IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 6 (June. 2018), ||V (V) || PP 26-36

Impact Analysis of Attack in Balanced Leach Protocol in Wan

Nitika Singhi[1], Ravi Singh Pippal[2]
[1](Research Scholar, RKDF University, Bhopal)
[2](Professor, Vedica Institute of Technology, RKDF University, Bhopal)
Corresponding Author: Nitika Singhi

Abstract: - This paper aims to analyse the impact of attacks in cluster based Wireless Sensor Networks (WSN). It attempts to analyze performance analysis of attack under Balanced LEACH protocol. In this experiment, the MATLAB simulator is used here to evaluate the performance of different types of attack under Balanced LEACH protocol.

Keywords: - Wireless Sensor Network, Cluster-based, Attack Analysis, Security

---

Date of Submission: 07-06-2018 \ Date of acceptance: 23-06-2018

I. INTRODUCTION

Cluster-Based [1] is considered a clustered mobile wireless network. For structuring the network into distinct however interrelated groups, they elects cluster heads using cluster head selection algorithm. This protocol achieves a distributed process methodology by forming many clusters among a network. However, one disadvantage of this protocol is that the fact that, frequent change or number of cluster heads can be resource hungry plus it would have an effect on the routing performance. CGSR uses DSDV protocol since the underlying routing scheme and, hence, it offers the identical overhead as DSDV. It modifies DSDV algorithm by adding a hierarchal cluster-head-to-gateway based routing technique for routing from source to the final destination. Gateway nodes are nodes that are from the communication ranges of two or additional cluster heads. A packet sent with a node is first sent to its cluster head, and therefore the packet is sent from the cluster head over to a gateway completely to a different cluster head, etc till the cluster head within the destination node is reached. The packet is then transmitted on the destination looking at the own cluster head [2-4].

II. LITERATURE REVIEW

Divya Acharya et al. [5] analyzed the effect of the selected attack is that some data packets can be deleted. The Adaptive Low Energy Cluster Hierarchy (LEACHES) applies cluster rotation randomly to the distribution of energy between all sensor nodes. In this white paper, the creation, detection and removal of selective transfer attacks are performed on LEACH routing in wireless sensor networks. Fares Mezrag et al. [6] proposes a new secure protocol based on the well-known LEACH routing protocol called Hybrid Cryptography Based Scheme for the secure communication of data in the WSN cluster (HCBS). As an approach with several limited criteria, HCBS relies on a combination of elliptical cryptographic curve techniques for the exchange of keys that use symmetric keys for data encryption and MAC operations. Ewa et al. [7] have developed in the test bench networks an SLE-AODV routing protocol that support energy for secure communications in a large-scale WSN network. SLE-AODV was developed on the basis of Ad Hoc Distance (AODV) and Low Energy Adaptive Hierarchy (LEACH). Encrypt data transmitted using Advanced Encryption Standard (AES).

Amira Zrelli and Tahar Ezzedine [8] focused on the hierarchies of specific CTP (Collect Tree Protocol) and LEACH (Hierarchy of Low Energy Adaptive Groups) routing protocols, which are the most commonly used protocols in WSN-based SHM systems. Kaur and Kaur [9] developed a paper for an analyzation and implementation of cluster based routing protocol in MANET networks. MANET is a self-supporting Ad Hoc networks with cellular nodes that can be migrate and connection between each node. Diwaker and Mehla [10] proposed a route optimization technique using PSO and DSDV protocols. This particle swarm intelligence-based route optimization will enhance the life time of the network. It provides gateways and shortest path to find out the sent packets or to initialize the communication between the nodes.

Rahman and Akhtaruzzaman [11] proposed an efficient scheme depends on the speed, distance remaining battery of nodes for determination of route in wireless MANET. To increase the network lifetime and network performance, the difference in velocities and weight has to be balanced. Khalili-Shoja et al. [12] proposed a method using secret mutual chanciness between two or more multiple nodes for communication security. In this paper, network routing metadata by achieving pure randomness generation and secret key agreement. Chaitra and Ravi Kumar [13] discussed improving the life of the network to a certain extent. The

routing of data in the sensor nodes plays a fundamental role in the transmission of data to the base station (BS). Different types of routing algorithms have been used as grid-based, multi-hop, hierarchical and LEACH-based classification, HEED, etc. The existing LEACH protocol is designed in such a way that safety is not considered a problem.

Selim and Chan [14] discussed the fact that there is a difficult problem in the development of various energy-efficient cluster protocols to improve the compromised life with some WSN damaging nodes to apply the most effective group-leader selection approach to extend the life of WSN. The attacks with Gray hole and Black hole are denial of service attacks that reduce the performance of the WSN. Barad and Kadhiwala [15] argued that secure management of communication keys is very important because WSN messages are encrypted because sensor nodes are used in a hostile or remote environment and are not manned by humans. They are vulnerable to various types of attacks. Barad and Kadhiwala [16] Various key management systems in the WSN, deterministic key management system with LEACH, called DKS LEACH, is the system to ensure a wireless sensor network in an efficient way and provides authentication, confidentiality and integrity of acquired data. With DKS-LEACH in energy consumption and resistance against node acquisition is still a problem. Deepa and Latha [17] focused on supporting a safe, resilient and reliable environment with multi-route routing. Efficient routing is an important factor in the global WSN protocol for managing loss of nodes, intrusions and resource limits.

