IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 2 - V7I2-1364)
Available online at: https://www.ijariit.com

Detection and Prevention of Black hole attack by Grey Wolf Optimization in Wireless Sensor Network

Nasir Hussain Mir
nasirmir390@gmail.com
Adesh Institute of Technology, Gharuan, Punjab

Dr. Rajat Joshi
errajatjoshi@gmail.com
Adesh Institute of Technology, Gharuan, Punjab

ABSTRACT

Wireless sensor network is a group of nodes that are connected to each other by wireless connection. These types of network work on the dynamic topology of the network because positions of nodes in the wireless network are changing continuously. The nodes in WSN are basically made up of small electronics device which are used for sensing, computing and transmitting the data. The nodes are run on the battery power during communication process. The battery consumption in WSN is very high due to high computation operations on it. In the recent years WSN grows at very high at the research area is also increased in this field to provide effective computation. major concern for maintaining the security of the system greatly depends upon the limited energy of the sensor nodes. Thus the communication and the computational measures for the measure of security should be kept small. Dealing with the issues related to security, the limited form of energy provides a challenging path with an additional set target research work done on the wireless sensor network by using the concept of leach routing of nodes and optimize the routing process by using Grey Wolf Optimization algorithm. The GWO algorithm provides the optimal results. The optimal result provided by GWO reduced the time delay, dead nodes and energy consumption and improve the network quality.

Keywords: *Wireless Sensor Network, Grey Wolf Optimization algorithm, MANET*

1. INTRODUCTION

There are three main components in WSN: nodes, gateways and software. Spatially distributed measured node's interface with sensors to monitor assets. The collected data transmit to gateway wirelessly, and can operate independently. It is connected to a host system where we can collect data, process, analyze and present our measurement data by using software. To extend WSN distance and reliability special type of measurement node is used such as router node. WSN is a widely used system because of its low costs and high efficiency.

In a typical wireless sensor network (WSN), sensor nodes consist of sensing, communicating, and data processing components. Sensor nodes can be used in numerous industrial, military, and agricultural applications, such as transportation traffic monitoring, environmental monitoring, smart offices, and battlefield surveillance. In these applications, sensors are deployed in an ad-hoc manner and operate autonomously. In these unattended environments, these sensors cannot be easily replaced or recharged, and energy consumption is the most critical problem that must be considered. The sensor is a small device which is used to detect the amount of physical parameters,event occurring, measures the presence of an object and then it converts the electrical signal value according to need it actuates a process using electrical actuators.

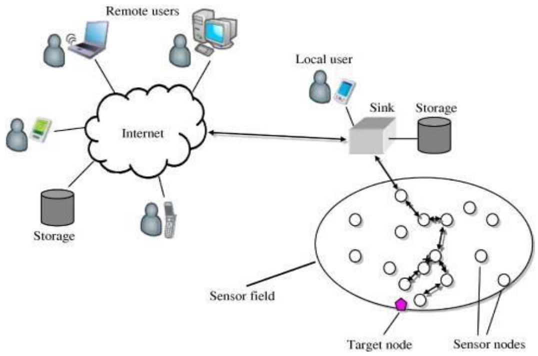

Fig. 1.2: WSN Architecture

ATTACKS

In WSN, the attacks are mainly affecting the functionality of network layer which is responsible for the routing in MANET. There are mainly two types of attacks which are occurred in the mobile ad-hoc network.

A. Active Attack

In active attack, attacker modifies the content of data which is exchanged in the network. In this process attacker can inject the new packets, drop the packets and modify the existing data packets. This type of attacks is very harmful for the network and the senders. It is further divided into two parts the attack done by the node which present in network is called internal attack and node which attack from outside is called external attack.

B. *Passive Attack*

In passive attack, the attacker captures the data without altering of modifying it. This attack does not affect the normal working of the network this is the main difficulty reason

in detection. This attack is done mainly to gather the information about the communication between the sender and receiver.

