A REVIEW OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK

Dinesh Bhuriya

Lecturer
Computer Science and Engineering
Govt. Women's Polytechnic College Indore

***ABSTRACT*: Sensor hubs, when conveyed to shape Wireless sensor organize working under control of focal expert i.e. Base station are equipped for displaying fascinating applications because of their capacity to be conveyed universally in unfriendly and inescapable situations. In any case, because of same reason security is turning into a noteworthy worry for these systems. Remote sensor systems are defenseless against different sorts of outside and inward assaults being constrained by calculation assets, littler memory limit, restricted battery life, handling power and absence of alter safe bundling. This study paper is an endeavor to dissect dangers to Wireless sensor arranges and to report different research endeavors in examining assortment of steering assaults which focus on the system layer. Especially decimating assault is Wormhole assault a Denial of Service assault, where aggressors make a low-idleness interface between two focuses in the system. With concentrate on overview of existing strategies for recognizing Wormhole assaults, analysts are in procedure to distinguish and differentiate 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.

1. INTRODUCTION

Remote sensor arranges as a piece of MANET comprises of a substantial number of minor sensor hubs that constantly screens natural conditions. Sensor hubs perform different noteworthy assignments as flag preparing, calculation, and system self-setup to grow arrange scope and reinforce its versatility. The sensors all together give worldwide situation of the conditions that offer more data than those given by autonomously working sensors. They are likewise in charge of detecting condition and transmission data. Generally the transmission undertaking is basic as there is gigantic measure of information and sensors gadgets are limited. As sensor gadgets are restricted the system is presented to assortment of assaults. Customary security instruments are not pertinent for WSNs as they are normally overwhelming and hubs are restricted. Additionally these instruments don't kill danger of different assaults. WSNs are helpful in different basic areas, for example, condition, industry, military, human services, security and numerous others. For an example, in a military operation, a remote sensor arrange screens a few exercises. On the off chance that an occasion is recognized, 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 requirements. Total focuses assemble information from neighboring sensor hubs coordinate the information and forward them to base stations, where the information are additionally prepared or sent to a handling focus. Along these lines, vitality can be monitored in WSNs and system life time is in this way drawn out.
In this way, the review paper concentrates on different ways to deal with recognize wormhole assaults. Area 2 depicts the difficulties of sensor systems; segment 3 presents assaults on sensor systems; segment 4 contemplates foundation and centrality of wormhole assault; segment 5 portrays wormhole assault demonstrate; 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.

2. Difficulties OF SENSOR NETWORKS

A remote sensor system is an extraordinary system which has numerous limitation contrasted with an ordinary PC arrange Security in remote sensor systems has pulled in a considerable measure of consideration in the current years. Larger part of asset requirements makes PC security additionally difficult errand for these frameworks. The different difficulties are talked about as takes after.

2.1. Remote nature of correspondence

The open way of remote medium is inalienably less secure and subsequently makes it powerless against different sorts of malignant assaults. These assaults can be either aloof or dynamic assaults. Uninvolved assault means to take data and to listen stealthily on correspondence inside the system In dynamic assaults, aggressor changes and infuses parcels into the system. This calculates ought to be taken thought so that execution of the framework is not altogether influenced.

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

2.3. Antagonistic Environment
Antagonistic condition in which sensor hubs are sent is another testing element. Because of the communicate way of the transmission medium, remote sensor systems are helpless against different security assaults. Additionally hubs are put in an unsafe or unguarded condition where they are not physically secured. Aggressors may catch a hub, physically alter it, and concentrate important data from it. The exceedingly antagonistic condition speaks to testing approach for security specialists.

2.4. Asset Limitation
Satisfactory measure of assets is required for the usage of all security approaches. counting memory, transmission capacity, and vitality to control the sensor. Be that as it may, presently these assets are exceptionally restricted in a modest remote sensor which postures impressive 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 successful 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. Accordingly, a few components must be intended to preserve vitality asset.

2.5. Versatility
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 region must be versatile in order to adjust with changing system topology.

2.6. Questionable Communication
Positively, temperamental nature of correspondence channel is another testing issue to sensor security. The security of the system depends intensely on a characterized convention, which thus relies on upon correspondence.

2.6.1 Unreliable Transmission:
Sensor organizes takes after bundle based directing methodology for correspondence. Consequently transmission is connectionless and along these lines characteristically questionable.

