Greyhole and Blackhole Attack Identification and Prevention using IP Backtracking in WSN

Shaiffu
Research Scholar
Department of Computer Science and Engineering
Sri Guru Granth Sahib World University,
Fatehgarh Sahib

Amandeep Kaur Virk
Assistant Professor
Department of Computer Science and Engineering
Sri Guru Granth Sahib World University,
Fatehgarh Sahib

ABSTRACT
The network in which a large number of small and low-cost sensor nodes are randomly deployed is called Wireless Sensor Network(WSN). These sensor nodes can collectively monitor physical and environmental conditions like pressure, temperature, humidity etc. Issues in WSN are Energy Efficiency, Reliability, Production Cost, Security, etc. Security is one of the major concerns in the network. A sensor network must achieve all security goals like availability, freshness, integrity etc. AODV is a reactive routing protocol in which the establishment of the route takes place only when there is demand for new routes. A novel hybrid black/grey hole detection and prevention approach is proposed for detecting and preventing both the black and grey hole attacks in Ad hoc On-demand Distance Vector Routing (AODV) protocol for WSN. In this research work, we will be implementing the AODV routing protocol using WSN. The work presented in this thesis adopted a hybrid trace-back approach in which packet marking and packet logging are integrated. Experimental results show that the proposed hybrid approach detects and eliminates the attacks effectively with better throughput, delay, load and jitter.

Keywords
Wireless Sensor Network, AODV, Grey hole attack, Black hole Attack, IP Backtracking, Packet Marking, Packet Logging.

1. INTRODUCTION
The composition of large number of a sensor nodes, which are deployed in a sensor field is defined as the Wireless Sensor Network(WSN). Sensors are tiny devices in a sensor field which monitor various conditions like temperature, humidity, pressure, etc. and later convert it into an electrical signal. These sensor devices communicate either directly to the Base Station (BS) or among each other. The self-organizing capability of sensor nodes provides several challenges among researchers for designing the network protocols [1].

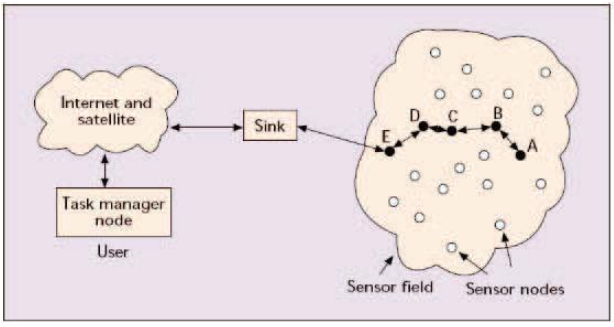

Fig 1: Communication Architecture of WSN [1]

The communication architecture of WSN consists of sensor nodes scattered in a sensor field with each of these nodes capable of collecting and routing data back to sink and to end user.

2. ROUTING PROTOCOLS IN WSN
Routing of packets in WSN is controlled by an ad-hoc routing protocol. Nodes are not aware of the topology of the network in WSN. An ad-hoc routing protocol are classified in reactive protocol, proactive protocol, hybrid protocol.

2.1 Proactive(tabledriven) Routing Protocol
It is a table driven routing protocol. In this protocol, routing information is broadcasted by mobile nodes to the neighbours. Each node need to keep their routing table which contains the information of neighbourhood nodes, reachable nodes and the number of hops. The disadvantage of this protocol is one size of network increases, then overhead increase [2].

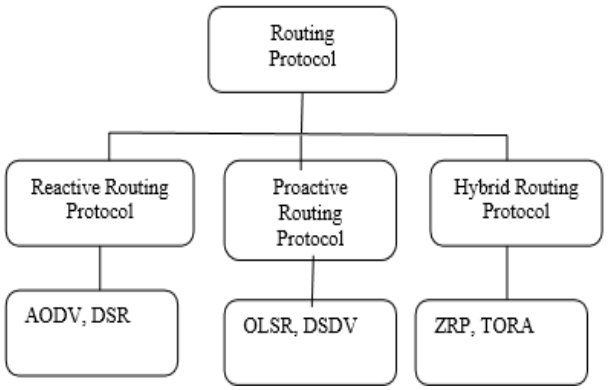

Fig 2: Routing Protocols in WSN [2]

2.1.1 Destination Sequenced Distance Vector (DSDV) Protocol
It is table driven DSDV protocol, which is a modification in the Distributed Bellman-Ford(DBF) Algorithm which was used successfully in many of the dynamic packet switched networks. Every node in mobile network is required to send a sequence number, which is periodically increased by two and it is transmitted along with other routing update messages to all other neighboring nodes [2].