Attacks on Wireless Sensor Networks

Wireless sensor network is used in various fields for the effective communication process in which user sends their information from one node to another node. Sometimes a user sends the secret information, data on the wireless network, it is very important to send this information very safely. In this network sensor nodes used wireless communication and it is easy to eavesdrop. The attacker can easily inject malicious messages into the network.

Types of Attacks in WSN

- Grey Hole Attack: This attack is modification of black hole attack. In this attack attacker node behaves like a normal node for discovering route in the network. After it discovers the route then it drop the infected packets in network. This attack is difficult to detect because packet is dropped with certainty [4].

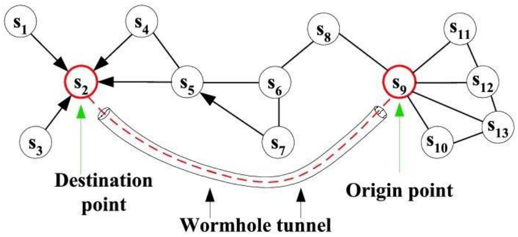

Fig. 1: Wormhole Attack

- Wormhole Attack: In wormhole attack, the attacker can record the data packets at one location in the network and retransmit the data from another route of the data. Wormhole attack is a serious issue that occurred into the wireless sensor network. In the figure [1.3] the tunnel may be a wired link or wireless link between two nodes, this creates an illusion that the end point are very close to each other [2].

A wormhole attack has two modes.

1. Hidden mode
2. Participation mode

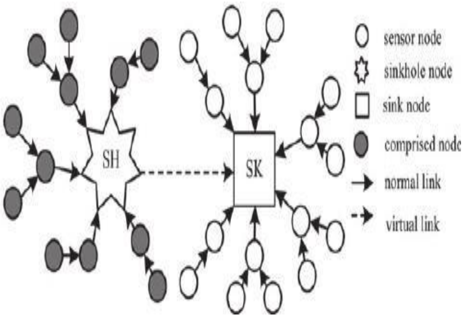

Fig. 2: Sinkhole Attack

- Black hole Attack: in this attack incorrect information of the routing is send to the nodes as it is low cost and it provides proper destination node. Due to incorrect routing information it leads to packet loss and manipulation in original data packets. This attack disturbs all the network process because nodes are sometime dependent on each other for information [4].

2. RELATED WORK

In [1] explained an energy efficient sinkhole detection approach which detects the malicious node effectively than the existing nodes. In this approach frequency of all nodes is established by m routes with optimal hops from per node to sink node. This method is based on the dynamic programming. This approach enhanced the detection rate and false positive rate.

In [2]proposed neighbor constraint traffic centric approach which is used to detect sinkhole attack and improve the quality of the WSN. It identifies the malicious node by the data send by neighbor node. It verifies the location of the node from where data is send to the node. This method provides sinkhole detection with high throughput and packet delivery ratio.

In [3] described the anomaly detection approach which detects the sinkhole attack in wireless sensor networks. This type of attack is not easy to detect due virtual path of the node. In this work Acceptance Acknowledgement approach is used to activate the digital signature system. This approach does not make any impact on the network and provides high detection rate of the malicious node.

In[4]proposed the RAEED protocol which is used to detect the simple and intelligent tunnel attacks. This protocol helps to reduce the problem of DOS attack which disturbs the data routing and forward the data comes from the sink node. In future this work will be enhanced by applying formal methods to verify the communication issues.

In [5] worked on the detection of sinkhole attack in AODV routing. This method uses energy power consumption in AODV and external energy by using battery. In this work MD5 algorithm is proposed for black hole attack detection which prevent the network from the sever attack. This algorithm checks the energy transmitted by the node to the other nodes. This algorithm work effectively and enhance the packet delivery rate and throughput. It reduces the end to end delay in the network.

In [6] described the adaptive sinkhole aware algorithm in wireless sensor network. This work is based on the finding probability of affected nodes by sinkhole attack. In this the routing of the nodes is based on AODV protocols to route packets over the most reliable nodes. The subjective model identifies the behavior of the nodes in data receiving and sending. The behavior of whole network is observed by using probabilistic automation and captures the behavior of the network which is generated at the base station. The result of the proposed approach provides low packet loss rate and effective routing between the reliable nodes.

