Energy Efficiency in wireless sensor Networks

Harpreet Singh Bedi, Manoj Sindhwani*

School of Electronics and Electrical Engineering

Lovely Professional University, Phagwara, Punjab

Abstract

Wireless network invoke for the networks through which the communication between devices is implemented without use of wires In black hole attack, attacker publicize itself as a node which have shortest path to destination node from sender and when attacker or malicious node receives the packet, it decides whether to packet or drop it. The black hole attack reduces the performance of network. Literature review shows that with time lots of changes have been proposed in AODV and DSR for prevention of attacks. In our proposed algorithm we use cluster head concept which is used for communication. The node selected as cluster head which has highest node value means highest battery power, buffer length, serve time etc. In this algorithm we use the concept of distance time value, packet drop value which helps further to boost PDR and throughput of the network. It uses the least energy for communication.

Introduction

Wireless network invoke for the type of connections through which the communication through devices is implemented without use of wires. Radio wave and microwaves are used for communication in the wireless network and it eliminates the cost of wires. It is necessary that, both devices/mobile nodes that are communicating to each other, they remain within the radio range of each other. The IEEE standard 802.11 [1][2] is used for wireless network. Wireless networks have many characteristics like easy setup, mobility, productivity, security and economic and cost saving installation.

First type called Infrastructure network has center administrator which is known as Access Point (AP). All the wireless devices such as laptops, mobile phones are connected with each other through Access point.

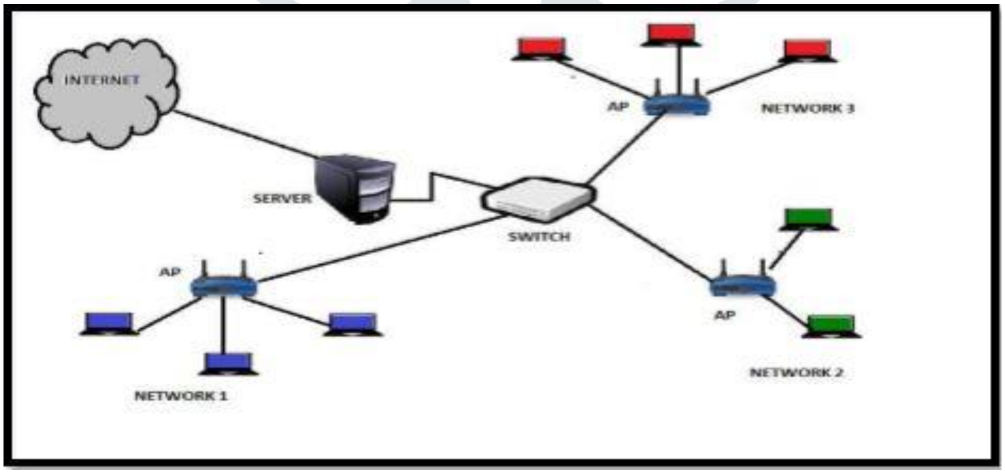

Figure 1.1: Infrastructure network

Access point is also responsible for data routing means if any of the terminal wants to send the data to other terminal, that information is routed through the access points. In infrastructure network, fixed base station is there which is called access points and all wireless devices that are communicating with other are connected with a point. In figure 1.1 shows the three access points are used and wireless devices are connected to that access points and these devices are communicating to each other by using Access point.

Ad hoc networks: [1][2] This network is also known as temporary network, in this type of networks, there is no central coordinator means no Access point. When node is entered in the temporary network for forwarding the data to the destination, and then the decision of the nodes to forwarding the data is made at run time execution is completely based upon the network connectivity. It is a network which is used for emergency purpose. In ad hoc wireless network nodes can direct contact with each other or base station. Figure 1.2 shows the example of ad hoc wireless networks. In this various nodes are communicating with each other directly without any Access points.

