# IMPROVING SECURITY AND DETECTING BLACK HOLE ATTACK IN WIRELESS SENSOR NETWORK

[1]Y. PAVAN KUMAR GUPTHA [2] M. MADHU

[1]Assistant Professor, CSE, Sri Indu College of Engineering and Technology, Recognized by UGC, NBA Accredited and Affiliated to JNTUH.

[1]Assistant Professor, CSE, Sri Indu College of Engineering and Technology, Recognized by UGC, NBA Accredited and Affiliated to JNTUH.

Mail: ypavanguptha@gmail.com, Contact: 9492673656

Mail: madhualmpr@gmail.com, Contact: 7995384909

**ABSTRACT:**

***A Wireless sensor Network (WSN) includes a wide range of application, slowly changing into an integral a part of the living life. Wireless means that the node will communicate without any physical media, i.e., the info is transmitted from one node to a different within the sort of packet. WSN is being deployed for several real time applications wherever the dynamical watching of detected information is needed. Sensor networks are application-specific and also the routing of information between the device nodes needs to be while not interruption and errorless. Routing protocols attempt to incorporate ways to ensure turning away of misbehavior of intermediate nodes. The trust among the distributed network is mostly used as a powerful tool to enhance the performance of device networks. In this paper presents an in depth analysis on the security and trust communication between the device nodes with routing techniques to discover and prevent information packet from the being exposed to black hole attack. The paper additionally concludes with a comparison among the present works.***

## 1. INTRODUCTION

Wireless sensor networks (WSNs) have attracted a good range of disciplines sensor node interactions with the physical world are essential. Wireless network consisting of spatially distributed autonomous devices exploitation sensor to monitor the physical or environmental conditions. The sensor network consists sensor node, i.e. small, light-weight and transportable. The most task of WSN is to sense and collect data, method and transmit in to the sink. WSN application and communication are primarily providing the high energy efficient. Wireless communication paradigm makes WSNs an important part of our daily lives; WSNs are composed of individual embedded system that's capable of interacting with their surroundings through varied sensors, processing data regionally and communication this with their neighbors. WSN application are space, health care and pollution observation, environmental/earth sensing, forest fire

detection, landslide detection, knowledge work then on. Routing is that the method of choosing the most effective ways in a network. Router performs the traffic direction operate on the web. A router has 2 stage of operation they're control plane and forwarding plane. Up to the mark plane, a router maintain a routing table list a route ought to be used to forward an information packet and through physical interface connection. In forwarding plane, a route forward information packet between incoming and outgoing interface association. The routing techniques are classified into 3 classes they are flat, hierarchal and placement based mostly routing. Router may give property among and between enterprises and the web or between web service suppliers (ISP) networks. The foremost powerful routers are sometimes found in ISPs. Routing is performed for several forms of networks including the general public switched telephone network (circuit switching), electronic information networks and transportation networks. Trust on the behavior of the component of the network is key facet of WSN. Trust management system for WSN could be very helpful for detection misbehaving nodes and for aiding the choice creating method. Trust is an important issue of social and computing network environment. The success of trust is betting on the adopting of the proper approach for trust management system of WSN. Trust management system is often classified into 2 categories: credential-based trust management system and behavior-based trust management system. Trust management improves the safety of WSN.

## 2. RELATED WORK

Yuxin Liu et al. have given the trust technique for WSN. This technique avoids black holes by keeping track of their variety and obtains a trust model. Therefore the strategy improves the information route security. Active Trust will significantly improve the information route success likelihood and ability against region attacks and may optimize network lifetime. The Active Trust scheme is that the 1st routing scheme that uses active detection routing to handle black hole Attack. The recommended routing protocol has higher energy efficiency and security performance. Active Trust scheme designs the Active detection routing protocol that may be to identify the attack behavior and so mark the region location and information routing protocol refers to the method of nodal information routing to the sink. It selects a node with high trust for ensuing hop to avoid black holes and improve the success ratio of reaching the sink. Active Trust has the high successful routing probability, security and measurability and high energy efficiency. R. K. Bar et al. have recommended the trust based mostly AODV routing protocol by exclusion of region Attack. In the AODV routing protocol a path is chosen in such a way that a lot of sure nodes are concerned. A Trust price for each node is calculated depending upon the packet forwarding ability and weight issue of the node. A rank is generated supported this trust value. Weight issue is defined as the ratio of variety of RREP set to the quantity of RREQ received by the node. Trust price is inserted within the routing table and also the route discovery is completed in step with this trust value by avoiding a less sure node. Depending upon the trust price and also the threshold value the region node is known and it's excluded from the route institution method. It avoid the low trusted nodes, the typical packet loss of the network is additionally decreased considerably. Therefore the standard of service of the network is increased in terms of packet