In [7] worked on the clustered network in wireless sensor network to detect the sinkhole attack. This method is based on the agent-based quality of service to detect the sinkhole attack. The agent- based approach detects the attack effectively and enhances the network performance. Agent based protocol is very helpful to provides the effective performance and throughput.

In [8] in this paper, the author proposed optimized link state routing mechanism to solve the issues of attacks in the wireless sensor networks. In this protocol trust based mechanism is used with fuzzy rules to evaluate the trust values of the mobile nodes. This algorithm selects the route on the basis of maximum path trust value between the nodes. To evaluate the trust of nodes trust factor collection method is used. It generates only relevant information and do not generate extra control messages. In results it enhances the packet delivery ratio and latency and reduced the network overhead.

In [9] proposed an intrusion detection system and attach it of the wireless sensor network to detect the sinkhole attacks. In this work author studies and analyzed how black hole attack is performed on the real network and uses MintRoute protocol. This protocol uses link quality metric to build the routing trees. By using tiny OS and proposed protocol sinkhole attack is detected effectively in random topologies also.

In [10] proposed sinkhole detectionon the basis of LQI in meshed routing network. Sinkhole attack can also modify in various type of attack. The attack can be detected by using few detector nodes.

In [11] worked on the clustered network in wireless sensor network to detect the sinkhole attack. This method is based on the agent-based quality of service to detect the sinkhole attack. The agent- based approach detects the attack effectively and enhances the network performance. Agent based protocol is very helpful to provides the effective performance and throughput.

In [12] In this paper, the author focused on the packet scheduling technique for the ad-hoc on demand distance vector (AODV) protocol. In this transitional node starts the packet scheduling and manage the memory, according to the flow of data. Data packets are stored and route repaired y the intermediate node. In the proposed scheme data packets are utilized by backup routes not to dropping it.

In [13] Proposed two types of defense strategies that are based on the monitoring the behavior of neighboring node and location information of the neighboring node. In this paper, the concept of packet encapsulation is used to provide the most effective method for wormhole attack. Running a state is simulated under the normal condition and wormhole condition by using OMNET++ simulation environment. In wormhole attack, the running state applies to defense method which is based on location information and monitoring the neighbor node. The analysis results of the simulation show that it works effectively on the attacks in WSN.

3. PROPOSED APPROACH

Grey Wolf Optimizer (GWO)

Grey Wolf optimization algorithm is a bio-inspired algorithm which is based on the leadership and hunting behavior of the wolves in the pack. The grey wolves prefer to live in the pack which is a group of approximate 5-12 wolves. In the pack each member has social dominant and consisting according to four different levels. The below given figure shows the social hierarchy of the wolves which plays and important role in hunting.

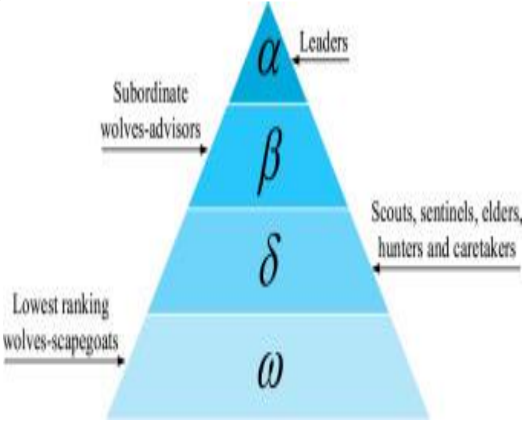

Fig. 3: GWO Hierarchy [36]

1. The wolves on the first level are called alpha wolves (α) and they are leaders in the hierarchy. Wolves at this level are the guides to the hunting process in which other wolves seek, follow and hunt and work as a team. Decision making is the main task that is performed by the alpha wolves and the order by the alpha wolves is followed by all members of the pack.

2. Second level wolves are called beta (β). These wolves are called subordinates and advisors of alpha nodes. The beta wolf council helps in decision making. Beta wolves transmit alpha control to the entire packet and transmit the return to alpha.