Radhika and Thejiya [18] proposed a MANET network which has improved security. Trust worthiness is used to avoid vulnerable attacks. Trust model is designed using Ad Hoc on demand distance vector routing protocol. Instead of signature verification, cryptography is used. Duan et al. [19] proposed a secure routing framework based on the calculation of the confidence factor. The proposed scheme involves reliable nodes and reliable paths. Finally, the system uses the combination of trust metrics and service quality metrics (QoS) to decide on optimized routing. Tarun Varshney et al. [20] proposed their mechanism to prevent network form Black hole. Their approach is called watchdog mechanism. In their approach, when node sends data, it sets a watchdog. This watchdog monitors that whether the forwarded packet is also forwarded from next node in the route. Anand A. Aware and Kiran Bhandari [21] proposed an approach to prevent Black hole attack. In this approach, first RREP is ignored as it assumes that it is from attacker. When the source node sends the data packet they use SHA 1 hash function for the message digest.

Alrajeh et al. [22] proposed a secure routing protocol based on biologically inspired mechanisms. The proposed protocol recognizes two safe paths between a pair of nodes for data transmission. The protocol is based on an optimization technique for ant colonies. However, this protocol does not take into account the mobility of nodes in the sensor network. Samir Athmani et al. [23] have discussed the fact that the Black hole is one of the most violent attacks that target sensor routing protocols. These types of attacks can have devastating effects on hierarchical routing protocols. Several security solutions have been proposed to protect the WSN from Black hole attacks. Muneer et al. [24] aims to improve the current security mechanisms in wireless sensor networks and to reduce energy consumption. The LEACH protocol provides an energy routing protocol. However, security problems are not covered. Alternatively, this work aims to provide a safer and more energy-efficient routing protocol called LS-LEACH (Lightweight Secure Secure).

Koul et al. [25] discussed link stability, frequency and distance of nodes in MANET. In this paper, link remains connected with neighboring nodes and the communication time is predicted. The next hop node is selected based on the time of link and not by the shortest distance. Nital et al. [26] presented that each node should have Black hole Identification Table (BIT) that contains source, target, current node ID, Packet received count (PRC), Packet forwarded count (PFC). If difference between PRC and PFC is significant, then the node is identified as malicious and is isolated from the network. Mandicou et al. [27] goal of Cluster-based sensor networks is to decrease system delay and reduce energy consumption. LEACH is a cluster-based protocol for micro sensor networks which achieves energy-efficient, scalable routing and fair media access for sensor nodes.

Zhang et al. [28] proposed a new concept of wireless security network security based on an ID-based approach to protect group key management. This approach minimizes the key store request and the number of rekey input communication messages.

Cao et al. [29] proposed a secure feedback-based routing protocol for wireless sensor networks that uses feedback from neighboring nodes to make the routing decision safe and energy efficient. Jiangtao et al. [30] proposed a type of safe LEACH routing protocol (SC-LEACH) based on a low-power cluster head selection algorithm. This protocol will receive the total number of all the nodes of their cooperation in the selection, in order to accurately calculate the current thresholds with which the cluster heads are produced. Nasser and Chen [31] proposed a safe and energy efficient multi-channel routing protocol for wireless sensor networks and, alternatively, uses multiple paths as a communication path between two nodes. Ertau and Chavan [32] explained the elliptic curve cryptography based on threshold, which provides promise of securing the network. MANET is a network; allow communication with each other without any infrastructure. ECC algorithm is more efficient when compared to RSA that gives result as ECC is most suitable method for MANET. Wood et al. [33]

developed a family of secure and configurable routing protocols for wireless sensor networks. It can provide a resource-based security solution that is sufficiently powerful and powerful. Deng et al. [34] proposed their mechanism to prevent network form Black hole. In their mechanism, sender node searches for alternative path of destination node. If path exists then there is node attack. This approach does not prevent from cooperative Black hole attack. Singhi and Pippal have done remarkable contribution in this field [35].

III. ATTACK ANALYSIS UNDER BALANCED LEACH PROTOCOL

In this section, three different attacks are analyzed which are discussed below:

1. Black Hole Attack

It is a type of DoS attack in which packets are dropped from the network and hence reduces the performance efficiency of the network. The malicious node enters into the network and pretends to be having the shortest path to the destination node in order to intercept the data packets. These nodes send the route request reply message to the sender having the shortest path to the destination node and sender node sends them the data packets [36, 37]. Further the malicious node then ultimately drops the data packets instead of forwarding them to the destination node and decreases the performance of the network. In cluster-based network the malicious node or Black node attracts all the data traffic from its neighboring nodes by advertising that it has high residual energy and becomes the cluster head. Ultimately drops all the incoming packets from the neighbors.

2. Sink hole Attack

Sink hole attack also behaves as the Black hole attack with little deviation. In Sink hole attack the malicious node advertises to all the nodes that it has high residual energy and comes in the race of becoming the cluster head node. Once malicious node becomes Cluster head node, it collects data packets and applies attacks such as selective forwarding, altering packets or dropping them instead of dropping all the packets. Apart from these, even fake packets can be sent to the base station node, so that the compromised node is included in the path of packet flow.