2.2 Reactive(on-demand) Routing Protocol
This type of protocol finds routes by using the route request packet. It is bandwidth efficient on-demand routing protocol. The protocols deal with two functions of Route Discovery and Route Maintenance. One of reactive protocol is AODV [2].

2.2.1 Ad hoc On-demand Distance Vector Routing (AODV) Protocol

AODV is Ad hoc On-demand Distance Vector Routing Protocol. In AODV, route establishment takes place only when there is a demand for new routes. AODV is capable of unicast, broadcast and multicast routing. AODV is able to react quickly to the changes in the network topology and it updates only the hosts that may be affected by the changes in the network by using the RREQ message. The RREQ and RREP messages are responsible for the route discovery [2].

2.3 Hybrid Routing Protocol

It consolidates receptive and proactive directing protocols. The Zone Routing Protocol (ZRP) is a half breed directing protocol that partitions the system into zones [2].

3. ATTACKS IN WSN

3.1 Sybil Attack

Sybil Attack is named after the subject of the book Sybil. The fake identities are known as Sybil nodes. The Sybil nodes can out vote the honest nodes in the system. Usually, peer to peer systems are vulnerable to Sybil attack. The attacker or Nasty Node shows its multi identity. Hence, affect the routing table.

3.2 Wormhole Attack

Wormhole attack is an attack on the routing protocol in which the packets or individual bits of the packets are captured at one location, tunnelled to another location and then replayed at another location [4]. This convinces the neighbour nodes of these two end points that these two distant points at either end of the tunnel are very close to each other. If one endpoint of the tunnel is as near to the base station, the worm hole tunnel can attract a significant amount of data traffic to disrupt the routing and operational functionality of WSN [5].

3.3 Black hole Attack

A black hole is a malicious node that attracts all the traffic in the network by advertising that it has the shortest path in the network. Black hole drops all the packets it receives from the other nodes. In a black hole attack, malicious nodes do not send true control messages [4].

3.4 Grey Hole Attack

In the Grey Hole attack, nasty or malicious node is acting as normal node and drops the message or packets which is passing through them, hence hiding the important information to forward to the next node or destiny node. A grey hole attack affects one or two nodes in the network, whereas a black hole attack affects the whole network [3].

4. LITERATURE SURVEY

Satvir Singh and Meenaxi (2013) [4] Wireless sensor networks (WSNs) have emerged as an effective solution for a wide range of applications. Most of the traditional WSN architectures consist of static nodes, which are densely deployed over a sensing area. Recently, several WSN architectures based on mobile elements (MEs) have been proposed. Most of them exploit mobility to address the problem of data collection in WSNs. This paper first defines WSNs with MEs and provide a comprehensive taxonomy of their architectures, based on the role of the MEs. Then, we present an overview of the data collection process in such scenario, and identify the corresponding issues and challenges.

Neeraj Kumar et al. (2010) [5] proposed a novel approach for the mobile users to collect data network wide. Most of the traditional Wireless Sensor Network (WSN) architectures consist of static, nodes which are densely deployed over a sensing area. The route structure of data collection is updated every time when the movement of the mobile user changes. By considering this approach we perform limited modification to update the route structure while the route performance is bounded and controlled compared to the optimal performance in the Wireless Sensor Network. In this we need to update the route structure of data collection whenever there is mobile movement. The proposed protocol to update route structure is easy to implement.