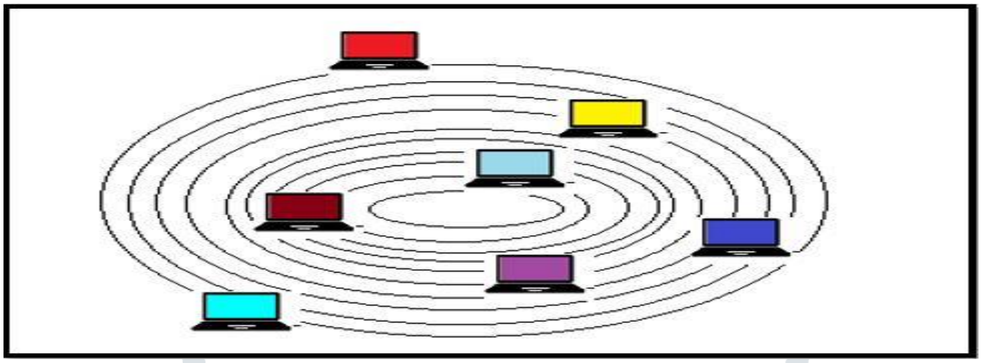

Figure 1.2: Ad-hoc network

MOBILE AD HOC NETWORK (MANET)

In this kind of network, every device actively participates in data forwarding and work like a router. Communication between two nodes performed via radio links.

.

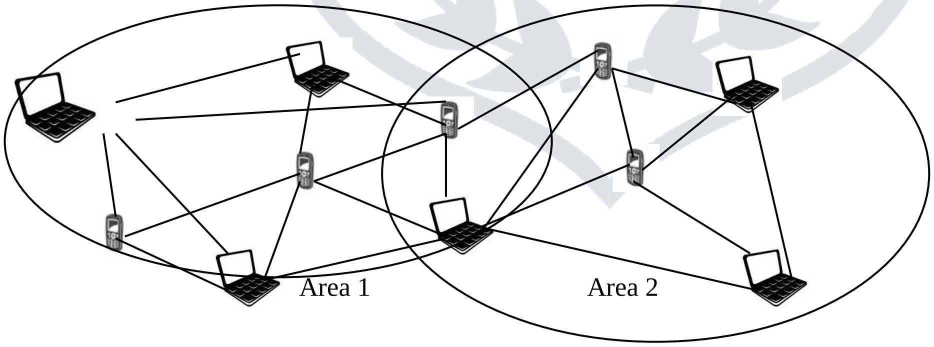

Figure 1.3: Mobile Ad hoc Network

The temporary network is an infrastructure-less kind of network, in which number of nodes are there which can move anywhere in the network. Node in MANET can simply leave or join the network any time. In every year there are tons of researches completed to provide security to black hole attack in MANET. Various solutions are provide by researchers for securing network from malicious node but still security mechanisms are not this much of sufficient only due to MANET challenges and its characteristics. As security increases attackers also become smarter and intelligent they found new ways or technique for doing attack.

In existing technology it detects single black hole attack for which a step verification method is used to detect black hole so attackers start doing attack with the help of each other by using more than two nodes they start doing black hole attack. Problem in this system is there energy usage of mobile nodes and neighbor node is also malicious one and it simply verifies that node is having true path and path is selected which causes black hole attack in the network**.**

Result and Discussions

In the MANET problem of energy efficiency is still there and the security of our data packets is big issue. There are several techniques which are used in detection the black hole attack and to save the energy of network but our algorithm is able to detect the malicious at various levels with the usage of energy efficiency by using clustering model. Ns-2 is used for simulation and it is an IEEE 802.1 standard which is used at data link layer and physical layer. AODV routing protocol is used at network layer and TCP protocol is used at transport layer. Radio propagation and wireless channel is used in an area of 800m * 800m. Constant Bit Rate (CBR) packets are used for transmission.

To check the performance of proposed technique, simulation of AODV in the under black hole attack and under proposed algorithm is done. The parameters for evaluating the performance are throughput, energy and packet delivery ratio (PDR).

