A Evaluation of Black hole Detection and Prevention Techniques

Ajay Jangra, Rajesh

Department of computer science and engineering, UIET, K.U., Kurukshetra, Haryana ,India

Abstract: Wireless Sensor Networks are infrastructure less network in which data transmission takes place through base station. When nodes wants to transmit data in open environment, then there are more chances occurred for malicious node to perform malicious activities by disturbing network routing process. In this paper characteristic, architecture of WSN has been discussed with security issues of WSN and various attacks presented in WSN has been studied, with the analysis of different existing techniques specially designed for black hole detection and prevention methods has been presented.

Keywords: Wireless Sensor Network (WSN), Security, Black hole, Trust and REWARD.

I. Introduction

A wireless sensor network (WSN) is a network made of various autonomous little sensor nodes, which are self configuring units comprising of a battery, sensors, and an insignificant measure of on-board processing power. A wireless sensor networks comprise of a lightweight, un-fastened, battery-fueled gadget, it has restricted wellspring of energy. In this manner, energy utilization is a fundamental issue in sensor networks. Whenever the assault is occur in this sensor networks it takes more battery energy to identify the attacks. In engineering of WSNs there are two different parts, called "accumulation "and "base station" which have more assets than ordinary sensors. Conglomeration to gathers data from the sensors nodes and after that forward to the base station to prepare accumulated information, as appeared in fig1 and fig 2. Every node is to gather information and course information back to the sink (Base Station).Protocols and calculations with self-association. Nodes have act as a team and process the detected information. Constraints, for example, cost, undetectable arrangement and assortment application spaces, prompt requiring little size and constrained assets (like energy, stockpiling and handling) sensors [1].

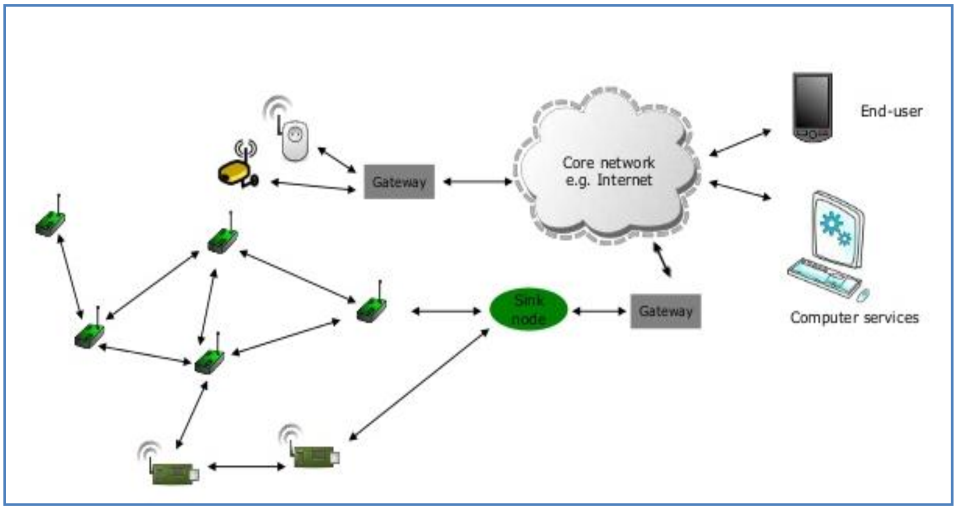

Fig1: Architecture of WSN [1]

The sensor's parts are: sensor unit, handling unit, Capacity unit, control supply unit and wireless radio handset, these units are conveying to each other. The sensors in the sensing unit interact physically with the deployed environment. The sensed data is transferred to the ADC/DAC converters for analog to digital conversion. The micro-controller in processing unit receives this digital data and does the required processing by using the temporary storage. The processed data are then moved to the transmitter of the communication unit for transmission towards the cluster head or base station. On the other hand, the data from the cluster head or base station is received by the receiver and then transferred to the processor for further processing. The energy source used in sensor node is a lithium battery. The tiny size of the sensor node only allows for a very small size of battery.

