A Review on Energy Consumption Minimization using Various Methods

Kanika Madaan, Nisha Nandal, Ravi Malik
Student, Student, Assistant Professor (HOD)
Electronics & Communication Engineering Department
Geeta Engineering College, Panipat, India.

Abstract- In the present scenario the energy usage increasing day by day. To fulfill the energy requirement we use different techniques. The wireless sensor network (WSN) is the basic system. Its demand is increasing sharply because it has many advantages. This type of system connects to the virtual world as well as the physical world. By using the optimization algorithm the efficiency can be increased. Study of various papers give the idea of minimization of energy can be very useful in the WSN. Some of the algorithms like GA and MAC used for this purpose. EKF also gives the better results. The various attacks present in the MANET system like black hole attack. So for the detection of these attacks and repair they provide the less energy loss. The BHPD technique is used with the fuzzy logic case obtained the great solution to the network. Therefore in this paper a study of various methods of WSN for the minimization of energy consumption provided.

Keywords - MANET, GA, Fuzzy Logic, GWO etc.

I. INTRODUCTION

A wireless sensor network is comprised of different sensor nodes, small in size, battery powered devices that can communicate and compute signals with other nodes. Now days, a smart sensor network are deployed in large numbers to provide opportunity for monitoring and controlling homes, cities and the surroundings. In addition, they have a wide range of applications in providing new technology for surveillance, defense field. Sensors incorporated into machinery, structures and the environments are joined with the effective transmission of sensed data that can offer enormous benefits to guild. A sensor network is an infrastructure consist of sensing, computing, and communication elements that gives an administrator the capability to instrument, observe, and react to events and phenomena in a specified environment. A wireless sensor network (WSN) contains a number of gateway (or "base station") that can pass information with a number of sensors nodes via a wireless connection. Information gathered by the node is compressed and sent to the base station directly or if required, it uses other nodes to transfer information to the base station. The information which is transferred, then utilized by base station connection.

The wireless network transmission medium has a broadcast nature. Hence, it is more susceptible to security attacks compared with the traditional wired network. In wireless sensor networks, nodes can be deployed randomly in the hostile environment so an adversary can easily attack the targeted WSNs [18]. The security of WSNs can be investigated in different perspectives. This work formulate a threat model that distinguishes two major types of attacking classes [28 – 30] namely, (i) based on attacker's location, and (ii) based on attacker's strength. In this research, the work focused on the internal attacks of a WSN. In order to clarify all those mentioned terminologies, the definitions are described below: Attacks based on attacker's location Attacks based on attacker's location ocation: Based on knowledge and privileges of the attacker, attacks can be categorized as insider (internal) and outsider (external) depending on whether the attacker is a legitimate node of the network or not [22]. Attacks can also be classified as passive and active attacks.

Internal attacks*:* When a legitimate node of the network acts abnormally or illicitly it is considered as an internal attack. It uses the compromised node to attack the network which can destroy or disrupt the network easily. An adversary by physically capturing the node and reading its memory can obtain its key material and forge network messages. Having access to legitimate keys can give the attacker the ability to launch several kinds of attacks, such as false data injection and selective reporting, without easily being detected. Overall, insider attacks constitute the main security challenge in wireless sensor networks; that is why all of this research focusing this direction, which will be demonstrated in the following Chapters.

External attacks: This attack is defined as the attack performed by a node that does not belong to the network. Obviously, the attacker node does not have any internal information about the network such as cryptographic information.

Passive attacks: The attack does not have any direct effect on the network as it is outside the network. Passive attacks are in the nature of eavesdropping, or monitoring of packets exchanged within a WSNs when the communication takes place over a wireless channel. This type of attack does not create any interruption in communication process. An attacker can inject useless packets to drain the receiver's battery, or it can capture and physically destroy nodes. Usually authentication and encryption techniques prevent such attackers from gaining any special access to the network.

Active attacks: This type of attack involves disruption of the normal activity of the network. It can do information interruption, modification, traffic analysis, and traffic monitoring [13]. Active attacks are jamming, impersonating, and denial of servicing and message

replay. Attack based on attacker's strength Attack based on attacker's strength ased on attacker's strength: Attackers may use different types of devices to attack the targeted network; these devices have different computation power, radio antenna and other capabilities. Two common categories have been identified by Karlof and Wagner [19] including laptop-class and mote-class attackers.