3. Gray Hole Attack

In a Gray hole attack, a malicious node uses the LEACH protocol to market itself as a cluster header with a high probability of intercepting packets. Thus, the node removes the intercepted packets with a certain probability. A Gray hole can show its malevolent behavior in different ways. It simply removes packets from specific network nodes as it passes all packets to other nodes [38]. Another type of Gray hole Attack is a maliciously behaving node by dropping packets for a while, but can then switch to normal behavior or forward packets of some ID packets and other packets. A Gray hole can also have a random behavior in which randomly some packets fall while transmitting other packets, making it even more difficult to detect them.

IV. SIMULATION AND RESULT ANALYSIS

The protocol is analyzed by using the radio model which is illustrated in fig 1.

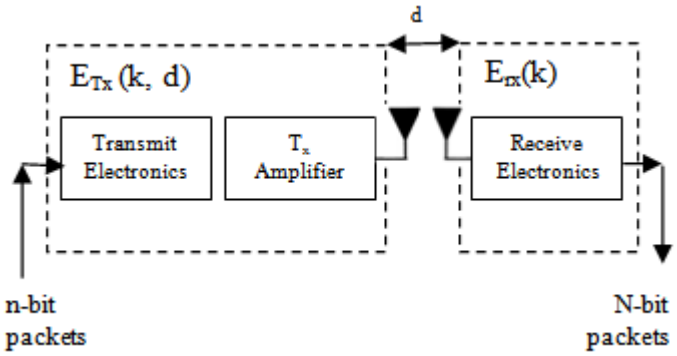

Figure 1: Radio model

In WSN, the radio energy dissipation model is a simple model of wireless energy consumption. The transmitter circuit dissipates the energy needed to operate the transmission electronics and power amplifiers. The receiver circuit dissipates energy to operate only the electronics of the receiver [39]. Depending on the distance between transmitter and receiver, multiple fade and free space channel patterns are used. The free space model (loss of power d^2) is mainly used for communication in a cluster or when the threshold distance is less

than d_0, while the power loss model d^4 is used for communication between clusters. The threshold distance is greater than or equal to d_0. The radio energy consumed by the transmitter to transmit a 1bit message at a distance d is:

$$E_{Tx}(I,d) = E_{Tx-elec}(I) + E_{TX-amp}(I,d)$$
$$= IE_{elec} + IE_{fs}d^2, d < d_o$$
$$= IE_{elec} + IE_{amp}4, d \geq d_o \quad \text{(i)}$$

And energy consumed by the receiver is:

$$E_{Rx}(I) = E_{Rx-elec}(I) = IE_{elec} \quad \text{(ii)}$$

Where E_{elec}=Per bit energy consumed to execute transmitter and receiver
E_{fs}= amplifier energies for free space
E_{amp} = amplifier energies for multipath models
The threshold transmission distance may be chosen as follows:

$$d_o = \frac{E_{fs}}{E_{amp}} \quad \text{(vi)}$$

Following parameters are used for simulation purpose:

Table 1: Simulation Parameters of alive node with Balanced LEACH protocol and various attacks

Parameter Name	Values
Network Area	100*100
Number of nodes	100
Packet Size	4000 bits
Initial Energy, E_O	.5J
Transmitter Energy, ETX	50nJ/bit
Receiver Energy, ERX	50nJ/bit
Amplification Energy for short distance, Efs	10pJ/bit/m^2
Amplification Energy for long distance, Emp	0.0013pJ/bit/m^2
Number of Rounds	2500
Attacks	Black hole, Sink hole, Gray hole

1. Black hole Analysis in Balanced LEACH Protocol

In this research work the MATLAB tool is used to simulate. For simulation environment we have assumed WSN consisted of 100 sensor nodes and nodes are randomly distributed in the 100*100m area as well as base station is located at the coordinates (50,50). The simulation parameters are given above in table 1.

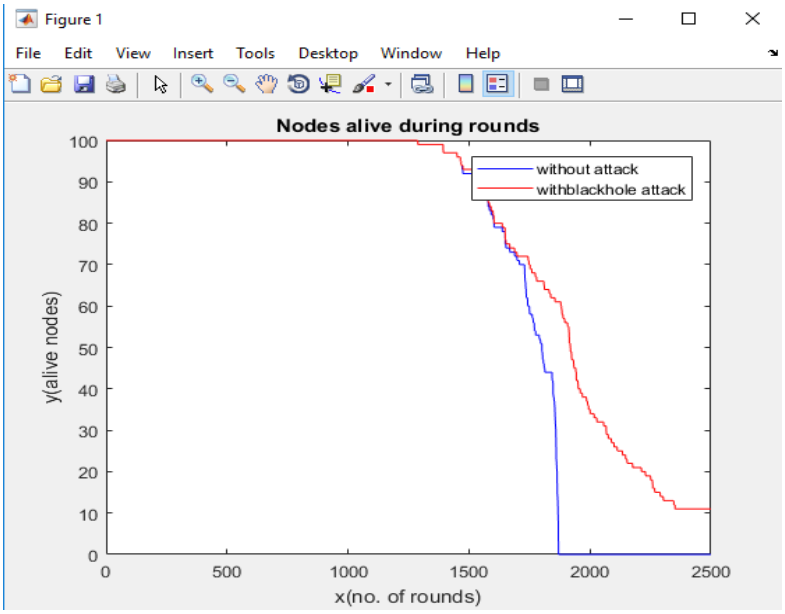

Figure 2: Alive nodes status with black hole attack and without attack

Fig. 2 represents the number of alive nodes in WSN after 2500 rounds. It has been seen from the Fig. that maximum alive node are in Black hole as compared to without attack situation. As it is known that in Black hole attack condition malicious nodes come in the network having highest energy. So, such nodes remain alive for long time in the network.