2.6.2 Conflicts:
Despite the fact that the channel is dependable, the correspondence may at present be inconsistent in view of blockage of information parcels. This is because of the communicate way of the remote sensor organize.

2.6.3 Latency:
Idleness is characterized by how much time a hub takes to screen, or sense and impart the action. Sensor hubs accumulate data, handle it and send it to the base station. Inactivity in a system is processed in view of these exercises and in addition how much time a sensor hub takes to forward the information in overwhelming system movement or in a low thickness organize.

3. ASSAULTS ON WIRELESS SENSOR NETWORKS

Remote sensor systems are defenseless to extensive variety of security assaults due to the multi-bounce nature of the transmission medium. Likewise, remote sensor systems have an extra helplessness since hubs are for the most part conveyed in an antagonistic or unprotected condition. Despite the fact that there is no standard layered design of the correspondence convention for remote sensor arrange, consequently there is have to condense the conceivable assaults and security arrangement in various layers as for ISO-OSI display as follows[3]:

Table 1. Attacks in OSI model

Layer Layer	Attacks	Security approaches
Physical Layer	Denial of Service , Tampering	Priority Messages , Tamper Proofing
Data Link Layer	Jamming	Use Error Correcting Codes
Network Layer	Wormhole attack , Flooding	Authorization
Transport Layer	Resynchronization, Packet injection attack	Packet Authentication
Application Layer	Aggregation based attacks	Cryptographic approach

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

WSNs are sorted out in layered frame. This layered engineering makes these systems helpless and prompt harm against different sorts of assaults. For each layer, different assaults and their protective instruments are characterized. In this way, WSNs are powerless against various system layer assaults, for example, dark opening, dim gap, wormhole, sinkhole, particular sending, hi surge, affirmation ridiculing, false steering, bundle replication and different assaults to network layer conventions [3].
Presently, the accompanying table shows organize layer assaults on WSNs, its arrangement and examination in light of their procedures and impacts.

Table 2. Classification of Network layer attacks on WSN

Attack Criteria	Attack Definition	Attack Effects
Black hole	The attacker is swallows in the black hole. All the messages he receives ,just a back hole absorbing everything passing by .	● It can disturb the communication between the base station and the rest of WSN. ● Throughput of a subset of nodes , around the attacker and with traffic through it is decreased
Wormhole	A wormhole require two or more adversaries, these adversaries have better communication resources than normal holes and can be establish better communication channels between them.	● False 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.	● Confusion and WSN disruption. ● Enable other attacks. ● Exploiting the routing race conditions.
Sinkhole	Sinkhole is more complex attack compared with black hole attack.	● Attacks almost all traffic. ● Triggering other attacks ,such as eavesdropping ,trivial selective forwarding, black hole and warmhole ● changes the base station's position.
Selective forwarding	In selective forwarding attack,attacker refuses to forward packets or selective drop them and act as black hole.	● Modification of messages. ● packet dropping. ● Modification of routing information.
Hello flood	In Hello Flood Attack, attacker broadcast hello message with strong transmission power to the network and act as a black hole.	● Creates an illusion to base station of being a neighbor to many nodes in the networks. ● confuse the network routing badly.

4. WORMHOLE ATTACK

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

Wormhole assault is an extreme kind of assault on Wireless sensor arrange steering where at least two aggressors are associated by rapid off-channel interface called wormhole connect [10].
Wormhole assaults exists in two distinct modes, to be specific "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. Steering systems can be confounded and disturbed when directing control messages are burrowed. The passage framed between the two plotting assailants is alluded as wormhole. Figure 1 demonstrates the wormhole assault. Parcels gotten by hub X is replayed through hub Y and the other way around.

Regularly it take a few bounces for a bundle to cross from an area close X to an area close Y, parcels transmitted close X going through the wormhole will land at Y before bundles going through numerous jumps 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].