Laptop class: To launch an attack, attackers may have access to powerful devices such as faster CPU, larger battery power, bigger memory space, high-power radio transmitter or a sensitive antenna. This hardware device allows a more broad range of attacks which are more difficult to stop. Their goal may be to run some malicious code and seek to steal secrets from the sensor network or disrupt network normal functions. For example, Harting ET. Al. demonstrated how to extract cryptographic keys from a sensor node using a JTAG programmer interface in a matter of seconds [14].

Mote-class: Attackers have accessed one or more sensor nodes with the same or similar capabilities like the sensor node deployed in the network. They may try to jam a radio link, but only in the sensor node's immediate vicinity. However, these attacks are more limited since the attackers try to exploit the network's vulnerabilities using only the sensor's node capabilities.

Operational environment: in most WSNs the operation Operational environment: al environment is always assumed to be unattended or even hostile. Since sensor nodes are usually not assumed to be physically protected by some tamper resistant hardware, an adversary is able to physically attack and compromise the nodes. The attackers are not only capable of physically damaging the device, but they can also alter device characteristics and security mechanisms to send out data readings of their choice. Once a WSN is in control, the attackers can do whatever attackers wanted to the node, such as altering the node to listen to information about the network, inputting malicious data or performing a variety of attacks. The above vulnerability can be enhanced by the absence of any fixed infrastructure. In particular, there is no central controller to monitor the operation of a network and identify attack attempts. Thus, even if security mechanisms are deployed, an adversary is able to participate in a network since it has access to all data, such as, cryptographic keys stored on the node can be obtained. Thus, security protocols should be able to operate when the sensor nodes are compromised, which prevents cooperating nodes from taking corrective measures against their corrupt neighbors so that they continue to rely on the fake information being fed to them.

Unreliable Communication: the WSN network has more security issues. The wireless network is in open form so many interrupt comes in this category. Sometime the data can be destroying. Various types of attack are present in the WSN network .The attackers increase the consumption of energy and the security system break by affecting the information of the nodes. Moreover, the unreliable transmission in wireless channel may result in damaged packets. If packets meet with others in the middle of transfer, conflicts will occur and the transfer itself will fail. Such a weakness can be exploited by an attacker, with a strong transmitter, who can easily produce interference or jamming of the network. In addition, wireless multi-hop communication can introduce great latency in a network, which makes it difficult to achieve synchronization among sensor nodes. Compromised nodes may be part of a route, enabling them to modify forwarded messages

II. LIERATURE REVIEW

Z. Luo et al. [1] provided a new technique for the intruder can ruin on sensors. It may be perform both theoretically and practically on a system version. The basic element of intrusion detection hassle is consistent with the speed of the intruder. The program is firstly derive for this we use disc model. A single and multiple sensing detection elements is also used for the detection model purpose. Some interesting elements in intrusion detection, along with transmission duration, sampling length, and the random entrance time of the intruder also are taken into consideration.

P. R. Vamsi et al. [2] provided the usage of TMS at node degree and IDS at base station for the WSN network. Each node is behaves as like its neighbour mode which includes the cluster node as well as the record and reporting to the base station. The base station analyze all records for the use of IDS. In this a model is designed which can be detected and isolate the malicious nodes from the other technique. Simulation consequences show the effectiveness of this version.

Ajith Abraham et al. [3] provided the improvement of an IDP intrusion detection program. For this the three techniques were used which are the classification of genetic algorithm. The design of IDP can be done by the Linear Genetic Programming (LGP), Multi-Expression Programming (MEP) and Gene Expression Programming (GEP). Without these three techniques the IDP cannot work properly therefore the genetic algorithm play important role for developing the programming.

Ioannis Krontiris et al. [4] defining the problem in the intrusion system and find the solution of all worst condition. Based on those situations we increase a time-honored algorithm for intrusion detection and gift simulations and experiments which show the effectiveness of our method.

Djallel Eddine Boubiche et al. [5] A new approach provided for the intruder detection system. The scheme is based on the cross layer interaction across the network and other important layers. Many of difficulties removed by the cross layer interaction technique in the IDS. We have experimentally evaluated our gadget using the NS simulator to illustrate its effectiveness in detecting one-of-a-kind forms of assaults at a couple of layers of the OSI model.