Fig. 3 represents the number of packets transmitted in WSN after 2500 rounds. It has been seen from the result shown in Fig. 3 that maximum packets are delivered in non-attack condition as compared to the Black hole attack situation because in Black hole attack situation malicious node drops packets.

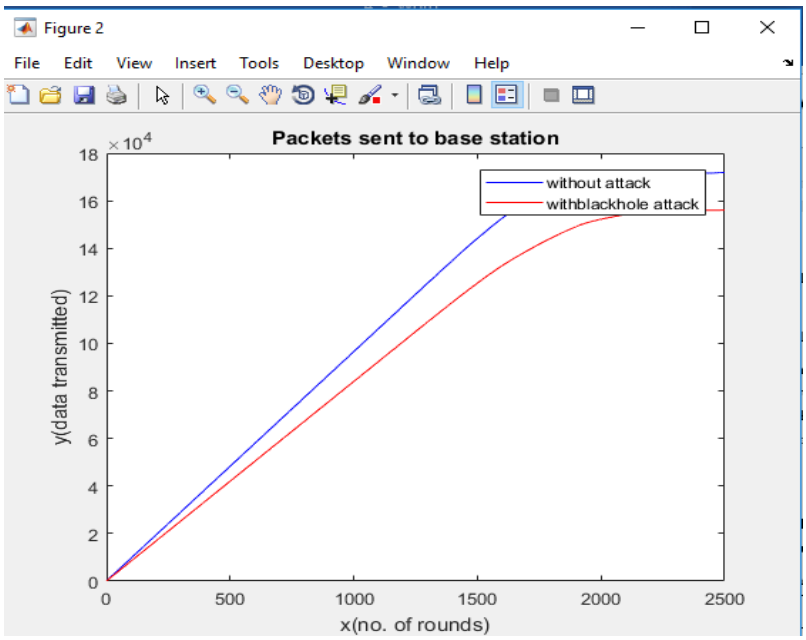

Figure 3: Packets delivery with black hole attack and without attack

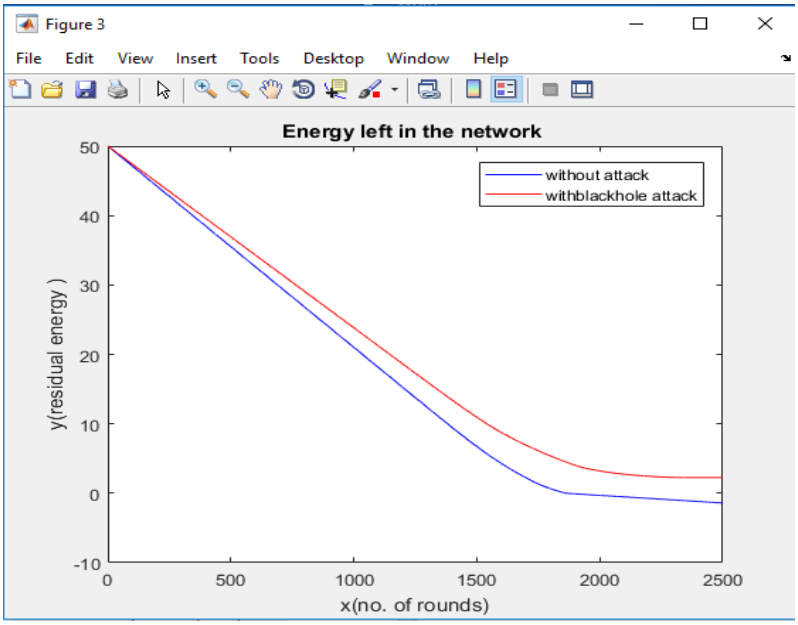

Figure 4: Residual energy with black hole attack and without attack

Fig. 4 represents the residual energy of the network after 2500 rounds. It has been seen from the result shown in Fig. 4 that residual energy is more in Black hole condition as compare non-attack condition because in Black hole attack condition malicious nodes come in the network having highest energy. So, they remain alive in entire network for more time as compared to normal nodes.

2. Sink hole Analysis in Balanced LEACH Protocol

According to this research work first of all Sink hole attack is analyzed under balanced LEACH protocol. Fig. 5 represents the number of alive nodes in WSN after 2500 rounds. It has been seen from the Fig. that maximum alive node is in Sink hole as compared to without attack situation. As it is known that in Sink hole attack condition malicious nodes come in the network having highest energy. So, such nodes remain alive for long time in the network.