3. The wolves of the third level are called Delta wolves (δ) and called scouts. Scout wolves at this level are responsible for monitoring boundaries and territory. The sentinel wolves are responsible for protecting the pack and the guards are responsible for the care of the wounded and injured.

4. The last and fourth level of the hierarchy are called Omega (ω). They are also called scapegoats and they must submit to all the other dominant wolves. These wolves follow the other three wolves.

Grey wolves have the ability of memorizing the prey position and encircling them. The alpha as a leader performs in the hunt. For simulating the grey wolves hunting behavior in the mathematical model, assuming the alpha (α) is the best solution. The second optimal solution is beta (β) and the third optimal solution is delta (δ). Omega (ω) is assumed to be the candidate solutions. Alpha, beta, and delta guide the hunting while position should be updated by the omega wolves by these three best solutions consideration.

Encircling prey

Prey encircled by the grey wolves during their hunt. Encircling behavior in the mathematical model, below equations is utilized.

$$\vec{A}(T+1) = \overrightarrow{A_P}(T) - \vec{X}.\vec{Z}$$

$$\vec{Z} = \left|\vec{Y}.\overrightarrow{A_P}(T) - \vec{A}(T)\right|$$

Where

T←iterative number

$\vec{A}$←grey wolf position

$\overrightarrow{A_P}$←prey position

$$\vec{X} = 2x.\overrightarrow{r_1} - x$$

$$\vec{Y} = 2\overrightarrow{r_2}$$

Where

$\overrightarrow{r_1}$and$\overrightarrow{r_2}$←random vector range[0,1]

The x value decreased from 2 to 0 over the iteration course.

$\vec{Y}$←random value with range [0,1] and is used for providing random weights for defining prey attractiveness.

Hunting

For grey wolves hunting behavior simulation, assuming α, β and δ have better knowledge about possible prey location. The three best solutions firstly and ω (other search agents) are forced for their position update in accordance to their best search agents position. Updating the wolves' positions as follows:

$$\vec{A}(T+1) = \frac{\overrightarrow{A_1}+\overrightarrow{A_2}+\overrightarrow{A_3}}{3} \qquad (1)$$

Where $\overrightarrow{A_1}, \overrightarrow{A_2}, and\ \overrightarrow{A_3}$ are determined,

$$\overrightarrow{A_1} = \left|\overrightarrow{A_\alpha} - \overrightarrow{X_1}.Z_\alpha\right|$$

$$\overrightarrow{A_2} = \left|\overrightarrow{A_\beta} - \overrightarrow{X_2}.Z_\beta\right|$$

$$\overrightarrow{A_3} = \left|\overrightarrow{A_\delta} - \overrightarrow{X_3}.Z_\delta\right|$$

Where $\overrightarrow{A_\alpha}, \overrightarrow{A_\beta}, and\ \overrightarrow{A_\delta}$ ← first three best solution at a given iterative T

Z_α, Z_β, and Z_ω are determined,

$$\overrightarrow{Z_\alpha} \leftarrow \left|\overrightarrow{Y_1}.\overrightarrow{A_\alpha} - \vec{A}\right|$$

$$\overrightarrow{Z_\beta} \leftarrow \left|\overrightarrow{Y_2}.\overrightarrow{A_\beta} - \vec{A}\right|$$

$$\overrightarrow{Z_\delta} \leftarrow \left|\overrightarrow{Y_3}.\overrightarrow{A_\delta} - \vec{A}\right|$$

The parameter x updating is the final process. The parameter x exploitation and exploration is updated linearly for ranging [2,0] in every iteration.