Mohit Saini and Rakesh Kumar Saini (2013) [6] proposed a secure and energy efficient data dissemination protocol for WSN. A routing metric is defined to choose the best route from the available routes. This metric guide those routes to be chosen that consume less energy. Moreover, for secure data dissemination, a session key is established between different parties to be communicated. This session key is then used for secure communication among nodes for data dissemination.

Xun Li et al. (2013) [7] The potential for collaborative, robust networks of micro sensors have attracted a great deal of research attention. For the most part, this is due to the compelling applications that will be enabled once wireless micro sensor networks are in place: location-sensing, environmental sensing, medical monitoring and similar applications are all gaining interest. However, wireless micro sensor networks pose numerous design challenges. For applications requiring long term, robust sensing, such as military reconnaissance, one important challenge is to design sensor networks that have long system lifetimes. This challenge is especially difficult due to the energy constrained nature of the devices. In order to design networks that have extremely long lifetimes, authors propose a physical layer driven approach to designing protocols and algorithms.

Sanjay Eknath Gawali et al. (2012) [8] introduced a subset of mobile wireless sensor networks, called smartphone sensor networks, where large numbers of smartphone devices cooperate to perform sensing tasks. While these emerging networks show high potential, little work has been done on design time verification and validation to ensure that a designed system will meet the specified goals. It introduces Empower, a simulation environment for smartphone sensor networks that simulates smartphone-specific properties of a sensor network, such as data collection policies, and outputs high-level system metrics, such as coverage of the environment being monitored.

5. METHODOLOGY

IP backtracking is the technique with which one can reliably find the source of a packet on the internet. Because the IP protocol is of trusting nature, the source IP address of a packet is not authenticated. The is why the source IP address in an IP packet can be falsified with the help of a technique called the IP address Spoofing that allowing the packets for attacks in which response from victim host is so well known that return packets need not be received to continue the attack. IP backtracking is the problem to find out the source of a packet.

1) If the traffic that is received, during the burst, by the receiver is same as that of sender node, then we shall place it in the suspicious list and all nodes in that list will be supervised by the network admin in every unit time.

2) If the burst is in the regular pattern, then we shall put nodes in the temporary table and also will add a counter with it.

3) If counter is greater than a certain limit that is assumed as 3 we shall put that node in the blocking list and trace back the source node.

4) If the source node is the same as that in the network it will be completely blocked otherwise we shall trace back to previous node to reach to the source node.

5) At last we shall discover the attacking node and will block it completely.

In hybrid scheme, it should deploy both packets marking scheme and packet logging scheme in the router. When packets come with to the router, it checks the hop count in the IP header to decide to conduct marking or logging. While in the single scheme approaches, the routers can do a single trace back task without judging. However, the overhead is accountable. However, the routers in hybrid scheme can reduce plenty of storage overhead. Therefore, the trade-off is reasonable and meaningful.

6. RESULTS AND ANALYSIS

For the comparison of the results of existing and proposed technique, MATLAB software is used. A comparison is made between hybrid routing schemes by taking 25 subscriber stations which are shown below.

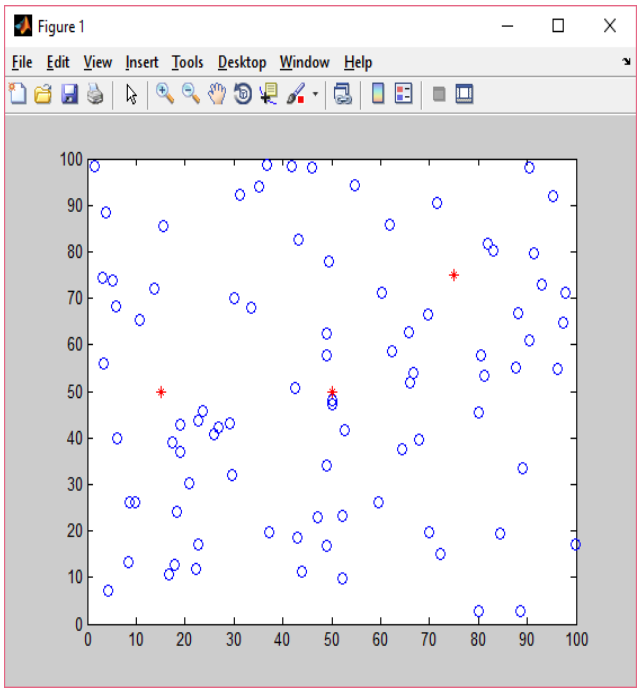

Fig.3 Deployment of Nodes

Figure3 is the presentation of the number of nodes deployed in an area of 100*100m^2. In this figure, there is a sink location that is specified in a location of x = 50 and y = 100 on which the nodes are to be deployed. In the above network, there are clusters which are red in color.