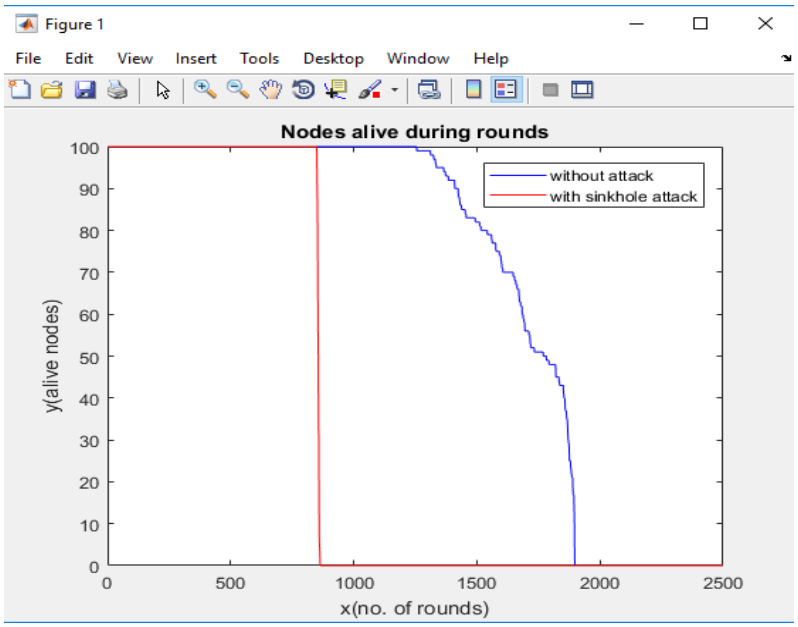

Figure 5: Alive nodes status with sink hole attack and without attack

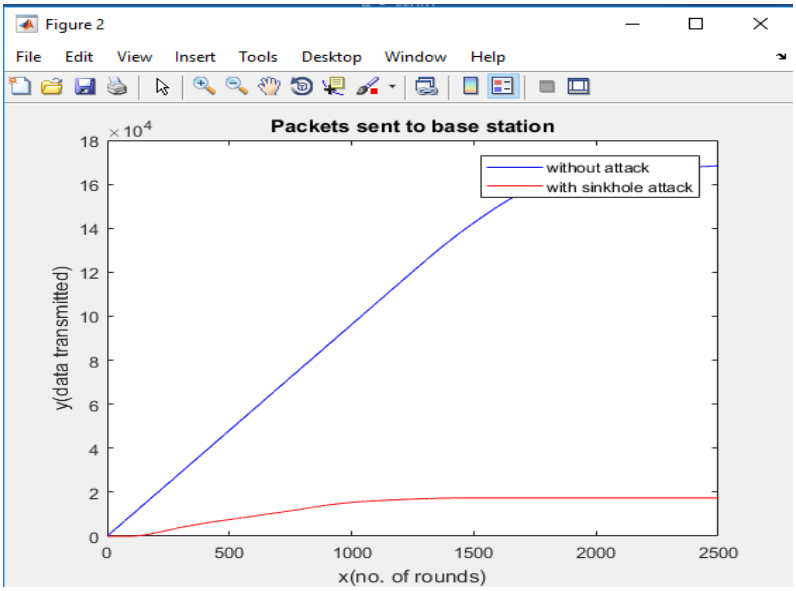

Figure 6: Packets delivery with sink hole attack and without attack

Fig. 6 represents the number of packets transmitted in WSN after 2500 rounds. It has been seen from the result shown in Fig. 6 that maximum packets are delivered in Sink hole attack condition as compared to the non- attack situation because in Sink hole attack situation malicious node may transmit some fake packets to the base station.

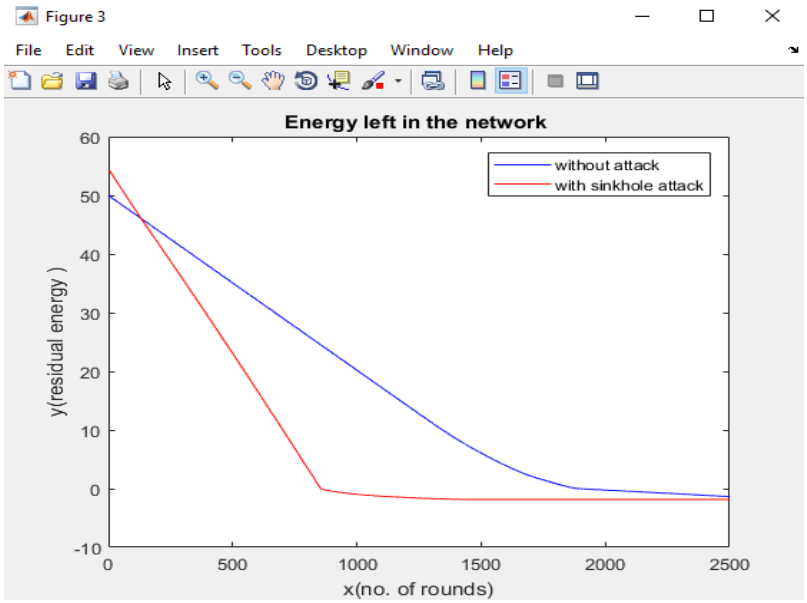

Figure 7: Residual energy with sink hole attack and without attack

Fig. 7 represents the residual energy of the network after 2500 rounds. It has been seen from the result shown in Fig. 7 that residual energy is more in Sink hole condition as compare non-attack condition because in Sink hole attack condition malicious nodes come in the network having highest energy. So, they remain alive in entire network for more time as compared to normal nodes.