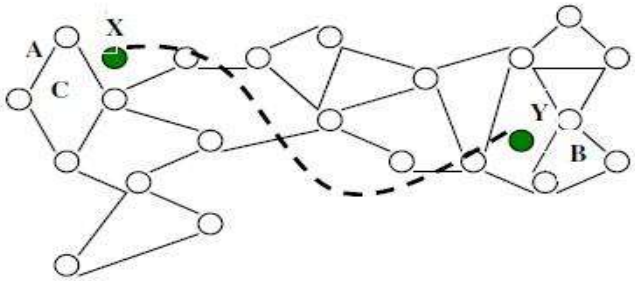

Figure 1: Wormhole Attack [13]

Table 3. Summary of wormhole attack modes

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

5. COUNTERMEASURES TO WORMHOLE ATTACK

A few Researchers have taken a shot at location and aversion of wormhole assaults in Wireless Sensor Networks. This segment will portray the critical wormhole assault recognition systems.

Table 4. Summary of wormhole attacks detection mechanisms

Methods	**Requirements**	**Comments**
Temporary packet leaches by Hu, perring and Jonson	Tightly synchronized clocks	Requirement time synchronization and currently not achievable in sensor networks
Geographical packet leaches	GPS coordinates of every node Loosely synchronized clocks (ms)	Robust straight forward solution, Inherit general limitations of GPS technology.
Statistical analysis	Requires statistical routing information each sensor nodes.	Works only with multi-path on demand protocols; easy integration with intrusion detection system
Directional antennas by Hu and vans	Nodes use specific 'sector' of their antennas to communicate with each other ; directional antennas on all nodes.	Good solutions for networks depending on directional antennas but not directly applicable to other networks.
Networks visualization(MDS-VOW) by Wang and Bhargava	Requires central coordination	Works best on dense networks; Mobility is not studied
Graph theoretic model by Lazos and poovendran	Requires coordination of location information and cryptography	Use location aware guard nodes equipped with GPS receiver s
Multipath Hop count analysis by shang,Laith and Kuo	No hardware requirement	Scheme has high efficiency and very good performance with low overhead.
Trust based model by Jain and jain	No Hardware requirement	Effectively locate dependable routers through the network

6. OPEN RESEARCH CHALLENGES

In the past segments, we have concentrated different procedures of system layer assaults, criticalness of wormhole assault and their countermeasures in Wireless sensor systems. This segment will distinguish open research challenges around there. In Table 3, rundown of wormhole identification method is displayed. The vast majority of the techniques utilize equipment which expands the assembling expense of a sensor hub. Later scientists concentrated on programming based wormhole identification systems. Yet at the same time the recognition of wormhole assaults in sensor systems is a testing undertaking for analysts.
Among programming based strategies, Multipath Hop number examination, voyaging time component, trust based models are broadly utilized as they are promising as far as identifying wormhole assaults with no equipment prerequisites. According to these procedures, it is accepted that time or separation information utilized for wormhole identification can't be changed. Since vindictive hubs can alter transmitted data, separate bouncing and time-based wormhole identification methods must be upheld with cryptographic validation systems so that genuineness of the data can be checked over the way.

Wormhole assaults are entirely identified with system layer conventions. As new steering conventions are proposed for WSNs, it is vital to recognize conceivable weaknesses of these new directing conventions, measure the execution of new steering convention with wormhole assault and to research the viability of the current wormhole location strategies on these conventions. Henceforth, there is a degree for further research as far as measuring execution of existing wormhole location procedures on new directing conventions. Future work around there spotlights on extra security upgrades for steering conventions in remote sensor systems.

In the ebb and flow wormhole recognition look into typically static topology of WSNs are considered. Consequently, wormhole discovery in a dynamic WSN is an open research region. In a dynamic WSN, any two certifiable sensor hubs that were beforehand many bounces a long way from each other may wind up noticeably one jump neighbors, and henceforth makes fantasy for the base station that a wormhole assault has been propelled. Henceforth, it is a testing assignment to recognize such honest to goodness hubs from pernicious hubs while distinguishing wormhole assaults.

7. CONCLUSION

Remote sensor systems are defenseless against extensive variety of security assaults in light of their arrangement in an open and unprotected condition. This study paper presents the real security dangers in WSN and furthermore explores distinctive wormhole recognition strategies, analyzes different existing techniques to discover how they have been executed to recognize wormhole assault. It has been concentrated that among the quantity of methods talked about, every system has its own particular quality and shortcomings and there is no legitimate wormhole identification procedure that can recognize all wormhole assaults totally. At long last, by breaking down the upsides and downsides of existing methods, the open research challenges in the wormhole discovery range are considered.

ACKNOWLEDGEMENTS

My genuine on account of my respectable 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. 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