loss. Satyajayant Misra et al. have conferred BAMBi technique to effectively mitigate the adverse effects of black hole attacks on WSNs. region attacks occur once an adversary captures and re-programs a collection of nodes within the network to drop the packets. BAMBi is predicated on the deployment of multiple base stations within the network and routing of copies of information packets to those base stations and the solution is extremely effective and needs little computation and message exchanges within the network, thus saving the energy of the SNs. this system can do more than ninety nine packet delivery success and prove that the scheme will determine 100% of the region nodes. Praveen K S et al. have compared AODV and OLSR routing protocols for analyzing the region Attack in ad hoc network. Here, the authors have shown that the offender node waits for the neighboring node to initiate the RREQ (route request) packet. The attacker gets the request, and sends the faux reply packet RREP (route reply) with a replacement sequences variety. Therefore the attacker takes control of the routing path and thereby reduces the throughput. Throughput is that the total variety of packets sent successfully from sender to receiver in an exceedingly nominal time. Throughput therefore computed is used because the metrics to detect presence of attacks. OLSR is an optimized routing protocol for Mobile Ad hoc Network as a result of messages are compacted and reduces the quantity of retransmission to flood these messages. OLSR could be a table driven, proactive link state protocol. Every node calculates the simplest next hop for alternative nodes and MPR (Multi purpose Relays) that are subsets of neighboring nodes. The most plan of MPR is reduce the flooding of broadcast messages within the network by minimizing duplicate retransmission messages. OLSR without region attack has most throughputs. AODV uses Client-server methodology that's Request-reply methodology for finding a sound path between sources to destination. AODV is one among the on demand and typical routing protocol, higher the throughput higher the performance by using AODV protocol has higher throughput because the packets are sent quick and overhead can is avoided because of the avoidance of black hole attack. The comparison shows that AODV outturn is better than OLSR protocol as a result of all the nodes ought to update the destination within the table whenever the trail is made. R. Kompella et al., present an easy and effective methodology to discover and diagnose the silent failures, i.e. information packets are silently born within the network without giving any responses. This methodology uses active measurement between edge routers to boost alarms whenever end property is disrupted. During this tier-I ISP network with success discover and localize the black holes. The authors specialize in detection and localization of silent faults arising from the interaction between MPLS and IP layers of backbone networks. Mistreatment real failure knowledge obtained from a tier-1 network's IPFM and MPFM systems, demonstrated that each systems will effectively aid network operators in troubleshooting failures. D. He et al., have planned the ReTrust (Attack-Resistant and light-weight Trust) for wireless MSD (Medical sensor Networks). The authors have known the security and performance challenges facing a sensor network for wireless medical observance and recommend the two-tier design, supported the design develop the ReTrust. ReTrust not solely will with efficiency discover malicious behaviors; however can even considerably improve the network performance. ReTrust work

with 2 topologies intracell and intercell topology. ReTrust is possible for enhancing the security and network performance of real MSN applications. T. Shu et al., have developed the mechanisms that generate randomized multipath routes to attenuate the end-to-end energy consumption below given security constraints. Multiple methods are computed during a randomized way to sent data packet, routes taken by varied shares of various packets keep dynamic over time. The authors are specifically interested in combating 2 varieties of attacks: compromised node (CN) and denial of service (DOS) .In the CN attack, a set of nodes to listen information. Within the DoS attack, the conventional operation of the network is ensured by actively disrupting, changing, or even paralyzing the practicality of a set of nodes. The algorithms are often applied to selective packets in WSNs to provide further security levels against adversaries attempting to acquire these packets.