3. Gray Hole Analysis in Balanced LEACH Protocol

According to this research work first of all Sink hole attack is analyzed under balanced LEACH protocol.

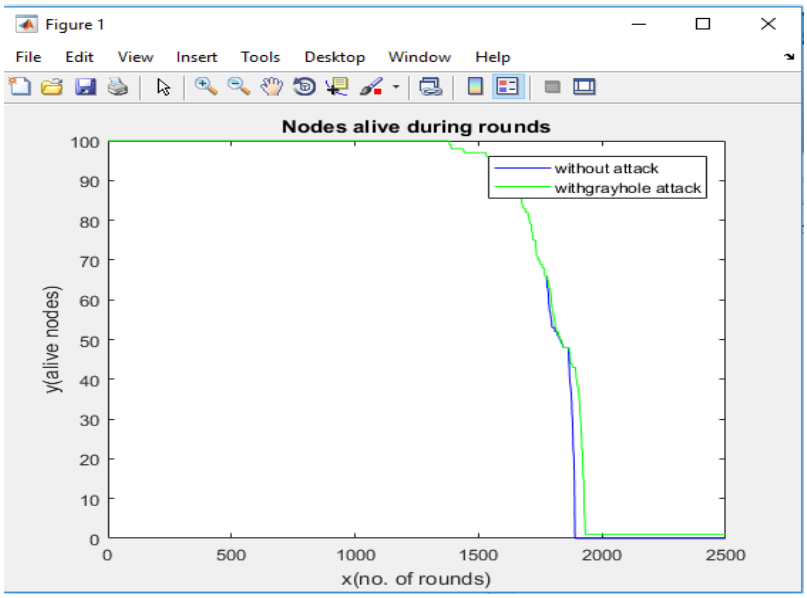

Figure 8: Alive nodes status with gray hole attack and without attack

Fig. 8 represents the number of alive nodes in WSN after 2500 rounds. It has been seen from the Fig. that maximum alive node is in Gray hole as compared to without attack situation. As it is known that in Gray hole attack condition malicious nodes come in the network having highest energy. So, such nodes remain alive for long time in the network.

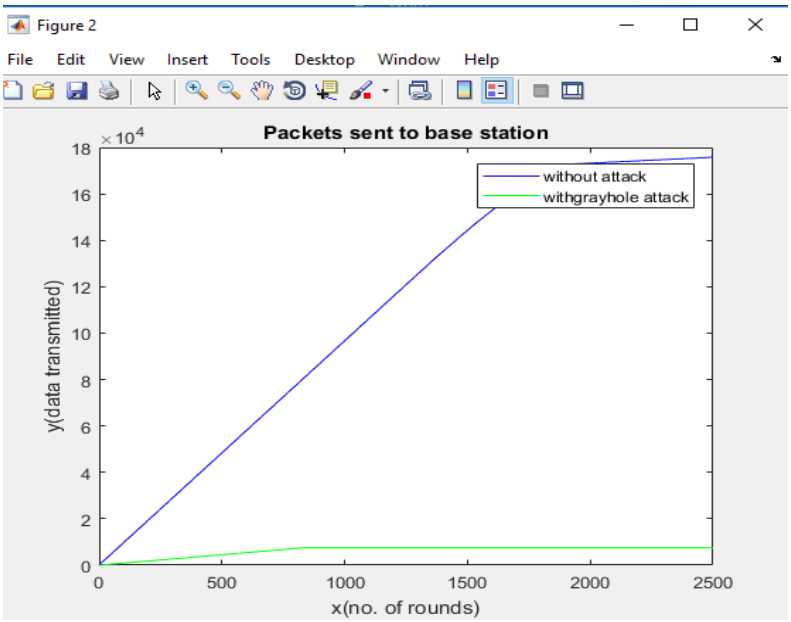

Figure 9: Packets delivery with gray hole attack and without attack

Fig. 9 represents the number of packets transmitted in WSN after 2500 rounds. It has been seen from the result shown in Fig. 9 that maximum packets are delivered in non-attack condition as compared to the Gray hole attack situation because in Gray hole attack situation malicious node drops selected packets.

Fig. 10 represents the residual energy of the network after 2500 rounds. It has been seen from the result shown in Fig. 10 that residual energy is more in Gray hole condition as compare non-attack condition because in Gray hole attack condition malicious nodes come in the network having highest energy. So, they remain alive in entire network for more time as compared to normal nodes.