Shio Kumar Singh et al. [6] provided the efficient MAC cope with tracking system which is avoided in the previous technique. So the new methodology developed in the intruder detection system for the cluster based WSN.

A. Anbumozhi et al. [7] used EKF method for the false information in the network. The main component which is used in the method is sensor. It can be control temperature, humidity, voltage. The sensor can analyze the false information and then EKF programming is applied. It shows

the behaviour of close nodes and are expecting their future states. Using different aggregation features (average, sum, max, and min), theoretical threshold price is calculated

Joseph Rish Simenthy et al. [8] provided the hybrid intrusion detection system (HIDS). The HIDS system is the combination of cross layer and the EPIDS (Energy Prediction based totally Intrusion Detection System) gives the maximum possible protection from the intrusion system. It is used for the large WSN. Also by combining these two techniques a huge WSN additionally provides the good flexibleness for the WSN system.

M. Riecker et al. [9] used advanced 3 decentralize light weight that will perform without the delay of the sensor node. This method calculates the attacks from the real data set. Then these results are compared to the other centralized schemes.

J. H. Cho et al. [10] an advanced model is used for the intrusion detection scheme and statically methods also used for the calculation process. The result is that sensitive false alarm with the appreciate to the minimum consider threshold beneath which a node is considered malicious. Our consequences display that there exists an best consider threshold for minimizing fake positives and fake negatives

G. S. Brar et al. [11] proposed a directional transmission-based energy aware routing protocol named PDORP to keep power intake. The proposed protocol PDORP has the traits of each strength efficient gathering sensor information machine and DSR routing protocols. In addition, hybridization of genetic algorithm and bacterial foraging optimization is carried out to proposed routing protocol to become aware of strength green most appropriate paths. The overall performance evaluation, assessment thru a hybridization approach of the proposed routing protocol, gives better end result comprising less bit error rate, less put off, much less strength consumption, and higher throughput, which ends up in better QoS and extend the life of the community.

L. Coppolino et al. [12] provided scheme for the wi-fi networks. The scheme is light weighted. The main agent is central agent which perform accurate intrusion detection by use of record meaning technique and a number of Local Agents going for walks lighter anomaly-based detection strategies at the nodes. The rules are applied to the central agents and the behaviour will be analysed .

R. Bhargavi et al. [13] used complex event processing (CEP) for the wireless sensor network. In the CEP the data can be process in discipline and selected the patterns of the interest from a couple of streams of activities. CEP is utilized in development of packages which must deal with voluminous streams of incoming information with the mission of finding significant activities or styles of activities, and respond to the occasions of hobby in real time

Harmandeep Kaur et al. [14] provided the method for removal of a black hole attack in MANNET. The algorithm is provided is generally provided the detection process for the network. A wi-fi system is used for the PC community that uses wireless statistics connections for connecting network nodes.

Anurag Singh Tomar et al. [15] genetic algorithm optimization is provided for the detection of attacks in WSN network. It is a highly efficient method because it can remove the black hole attack. They can manipulate the sensor interest and black hollow attack can be minimizing by the approaches. As we're using multiple Base Station (BS) for sending the equal data so it calls for added electricity to send the information so in destiny we are able to appearance to lower the energy intake of the sensor nodes.
Sowmya K.S et al. [16] as provided earlier the black hollow attack can be detect and remove by the algorithm in the MANNET system. In MANNET system the safety is the major feature for the network. With the increase in use of MANETS, safety has turn out to be a vital requirement to provide blanketed communication among cell nodes. MANETs are at risk of diverse assaults. It may be used as a denial-of-issuer attack wherein it can drop the packets later.

Manvi Arya et al. [17] proposed a good technique that uses a couple of base stations to be deployed every which manner within the network to counter the impact of black holes on data transmission. Our simulation consequences show that our method will advantage further than 99 packet transport fulfilments victimization one or base stations and moreover, the achievement charge can increase with three or larger base stations even though there is increase within the radius of the black hole region. Results confirmed that our approach could be very effective in lowering the effect of location nodes at the prevailing delivery charge of facts packets and, therefore decreasing the failure percent to a large quantity.