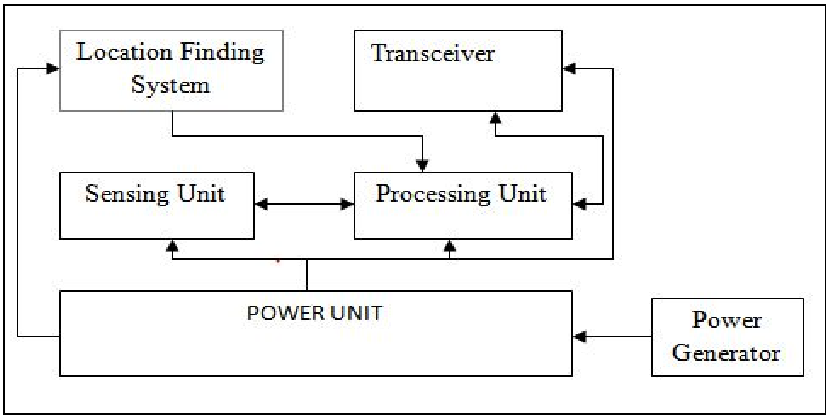

Fig. 2: Structural View of a Sensor Node [1]

A. Characteristics of WSN

Wireless sensor networks have different qualities and additionally requirements which are as follows:

- **Densely Deployed**
  Because of the thick organization of the network every node has many neighbors with which it can convey specifically when utilizing an adequately high transmission control.
- **Low Powered and Battery Operated**
  Sensor nodes utilize low power in full operation of detecting, handling and correspondence to build the lifetime of the network. For the most part nodes are conveyed in the remote regions and it is difficult to change batteries effectively.
- **Lack of Resources**
  Sensor nodes keep running with exceptionally restricted assets like battery, data transmission/channels and so forth and these assets are should have been saved.
- **Unreliability**
  There can be a questionable correspondence due to wireless medium. Since Sensor nodes are conveyed in unforgiving ecological conditions the odds of physical harms or disappointments are more [2].

B. Types of Attacks in WSNs:

These little devices (nodes) have more helplessness for attacks than ordinary wireless networks and significantly more than to wired networks. Around a wide range of assault component existing in wired and wireless networks have been presented bit by bit in wireless sensor networks too. Established methods to avert and to moderate such attacks are not reasonable for wireless sensor networks in light of restricted abilities of wireless sensor nodes. Numbers of attacks on wireless sensor networks are expanding quickly. Step by step these attacks are developing in number and also in complexities of assault dispatch. Attacks are making progressively greater misfortunes and harms enterprises and organizations: these are as follows:

- Sybil Attack: A Sybil attack creates its multiple identities in network and appears at multiple locations in network.
- Tampering Attack: this attack is mainly used for destroy some hardware part of a sensor node.
- Denial of service attack: In this attack, malicious node sends multiple replications of messages to obliterate the routing process in network.
- Eavesdropping: In this attack, malicious nodes just continually scans network routing process and then forge some control information of network.
- Black hole Attack: A black hole attack drops messages and modifies some existing messages and forward this modify message to next node [3].

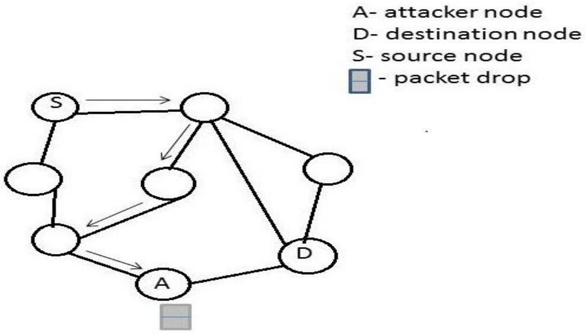

Fig 3: Example of Black Hole attacks by Fake RREP [3]

II. Related Work

Zurina Mohd Hanapi et al. [4] proposed a plan particularly suited for CTS surging and therefore dark opening and dim gaps.

Riaz Ahmed Shaikh et al. [5] proposed an original thought of utilizing two new factors viz. Course and area security and information detected protection calculations for remote sensor organizes as these component are inborn and inbuilt for remote sensor systems imperatives forced on bits, organization condition and bits capacities.

Guorui Li et.al. [6] proposed a cost and exertion sparing plan viz. consecutive work test. At the point when bundle drop alert is gotten, bunch head hubs conducts consecutive work test for parcel dropping.

Deng-yin Zhang et.al [7] proposed a plan in light of Digital watermarking innovation for location of Black holes/Gray holes.