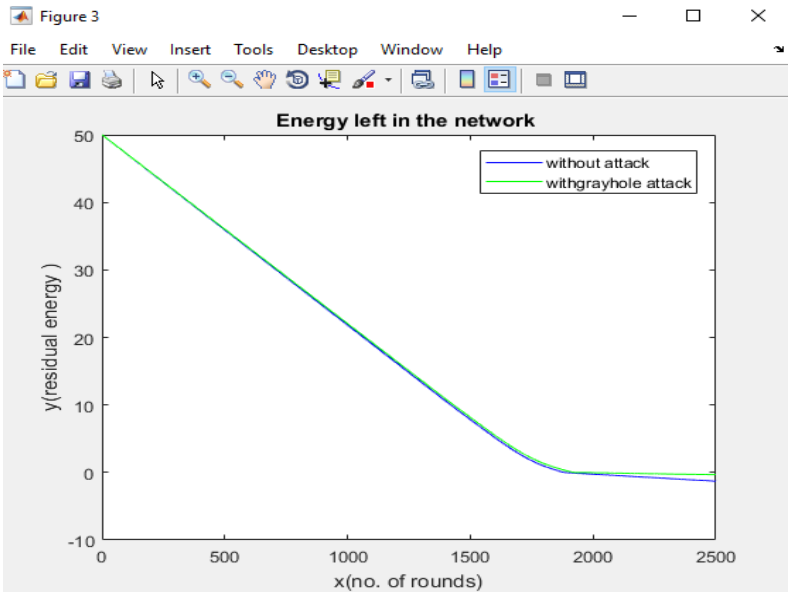

Figure 10: Residual energy with gray hole attack and without attack

V. CONCLUSION

Routing protocols in WSN are vulnerable due to the inherent design disadvantages. Many researchers have used diverse techniques to propose different types of detection and prevention mechanisms for different types of attacks. This paper shows the effect of black hole attack, sink hole attack and gray hole attack on Balanced LEACH routing protocol. As it is known that the cluster based wireless sensor network increases the energy efficiency of the entire sensor network. Attacks in cluster based wireless sensor network reduces the performance of the network with respect to packet delivery as well as energy efficiency.

REFERENCES

[1]. Krishna kumar A, Dr. Anuratha V, "An Energy-Efficient Cluster Head Selection of LEACH Protocol for Wireless Sensor Networks", International Conference on NextGen Electronic Technologies: Silicon to Software (ICNETS2) IEEE, 2017.

[2]. Wided Abidi, Tahar Ezzedine, "Fuzzy Cluster Head Election Algorithm based on LEACH protocol for Wireless Sensor Networks", Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International IEEE, 2017.

[3]. N.G. Palan, B.V. Barbadekar, Suahs Patil, "Low Energy Adaptive Clustering Hierarchy (LEACH) Protocol: A Retrospective Analysis", International Conference on Inventive Systems and Control, 2017

[4]. Ali Al Essa, Xuan Zhang, Peiqiao Wu and Abdelshakour Abuzneid, "ZigBee Network Using Low Power Techniques and Modified LEACH Protocol", Systems, Applications and Technology Conference (LISAT) IEEE, 2017.

[5]. Divya Acharya, Shubh Lakshmi Agrwal, Pankaj Sharma, Sandeep Kumar Gupta, "Performance analysis of detection technique for select forwarding attack on WSN", Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on IEEE, 2017.

[6]. Fares Mezrag, Salim Bitam, Abdel hamid Mellouk, "Secure Routing in Cluster-Based Wireless Sensor Networks", GLOBECOM 2017-2017 IEEE Global Communications Conference, 2017.

[7]. Ewa Niewia domska-Szynkiewicz, Filip Nabrdalik, "Secure low energy AODV protocol for wireless sensor networks", Telecommunication Networks and Applications Conference (ITNAC) IEEE, 2017.

[8]. Amira Zrelli, Tahar Ezzedine, "Evaluation of CTP and LEACH protocols for structural health monitoring systems", Intelligent Computer Communication and Processing (ICCP), 2017 13th IEEE International Conference, 2017.

[9]. Kaur, M., Kaur, S., "Analyze and implementation of cluster based routing protocol in MANETs", International. Journal Innovative Research in Science Engineering Technology Volume 5, issue 3, pp. 3098–3107, 2016.

[10]. Diwaker, C.,Mehla, "Based route optimization technique to enhance network lifetime", Int. J. Adv. Res. Computer Science Software Engineering Volume 6, issue 7, pp. 205–210, 2016.

[11]. Rahman, M., Akhtaruzzaman, "An efficient position-based power aware routing algorithm in mobile Ad Hoc networks", I. J. Computer Network Information Security Volume 7, pp. 43–49, 2016.