$$x = 2 - t\frac{2}{maxI}$$

Where

T←iterative number

MaxI←total number of iteration

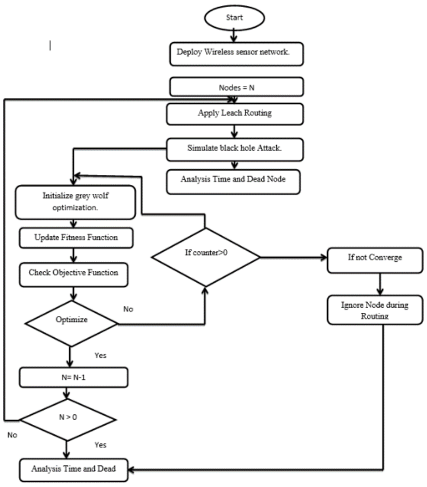

Fig. 4: Proposed approach

3. RESULT AND ANALYSIS

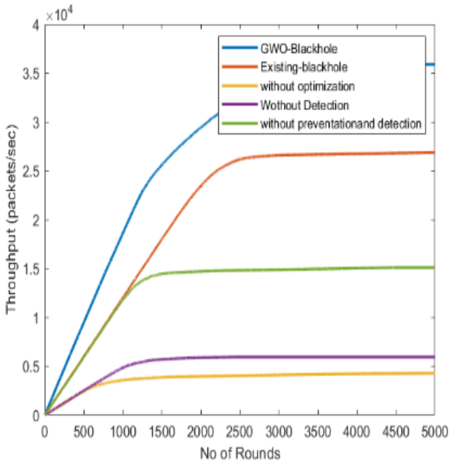

Fig. 5: Comparison of throughput in proposed and existing approaches

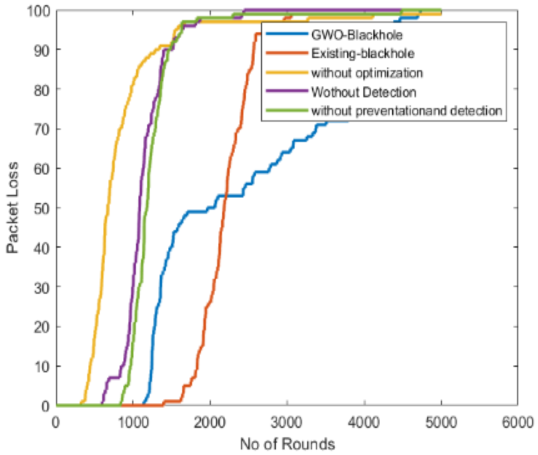

Fig. 6: Comparison of Packet loss in proposed and existing approaches

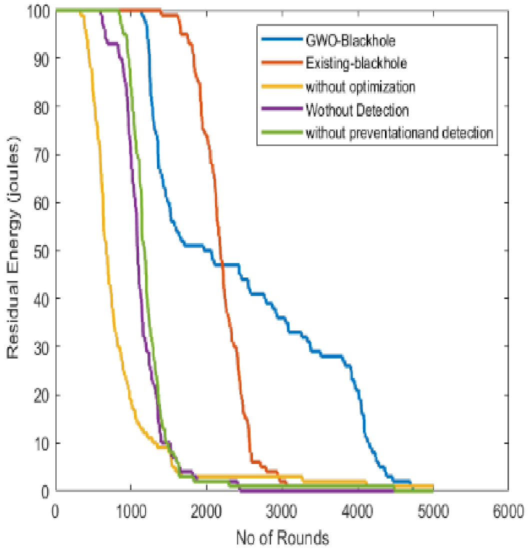

Fig. 7: Comparison of Residual energy in proposed and existing approaches

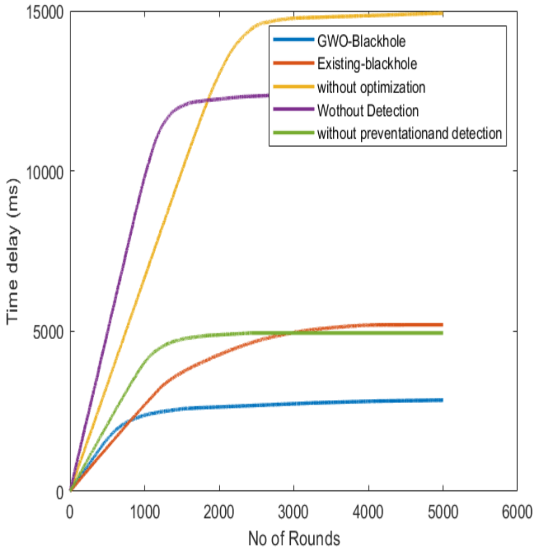

Fig. 8: Comparison of Time delay in proposed and existing approaches

5. CONCLUSION

Attacker modifies the content of data which is exchanged in the network. In this process attacker can inject the new packets, drop the packets and modify the existing data packets. This type of attacks is very harmful for the network and the senders. It is further divided into two parts the attack done by the node which present in network is called internal attack and node which attack from outside is called external attack.Reduce the confliction of attacker node by monitoring optimization approach. In the wireless sensor network energy reduction is important parameter, so attacker node shows the conflicts of shortest path and energy so routing will go through attacker node and drop the packet. So the challenge is monitoring the node behavior, in every node which reduces the energy loss and drop packet. To protect the network from the jamming attack the hybrid model is used in which three defense approaches are used for replication, evasion, and multipath routing. This approach provides effective communication on WSN and gives efficient results. Proposed sinkhole detection based on LQI in meshed routing network. Blackhole attack can also modify in various type of attack. The attack can be detected by using few detector nodes.

6. REFERENCES

[1] Amish, Parmar, and V. B. Vaghela. "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol." Procedia computer science 79 (2016): 700-707.

[2] Choi, Byung Goo, et al. "A sinkhole attack detection mechanism for LQI based mesh routing in WSN." Information Networking, 2009. ICOIN 2009. International Conference on. IEEE, 2009.

[3] Devibala, K., et al. "Neighbor constraint traffic centric distributed sinkhole detection and mitigation approach for quality of service improvement in wireless sensor networks." Industry Interactive Innovations in Science, Engineering and Technology. Springer, Singapore, 2018. 357- 366.