III. Comparative Analysis

Table 1: Different existing techniques to detect and prevent black hole attack

Techniques	Description	Problem
Exponential Trust Based[8]	Each node maintains a table that contains trust factor of it. This rust factor is checked by third party node and decides whether node is malicious or not.	Poor fault tolerance.
REWARD(Receive, Watch, Redirect)[9]	REWARD uses geographical location of node to forward packets towards it. It uses a data base that maintains records of malicious node	Supports only dense networks.
TBESP Algorithm (Topology Based Efficient Service Prediction) Algorithm[10]	TBESP is topology dependent mechanism in which topologies are compared and best topology was chosen for data transmission in black hole environment.	It detects black hole attack only in selected topologies not all.
Energy Efficient Intrusion Detection System for Black Hole Attacks in WSN [11]	It is simple and based on evaluation of control packets among sensor nodes and base station. also it used alarm packet that contains node identity table.	Selection of cluster head multiple times lead to occurrence of black hole attack.

Table 2: Comparative analysis of different existing techniques with performance parameters

Techniques	Delivery ratio	Drooped packets	End to end delay	Overhead ratio
Exponential Trust Based	High	Medium	High	High
REWARD(Receive, Watch, Redirect)	Medium	Low	High	Medium
TBESP Algorithm (Topology Based Efficient Service Prediction) Algorithm	Medium	High	Low	High
Energy Efficient Intrusion Detection System for Black Hole Attacks in WSN [8]	Medium	High	High	Medium

IV. Conclusion

In wireless sensor network security of data transmission is serious issue. Numbers of attacks are there in WSN out of tem it is difficult to detect black hole attack. To detect and present black hole attack number of techniques proposed by different researchers. In this paper comparison between existing techniques with different performance parameters like delivery ratio, dropped ratio etc. In future it is intended to propose a enhanced mechanism to detect black hole attack.

References

[1] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol. 38, pp: 393-422, 2002.

[2] K. Sharma and M. K. Ghose; Wireless Sensor Networks, “An Overview on its Security Threats” IJCA Special Issue on Mobile Ad-hoc Networks, Vol.1, pp: 42-45, 2010.

[3] Z. I. Khan and M. M. Afzal, “Security in Wireless Sensor Networks : DoS Perspective,” International Journal of Engineering Research & Technology (IJERT) Vol. 6, pp. 311–316, 2017.

[4] Zurina Mohd Hanapi, Mahmod Ismail and Kasmiran Jumari, “Priority and Random Selection for Dynamic Window Secured Implicit Geographic Routing in Wireless Sensor Network”, American Journal of Engineering and Applied Sciences, Vol. 2, pp: 494-500, 2009.

[5] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d’Auriol, Heejo Lee, Sungyoung Lee and Young-Jae Song, “Achieving Network Level Privacy in Wireless Sensor Networks”,Sensors, Vol.10, pp:1447-1472, 2010.

[6] G. Li, X. Liu and C. Wang, "A sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks," in proceedings of IEEE International Conference on Networking, Sensing and Control (ICNSC), Chicago, pp. 554-558, 2010.

[7] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin, “Lightweight defense scheme against selective forwarding attacks in wireless sensor networks”, in proceedings of IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Zhangijajie, China, pp: 226 – 232, 2009.

[8] Deepali Virmani, Manas Hemrajani and Shringarica Chandel, “Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network” Bhagwan Parshuram Institute of Technology,Vol.1, pp:1-5, 2014.

[9] Zdravko Karakehayov and Mads Clausen, “Using REWARD to detect team black-hole attacks in wireless sensor networks”, in proceedings of IEEE International Conference on Emerging Technologies and Factory Automation, 2007, Patras Greece ,pp:646-650, 2005.

[10]Mohammad Wazid, , Avita Katal, and R H Goudar “TBESP Algorithm for Wireless Sensor Network under Black hole Attack” in proceedings of IEEE International Conference on Communications and Signal Processing Melmaruvathur, India ,pp: 1086 - 1091 2013.

[11] Samir Athmani, Djallel Eddine Boubiche and Azeddine Bilami “Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs” in proceedings of IEEE International Conference on Computer and Information Technology (WCCIT) Sousse, Tunisia ,pp:1-5,2013.