## 3. FRAMEWORK

**3.1 Network Model:** (a) We consider a wireless sensor network consisting of sensor nodes that are uniformly and at random scattered during a circular network. The network radius is R, with nodal density ρ, and nodes don't move when being deploy. Upon detection of an occurrence, a sensor node can generate messages, and those messages should be sent to the sink node. (b) We tend to consider that link-level security has been established through a typical cryptography-based protocol. Thus, we tend to consider a link key to be safe unless the soul physically compromises either aspect of the link.

### 3.2 The Adversaries' Model

We consider that black holes are shaped by the compromised nodes and can unselectively discard all packets passed by to stop information from being sent to the sink. The adversary has the flexibility to compromise a number of the nodes. However, we tend to consider the soul to be unable to compromise the sink and its neighboring nodes.

### 3.3 Energy Consumption Model and Connected Definitions

According to the standard energy consumption model, represents energy consumption for transmission, and represents energy consumption for receiving. $E_{elec}$ represents the transmission circuit loss. Each the free space (d2 power loss) and therefore the multi-path fading (d4 power loss) channel models are utilized in the model counting on the gap between the transmitter and receiver.

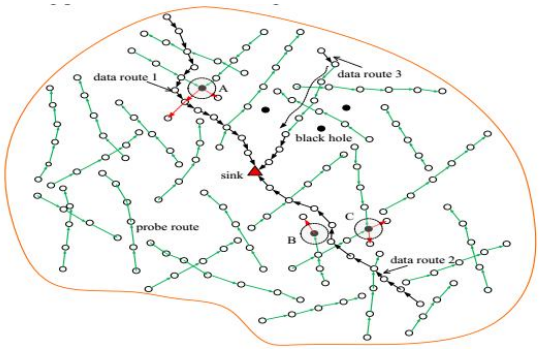


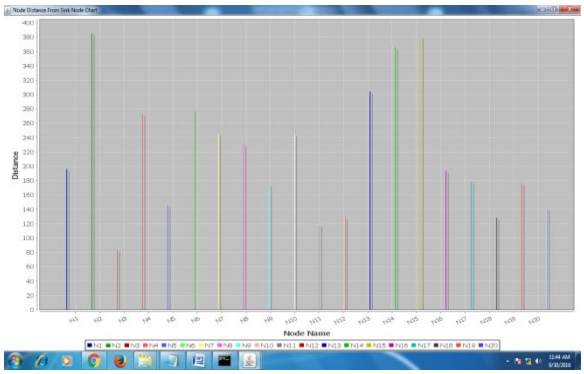

**Fig1: Illustration of the Active Trust scheme**

Overview of the proposed theme an overview of the trust theme that consists of an active detection routing protocol and information routing protocol; is shown in figure; Active detection routing protocol is A detection route refers to a route while not information packets whose goal is to convert the adversary to launch associate attack therefore the system will determine the attack behavior and so mark the part location. So, the system will lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Through active

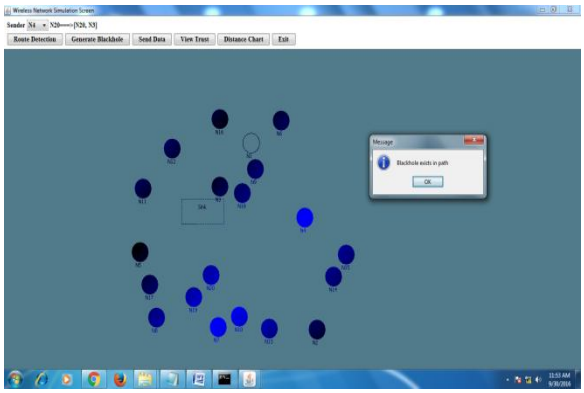
detection routing, nodal trust will be quickly obtained, and it can effectively guide the information route in selecting nodes with high trust to avoid black holes. The active detection routing protocol is shown via the inexperienced arrow in Fig. 1. During this theme, the source node at random selects an unobserved neighbor node to create an energetic detection route. Considering that the high detection route length is, the detection route decreases its length by one for each hop till the length is decreased to zero, and then the detection route ends. In Data routing protocol information routing refers to the process of nodal information routing to the sink. The routing protocol is similar to common routing protocols in WSNs; the difference is that the route can choose a node with high trust for the next hop to avoid black holes and so improve the success ratio of reaching the sink. The data routing is shown via the black arrow in Fig. 1. The routing protocol will adopt an existing routing protocol, and we take the shortest route protocol as an example. Node a in the route can select the neighbor that's nearer the sink and has high trust because the next hop. If there is not a node among all neighbors nearby the sink that has trust on leading of the default threshold, it'll report back to the higher node that there's no path from a to the sink. The higher node, operating within the same manner, can re-select a special node from among its neighbors nearer the sink till the information is routed to the sink or there's conclusively no path to the sink.

