSN is an open research territory. In a dynamic WSN, any two honest to goodness sensor hubs that were beforehand many jumps a long way from each other may end up plainly one bounce neighbors, and henceforth makes dream for the base station that a wormhole assault has been propelled. Thus, it is a testing assignment to recognize such honest to goodness hubs from vindictive hubs while distinguishing wormhole assaults.

IX. CONCLUSION

Remote sensor systems are helpless against extensive variety of security assaults as a result of their arrangement in an open and unprotected condition. This overview paper presents the significant security dangers in WSN and furthermore researches diverse wormhole location procedures, analyzes different existing techniques to discover how they have been actualized to distinguish wormhole assault. It has been concentrated that among the quantity of procedures talked about, every strategy has its own quality and shortcomings and there is no legitimate wormhole location system that can identify all wormhole assaults totally. At last, by dissecting the upsides and downsides of existing strategies, the open research challenges in the wormhole identification zone are examined.

X. AFFIRMATIONS

My genuine because of my noteworthy guide Prof. Niketa A.Chavhan and other people who have contributed towards the readiness of the paper.

REFERENCES

[1] Kia Xiang, Shyaam Sundhar Rajamadam,Srinivasan, Manny Rivera,Jiang Li, Xiuzhen Cheng, “Attacks and Countermeasures in Sensor Networks: A Survey”, pp 1-28, Springer, 2005.
[2] G. Padmavathi, Mrs. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security Vol. 4, No. 1 & 2, 2009.
[3] Nityananda Sarma , Sangram Panigrahi, Prabhudutta Mohanty and Siddhartha Sankar Satapathy, “Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey”, Journal of Theoretical and Applied Information Technology, 2005.
[4] Abhishek Jain,Kamal Kant, “Security Solutions for Wireless Sensor Networks”, IEEE Second International Conference on Advanced Computing & Communication Technologies, pp 430-433,2012.
[5] Shahriar Mohammadi and Hossein Jadidoleslamy, “A Comparison Of Link Layer Attacks On Wireless Sensor Networks”, International journal on applications of graph theory in wireless ad hoc networks and sensor networks(GRAPH-HOC) Vol.3, No.1, March 2011.
[6] Sushma, Deepak Nandal, Vikas Nandal, “Security Threats in Wireless Sensor Networks”, IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011.
[7] Syed Ashiqur Rahman ,Md. Safiqul Islam, “Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches”, International Journal of Advanced Science and Technology Vol. 36, November, 2011.

[8] Ali Modirkhazeni, Norafida Ithnin, Mohammadjavad Abbasi, "Secure Hierarchal Routing Protocols in Wireless Sensor Networks: Security Survey Analysis", IJCCN International Journal of Computer Communications and Networks, Volume 2, Issue 1, February 2012.
[9] Dhara Buch, Devesh Jinwala, "Detection of Wormhole Attacks in Wireless Sensor Networks", IEEE Conference on Advances in Recent Technologies in Communication and Computing, pp 7-14, 2011.
[10] Khin Sandar Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.
[11] Majid Meghdadi, Suat Ozdemir and Inan Guler , "A Survey of Wormhole based Attacks and their Countermeasures in Wireless Sensor Networks", IETE TECHNICAL REVIEW, VOL 28, ISSUE 2, Mar-Apr 2011.
[12] Mani Arora, Rama Krishna Challa," Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, pp 102-104, 2010.
[13] Rama Krishna Challa ,Mani Arora, Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", IEEE Second International Conference on Computer and Network Technology, pp 102-104, 2010.
[14] Dhara Buch, Devesh Jinwala, "Prevention of wormhole attack in Wireless sensor network",International Journal of Network Security & Its Applications (IJNSA), pp 85-98, Vol.3, No.5, Sep 2011.
[15] Marianne Azer, Sherif El-Kassas, Magdy El-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks", International Journal of Computer Science and Information Security(IJCSIS), pp 41-52, Vol. No. 1, May 2009.
[16] Preeti Nagrath,Bhawna Gupta,"Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A survey", pp 245-250, IEEE 2011.
[17] Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao, Fuxiang Gao, "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis", IEEE International Conference on Information Engineering, pp 251-254, 2010.
[18] Prasannajit B, Venkatesh, Anupama S, Vindhykumari, "An Approach towards Detection of Wormhole Attack in Sensor Networks", IEEE First International Conference on Integrated Intelligent Computing, pp 283-289, 2010.