[12]. Khalili-Shoja, M.R., Amariucai, G.T., Wei, S., Deng, J., "Secret common randomness from routing metadata in Ad Hoc networks", IEEE Transaction on Information Forensics Security, Volume 11, issue 8, pp. 1674–1684, 2016.
[13]. H. V. Chaitra, G. K. Ravi kumar, "A secure and energy efficient cluster optimization by using hierarchical clustering technique", Devices, Circuits and Systems (ICDCS), 3rd International Conference IEEE, 2016.
[14]. Bassant Selim, Chan YeobYeun, "Key Management for the MANET: A Survey", International Conference on Information and Communication Technology Research, IEEE, 2015.
[15]. Jaydeep Barad, Bintu Kadhiwala, "DIST-LEACH: A deterministic key management scheme for securing cluster-based sensor networks", Advances in Engineering and Technology Research (ICAETR), 2014 International Conference IEEE, 2014.
[16]. Jaydeep Barad, Bintu Kadhiwala, "Improvement of deterministic key management scheme for securing cluster-based sensor networks", Networks & Soft Computing (ICNSC), 2014 First International Conference IEEE, 2014.
[17]. C. Deepa, B. Latha, "HHCS: Hybrid hierarchical cluster based secure routing protocol for Wireless Sensor Networks", Information Communication and Embedded Systems (ICICES), 2014 International Conference IEEE, 2104.
[18]. Radhika, N., Thejiya, V., "Trust based solution for mobile Ad Hoc networks", International Journal Advance Research in Computer Science Software Engineering, Volume 4, issue 5, pp. 73–82, 2014.
[19]. Junqi Duan, Dong Yang, Haoqing Zhu, Sidong Zhang and Jing Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks. International Journal of Distributed Sensor Networks", doi:10.1155/2014/209436, 2014.
[20]. Varshney, T., Sharma, T., Sharma, P., "Implementation of watchdog protocol with AODV in mobile Ad Hoc network", International Conference on Communication Systems and Network Technologies (CSNT), pp. 217–221, IEEE, 2014.
[21]. Aware, A.A., Bhandari, K., "Prevention of Black hole attack on AODV in MANET using hash function", International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), pp. 1–6, IEEE, 2014.
[22]. Nabil Ali Alrajeh, Mohamad Souheil Alabed, Mohamed Shaaban Elwahiby, "Secure ant-based routing protocol for wireless sensor network", International Journal of Distributed Sensor Networks doi:10.1155/2013/326295, 2013.
[23]. Samir Athmani, DjallelEddineBoubiche, AzeddineBilami, "Hierarchical energy efficient intrusion detection system for Black hole attacks in WSNs", Computer and Information Technology (WCCIT), World Congress IEEE, 2013.
[24]. Muneer Alshowkan, Khaled Elleithy, Hussain Alhassan, "LS-LEACH: A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks", Distributed Simulation and Real Time Applications (DS-RT), IEEE/ACM 17th International Symposium IEEE, 2013.
[25]. Koul, A., Patel, R.B., Bhat, V.K. "Distance and frequency based route stability estimation in mobile Ad Hoc networks", J. Emerg. Technol. Web Intell. Vol 2, issue 2, pp. 89–95, 2010.
[26]. Nital Mistry, Devesh C Jinwala, Zaveri, "Improving AODV Protocol against Black hole Attacks", International Multiconference of Engineers and Computer Scientist VolumeII 2010.
[27]. Mandicou Ba, IbrahimaNiang, BambaGueye, Thomas Noel, "A Deterministic Key Management Scheme for Securing Cluster-Based Sensors Networks", Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference IEEE, 2010.
[28]. Zhang, J., &Varadharajan, V., "A new security scheme for wireless sensor networks", In Proceedings of IEEE Global Telecommunications Conference, 2008.
[29]. Cao, Z., Hu, J., Chen, Z., Xu, M., & Zhou, X., "FBSR: Feedback based secure routing protocol for wireless sensor networks", International Journal of Pervasive Computing and Communications, 1(1), 1–8, 2008.
[30]. Jiangtao Wang, Geng Yang, Shengshou Chen, Yanfei Sun, "Secure LEACH routing protocol based on low-power cluster-head selection algorithm for wireless sensor networks", Intelligent Signal Processing and Communication Systems, ISPACS . International Symposium IEEE, 2008.
[31]. Nasser, N., & Chen, Y., "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", Computer Communications, 30, 2401–2412, 2007.
[32]. Ertau, L., Chavan, N.J., "Elliptic curve cryptography based threshold cryptography (ECC-TC) implementation for MANETs", IJCSNS International Journal Computer Science Network Security Volume 7, issue 4, pp. 48–61, 2007.
[33]. Wood, A. D., Fang, L., Stankovic, J. A., & He, T., "SIGF: A family of configurable, secure routing protocols for wireless sensor networks", In Proceedings of SASN, Virginia, USA, Oct 2006.

[34]. Deng, Hongmei, Li, Wei, Agrawal, Dharma P., "Routing security in wireless Ad Hoc networks", IEEE Communications Magazine Volume 40, issue 10, pp. 70–75, 2002.
[35]. Nitika Singhi and Ravi Singh Pippal, "Analysis of Key Management Schemes in MANET," International Journal of Applied Environmental Sciences, Volume 13, Issue 2, 2018, pp. 161-169.
[36]. Padmalaya Nayak, V. Bhavani, B. Lavanya, "Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN", International Journal of Computer Applications, Volume 116 – No. 4, April 2015.
[37]. Gurung, S, Saluja, K. K., "Mitigating impact of Black hole attack in MANET", In Proceedings of 5th, ACEEE International Conference on Recent Trends in Information, Telecommunication and Computing, ITC, pp. 229–237, 2014.
[38]. X. Gao and W. Chen, "A novel Gray-hole attack detection scheme for mobile Ad Hoc networks". International Conference on network and parallel computing workshops, pp. 209–14, 2007.
[39]. Yuan, Y., Yang, Z., He, Z., & He, J., "An integrated energy aware wireless transmission system for QoS provisioning in wireless sensor network", Computer Communications, 29, 162–172, 2006.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Nitika Singhi "Impact Analysis of Attack in Balanced Leach Protocol in Wan." IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 6, 2018, pp. 26-36.