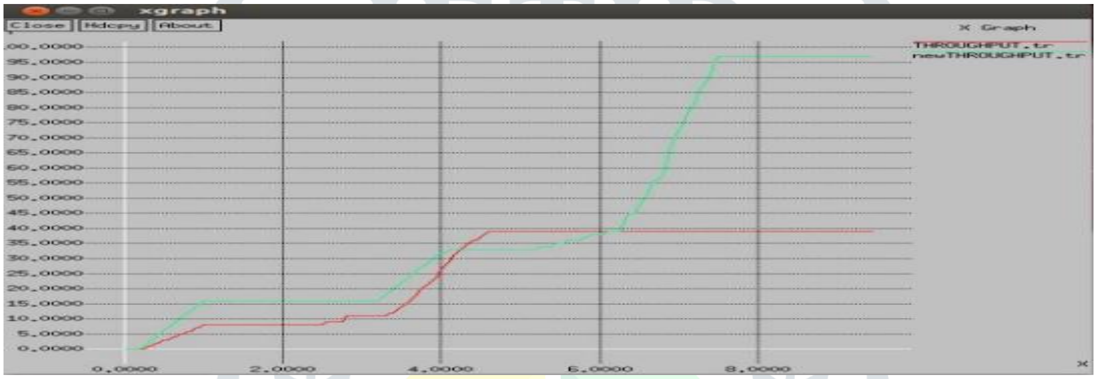

Figure 2.1 - Throughput Comparison

In Fig. 2.1, the Comparison of throughput is done. The simulation of this graph is based on under black hole attack and with proposed method. Throughput means number of successful packets transfer over the communication channel. So from the slope in the graph we can simply compare the obtained throughput value in which red line is under black hole attack and green is proposed method.

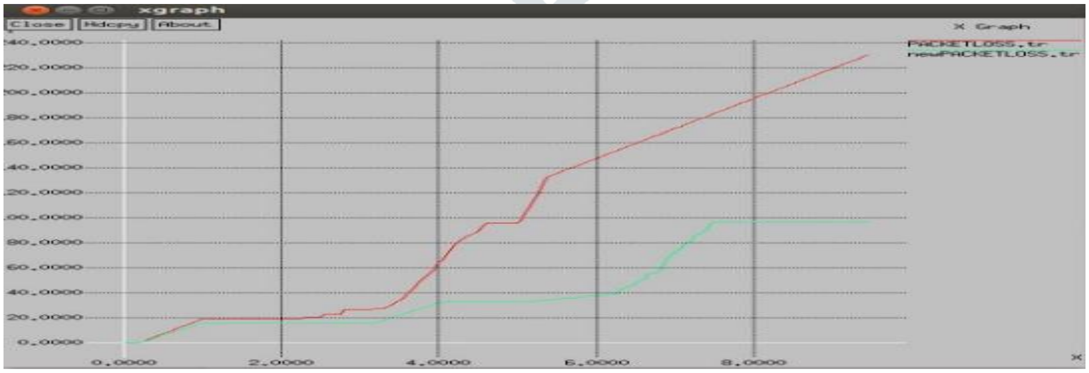

Figure 2.2- Packet loss ration comparison

In Fig. 2.2, Packet loss ration comparison is done between under black hole attack and proposed method. Packet loss ration means, how many packets are loss in one unit time or in one transmission. Red line in the graph shows the under black hole attack and green line show the proposed method packet loss ratio

Conclusion

In black hole attack, attacker publicize itself as a node which have shortest path to destination node from sender and when attacker or malicious node receives the packet, it decides whether to packet or drop it. The black hole attack reduces the performance of network. In the proposed algorithm various terms are used to detect black hole attack from MANET with energy efficiency which means saving the energy of mobile nodes.. In our proposed algorithm we use cluster head concept which is used for communication. The node selected as cluster head which has highest node value means highest battery power, buffer length, serve time etc. In this algorithm we use the concept of distance time value, packet drop value which helps in order to increase the PDR and throughput of the network. It uses the least energy for communication.

References

1. P. Sinha, R. Sivakumar, and V. Bharghavan, “Cedar: Core ex- traction distributed ad hoc routing,” in Proc. of IEEE INFO-COM, 1999.
2. K. Fall and K. Varadhan, “The vint project, ucberkeley,lbl, usc/isi, and xeroxparc,” 1997. [Online]. Available:http://www-mash.cs.berkeley.edu/ns/
3. J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva, “A performance comparison of multi-hop wireless ad hoc net-work routing protocols,” in Proc. of the ACM/IEEE Inter- national Conference on Mobile Computing and Networking (MobiCom98), 1998.
4. S. Jung, N. Hundewale, , and A. Zelikovsky, “Node caching enhancement of reactive ad hoc routing protocols,” in
5. WCNC’05, 2005. Y. Lee and G. Riley, “A workload-based adaptive load- balancing technique for mobile ad hoc networks,” in WCNC’05, 2005