[4] Jan, Mian, et al. "PAWN: a payload-based mutual authentication scheme for wireless sensor networks." Concurrency and Computation: Practice and Experience29.17 (2017).

[5] Jahandoust, Ghazaleh, and FatemehGhassemi. "An adaptive sinkhole aware algorithm in wireless sensor networks." Ad Hoc Networks 59 (2017): 24-34.

[6] Kalnoor, Gauri, JayashreeAgarkhed, and Siddarama R. Patil. "Agent-Based QoS Routing for Intrusion Detection of Sinkhole Attack in Clustered Wireless Sensor Networks." Proceedings of the First International Conference on Computational Intelligence and Informatics. Springer, Singapore, 2017.

[7] Krontiris, Ioannis, et al. "Intrusion detection of sinkhole attacks in wireless sensor networks." International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics. Springer, Berlin, Heidelberg, 2007.

[8] Kumar, Gulshan, Mritunjay Kumar Rai, and Rahul Saha. "Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in Wireless Sensor Networks." Journal of Network and Computer Applications 99 (2017): 10-16.

[9] Ma, Rui, et al. "Defenses Against Wormhole Attacks in Wireless Sensor Networks." International Conference on Network and System Security. Springer, Cham, 2017.

[10] Patel, Manish M., and Akshai Aggarwal. "Two phase wormhole detection approach for dynamic wireless sensor networks." Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. IEEE, 2016.

[11] Saghar, Kashif, HunainaFarid, and Ahmed Bouridane. "Formally verified solution to resolve tunnel attacks in wireless sensor network." Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on. IEEE, 2017.

[12] Tan, Shuaishuai, Xiaoping Li, and Qingkuan Dong. "Trust based routing mechanism for securing OSLR-based MANET." Ad Hoc Networks 30 (2015): 84-98.

[13] Vidhya, S., and T. Sasilatha. "Sinkhole Attack Detection in WSN using Pure MD5 Algorithm." Indian Journal of Science and Technology 10.24 (2017).

[14] Yasin, N. Mohammaed, et al. "ADSMS: Anomaly Detection Scheme for Mitigating Black hole Attack in Wireless Sensor Network." Technical Advancements in Computers and Communications (ICTACC), 2017 International Conference on. IEEE, 2017.

[15] Zhang, Zhaohui, et al. "M optimal routes hops strategy: detecting sinkhole attacks in wireless sensor networks." Cluster Computing (2018):