Yash Pal Singh et al. [18] A survey is done on the various technique that are used in the ad-hoc network of the WSN. In a black hollow attack a malicious node answers every path request with a pretend reply claiming to own the shortest and most up to date direction to the vacation spot. All the security feature are the major concern for the WSN system. So the comparison done among all of these. Manet rectangular measure very in chance of Attack resulting from their dynamically ever-changing topology, absence of historical safety infrastructure and open medium of spoken communication, that in contrast to their stressed opposite numbers cannot be at ease, stingy or malicious nodes may additionally do supposed packet dropping misbehaving..

Kiran Narang et al.[19] used the fuzzy logic rules for the WSN security concern. In MANNET the information is in dynamic form so it is a dynamic community therefore mobile nodes are available here. . The fuzzy commonplace enjoy is carried out on packet loss and facts fee at time of node communication. Now on this it will ship the packet from surrounding nodes. This algorithm will offer the better result.

Rajani Narayan et al.[20] PSO method is used for the detection of attack of the WSN system. The optimization is done after that all the minimize result used to avoid the dangerous attack of the WSN. a completely unique approach for transactional protection with chaos primarily based AES cryptography .The lifetime of the WSN system can be increased by the use of PSO optimization algorithm.

Binitha S et al. [21] provided the biologically stimulated optimization algorithm like EA and SI algorithm. They obtained a complex calculation. . It can be very drastic and has been performed to immoderate optimization troubles in laptop networks, control structures, bioinformatics, information mining, exercise concept, tune, biometrics, power systems, picture processing..

Jaspreet kaur et al. [22] proposed BHDP (Black Hole Detection and prevention the use of fuzzy excellent judgment algorithm) that used detects and stops the black hollow assault in WSN. The advantage is set of regulations is that it does no longer make any amendment to the packet. Hence the two base station is used for the detection process of black hollow. The parameters are packet delivery ratio, overall packet drop, routing overhead, theoretical packet used on this black hole assault efficiently at the Wi-Fi sensor community.

Satyajayant Misra et al. [23] BAMB approach is used for the WSN system. It is very costly and effective approach of the network. The simulation results effects shows the 99 packet shipping the nodes. It is based on the base station at duration of community and provide copy to the other base station. It is truly powerful and desires little or no computation and message exchanges at periods the network, therefore saving the strength of the SNs.

C.V. Anchugam et al. [24] proposed to stumble on the assault by way of using detection machine that makes use of FIS for routing protocol. FIS offers a natural way of representing and reasoning the troubles with uncertainty and imprecision. As the assessment cease end result suggests that the proposed gadget is acting better than cutting-edge routing set of rules in case of packet supply ratio, via positioned, surrender-to-quit put off so we are able to say that fuzzy commonplace feel does solves the hassle of malicious node inside the community and eventually increases the overall normal performance of the community.

Savita Shiwani et al. [25] used fuzzy logic approaches for the different types of attacks. The black hole attack is the main problem for the WSN system. this attack disrupt the general overall performance of Edouard Manet and what is greater studied of the effect of area attacks in Edouard Manet the utilization of every reactive and proactive protocols and to in shape the vulnerability of every the ones protocols in competition to assault. After, states of the nodes in addition are frequently used by the routing protocol to skip the ones malicious nodes. Our method suggests that in an incredibly dynamically converting community, this approach will come upon most of the malicious nodes with a reasonably excessive extremely good charge. The packet transport rate a few of the Edouard Manet additionally could also be extended thus

Naveen Kumar et al. [26] furnished a fuzzy primarily based definitely choice to test a node is infected via Black hollow attack or node. The proposed gadget will pick out the attack over the node further to offer the answer to reduce the records loss over the community. A Wireless community is a dynamic community with massive no. of nodes. As the traffic increases over the network such form of network suffers from the troubles like congestion and packet loss. The packet loss is appropriate up to three threshold rate but as there can be more packet loss we need a few solutions for this. The equal solution is supplied in this paper. Here we're imparting a fuzzy based choice to test a node is inflamed thru the use of Black hollow assault or node.