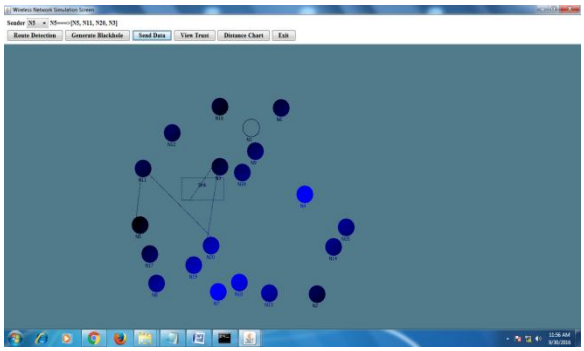
## 4. EXPERIMENTAL RESULTS

Enter the node size (the number of nodes to be created into the network) and select the node energy (the energy assigned for each node initially) then view on simulation. Created network with given number of nodes. In Route detection, then each node in the network establishes a route to the sink node by using intermediate relay nodes, after successfully establishing the routes for all the nodes. Initially the trust level and energy values for all the nodes is 10 and 100 respectively, if any nodes involves in route detection using intermediate nodes then its energy will be consumed. Select some sender node then send the data to the sink node from the selected sender. Here the data will send from N1 to N3 and then N3 to the sink node to view the trust and energy values of all the nodes. Here both N1 and N3 are involved in transmission so their energy values are reduced Click on distance chart, here it wills shows the distance between each node to the sink node:




To generate blackhole to make a node as black hole in the network; in this, N1 has become as a black hole node and the route detection will happens for all the nodes.





Detected routes after the black hole attack. Select some sender node then send data.

## 5. CONCLUSION

The main task of WSN is to sense and collect information, process and transmit to the sink. This paper presents a detailed survey on the trust based mostly routing techniques used for communication between the sensor nodes. One of the major security threats specifically black hole attack has been taken for study and also the techniques incorporated inside the trust based mostly routing to overcome such attacks have additionally been surveyed. The detection of those attacks has shown to improve the secure transmission of packets between the sensor nodes.

## REFERENCES:

1. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency," IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391, 2014.

2. M. Dong, K. Ota, A. Liu, et al. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016.

3. S. He, J. Chen, F. Jiang, et al. "Energy provisioning in wireless rechargeable sensor networks," IEEE transactions on mobile computing, vol. 12, no. 10, pp. 1931-1942, 2013.

4. X. Liu, M. Dong, K. Ota, P. Hung, A. Liu. "Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory," IEEE Transactions on Services Computing, vol. 9, no. 2, pp. 186-198, 2016.

5. C. Zhu, H. Nicanfar, V. C. M. Leung, et al. "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.

6. A. Liu, M. Dong, K. Ota, et al. "PHACK : An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs," Sensors, vol. 15, no. 12, pp. 30942-30963, 2015.

7. A. Liu, X. Jin, G. Cui, Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," Information Sciences, vol. 230, pp.197-226, 2013.

8. Z. Zheng, A. Liu, L. Cai, et al. "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks," IEEE Transactions on Mobile Computing.vol. 15, no. 5, pp. 1130-1143, 2016.

9. T. Shu, M. Krunz, S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941-954, 2010.

10. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.