III. ANALYSIS

The study of above papers many techniques are used for the improvement of WSN network using the optimization theory. In the first paper the basic of MANET is explained. The A single and multiple sensing detection elements is also used for the detection model purpose. In the next one the usage of TMS at node degree and IDS at base station for the WSN network. Each node is behaves as like its neighbor mode which includes the cluster node as well as the record and reporting to the base station. The design of IDP can be done by the Linear Genetic Programming (LGP), Multi-Expression Programming (MEP) and Gene Expression Programming (GEP). We have experimentally evaluated our gadget using the NS simulator to illustrate its effectiveness in detecting one-of-a-kind forms of assaults at a couple of layers of the OSI model. The sensor can analyze the false information and then EKF programming is applied. It shows the behavior of close nodes and are expecting their future states. the hybrid intrusion detection system (HIDS). The HIDS system is the combination of cross layer and the EPIDS (Energy Prediction based totally Intrusion Detection System) gives the maximum possible protection from the intrusion system. The fuzzy commonplace enjoy is carried out on packet loss and facts fee at time of node communication. the biologically stimulated optimization algorithm like EA and SI algorithm. They obtained a complex calculation. BHDP (Black Hole Detection and prevention the use of fuzzy excellent judgment algorithm) that used detects and stops the black hollow assault in WSN. The efficient results are obtained by using the various techniques for the energy loss minimization.

IV. CONCLUSION

The present scenario is basically depend on the MANET based system. There are many attacks comes in the MANET system. These attacks can be detected and repaired by the various techniques. These techniques are based on the optimization and many other software. We can implement the new GWO tuned for the energy consumption minimization. The fuzzy logic concept will be considered and find the compatible results. The MANET system efficiency will be increased.

REFRENCES

[1] Q. Yu, Z. Luo and P. Min, "Intrusion detection in wireless sensor networks for destructive intruders," 2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), Hong Kong, 2015, pp. 68-75.

[2] P. R. Vamsi and K. Kant, "Secure data aggregation and intrusion detection in wireless sensor networks," 2015 International Conference on Signal Processing and Communication (ICSC), Noida, 2015, pp. 127-131.

[3] Ajith Abraham, Crina Grosan and Carlos Martin-Vide, "Evolutionary Design of Intrusion Detection Programs," International Journal of Network Security, Vol.4, No.3, PP.328–339, Mar. 2007.

[4] Ioannis Krontiris, Zinaida Benenson, Thanassis Giannetsos, Felix C. Freiling and Tassos Dimitriou, "Cooperative Intrusion Detection in Wireless Sensor Networks.
[5] Djallel Eddine Boubiche and Azeddine Bilami, "CROSS LAYER INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORK," International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.
[6] Shio Kumar Singh, M P Singh and D K Singh, "Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks," International Journal of Advanced Science and Technology, Vol.30, May, 2011.
[7] A. Anbumozhi, K.Muneeswaran, Sivakasi, "Detection of Intruders in Wireless Sensor Networks Using Anomaly," International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014.
[8] Joseph Rish Simenthy CEng , AMIE, K. Vijayan, "Advanced Intrusion Detection System for Wireless," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, an ISO 3297: 2007 Certified Organization Vol. 3, Special Issue 3, April 2014.
[9] M. Riecker, A. Barroso, M. Hollick and S. Biedermann, "On Data-Centric Intrusion Detection in Wireless Sensor Networks," 2012 IEEE International Conference on Green Computing and Communications, Besancon, 2012, pp. 325-334.
[10] F. Bao, I. R. Chen, M. Chang and J. H. Cho, "Trust-Based Intrusion Detection in Wireless Sensor Networks," 2011 IEEE International Conference on Communications (ICC), Kyoto, 2011, pp. 1-6.
[11] G. S. Brar, S. Rani, V. Chopra, R. Malhotra, H. Song and S. H. Ahmed, "Energy Efficient Direction-Based PDORP Routing Protocol for WSN," in IEEE Access, vol. 4, no. , pp. 3182-3194, 2016.
[12] L. Coppolino, S. DAntonio, A. Garofalo and L. Romano, "Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks," 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Compiegne, 2013, pp. 247-254.
[13] R. Bhargavi, V. Vaidehi, P. T. V. Bhuvaneswari, P. Balamuralidhar and M. G. Chandra, "Complex Event Processing for object tracking and intrusion detection in Wireless Sensor Networks," 2010 11th International Conference on Control Automation Robotics & Vision, Singapore, 2010, pp. 848-853.
[14] Harmandeep Kaur, "A Novel Approach To Prevent Black Hole Attack In Wireless Sensor Network"International Journal For Advance Research In Engineering And Technology, Vol. 2, Issue VI, June 2014.
[15] Anurag Singh Tomar, "Optimized Positioning Of Multiple Base Station for Black Hole Attack" International Journal of Advanced Research in Computer Engineering & Technology Volume 3 Issue 8, August 2014.
[16] Sowmya K.S, "Detection and Prevention of Blackhole Attack in MANET Using ACO" International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012.
[17] Manvi Arya, "BFO Based Optimized Positioning for Black Hole Attack Mitigation inWSN" International Journal of Engineering Trends and Technology (IJETT) – Volume 14 Number 1 – Aug 2014.
[18] Yash Pal Singh, "A Survey on Detection and Prevention of Black Hole Attack in AODV- based MANETs" journal of information, knowledge and research in computer engineering, nov12 to oct13 ,volume – 02, issue – 02.
[19] Kiran Narang, "Black Hole Attack Detection using Fuzzy Logic" International Journal of Science and Research, Volume 2 Issue 8, August 2013.
[20] Rajani Narayan, "Self-optimization and Self-Protection in AODV Based Wireless Sensor Network" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 244-254.
[21] Binitha S, "A Survey of Bio inspired Optimization Algorithms" International Journal of Soft Computing and Engineering ISSN: 2231-2307, Volume-2, Issue-2, and May 2012.

Table 1 Literature Review

S.No.	Technique	Author	Advantage	Limitation
1	Disc model for utilization	Z. Luo et al.	Improve the security concern	NA
2	Wireless Sensor Networks (WSNs) the usage of TMS at node degree and IDS at Base Station (BS) aspect	P. R. Vamsi et al.	Simulation results are very effective	Perform community activity
3	Linear Genetic Programming (LGP), Multi-Expression Programming (MEP) and Gene Expression Programming (GEP)	Ajith Abraham et al.	light weight and accurate	NA
4	Intrusion Detection System de-signed for wireless sensor	Ioannis Krontiris et al.	Provide Mint Route protocol of TinyOS	attack in TinyOS
5	cross layer interaction IDS	Djallel Eddine Boubiche et al.	Detecting one-of-a-kind forms of assaults at a couple of layers of the OSI model.	NA
6	MAC address based intruder tracking	Shio Kumar Singh et al.	providing security mechanisms in the network	NA
7	EKF	A. Anbumozhi et al.	theoretical threshold price is calculated	Neighbor sensor required

8	Energy Prediction based totally Intrusion Detection System (EPIDS) as well as the Cross layer Detection System	Joseph Rish Simenthy et al.	provide a huge range of flexibleness	Combined effort required
9	light-weight information anomaly detection mechanisms	M. Riecker et al.	Improve security feature	brought plausible attacks
10	stochastic Petri nets for performance evaluation	J. H. Cho et al.	Threshold for minimizing fake positives and fake negatives.	NA
11	proposed protocol PDORP, DSR protocol	G. S. Brar et al.	much less strength consumption, and higher throughput	NA
12	IDS uses each misuse-primarily based and anomaly-based totally detection techniques	L. Coppolino et al.	Effectiveness through security concern	Central Agent and their behaviour has been analysed in selected attacks situations
13	CEP (Complex Event Processing)	R. Bhargavi et al.	It can be find significance and styles of activity	ESPER, an open source Complex Event Processing engine is used to expand the software
14	Wi-Fi network	Harmandeep Kaur et al	prevent black hole attack in MANET	NA
15	Genetic algorithm	Anurag Singh Tomar et al.	manipulation of sensor interest	Black hollow attack
16	exceptional nodes within the community of the incident	Sowmya K.S et al.	Prevent black hole attack in Mannet	risk of diverse assaults
17	couple of base stations to be deployed	Manvi Arya et al.	99 packet transport fullfilments victimization one or base stations	NA
18	Survey of ad-hoc network	Yash Pal Singh et al	Black hollow attack removed	absence of historical safety infrastructure
19	Fuzzy rules	Kiran Narang et al	Remove packet loss completely	NA
20	PSO	Rajani Narayan et al.	Stop to end transport ratio and network lifetime.	AES cryptography
21	biologically stimulated optimization EA and SI algorithms	Binitha S et al.	These are very efficient	NA