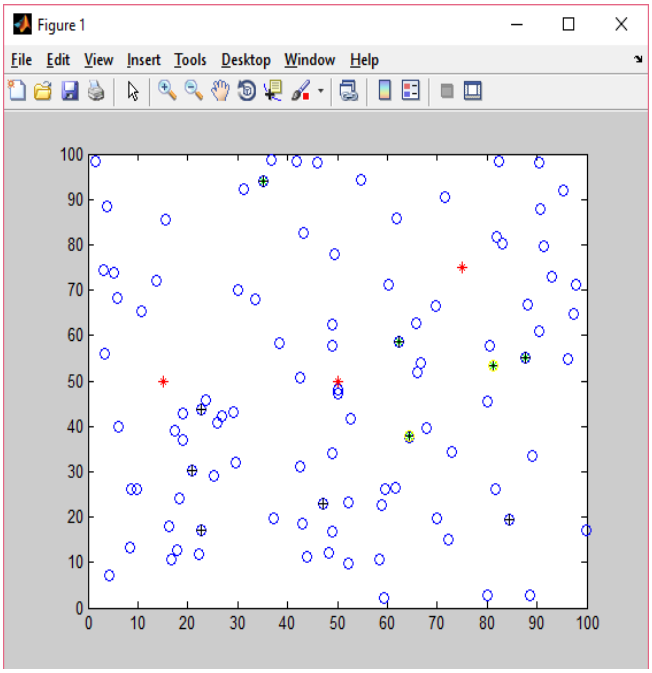

Fig.4 Blacklisted and Attacker nodes

Figure4 is the presentation of the number of nodes deployed in an area of 100*100m^2. In this figure nodes with yellow color are blacklisted and nodes with a plus sign are attacker nodes.

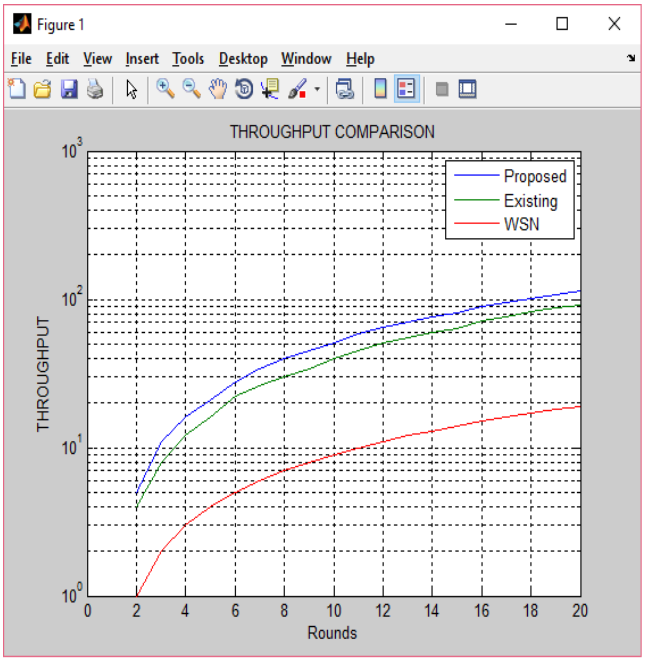

Fig.5 Throughput

THROUGHPUT: It is the amount of data moved successfully from one place to another in a given time period.

Figure5 is the presentation of throughput against the number of rounds. This figure is a comparative study of proposed technique i.e. IP Backtracking and existing technique, i.e. Control Sequence. It is clear that the throughput in proposed technique is more than that of WSN and existing technique.

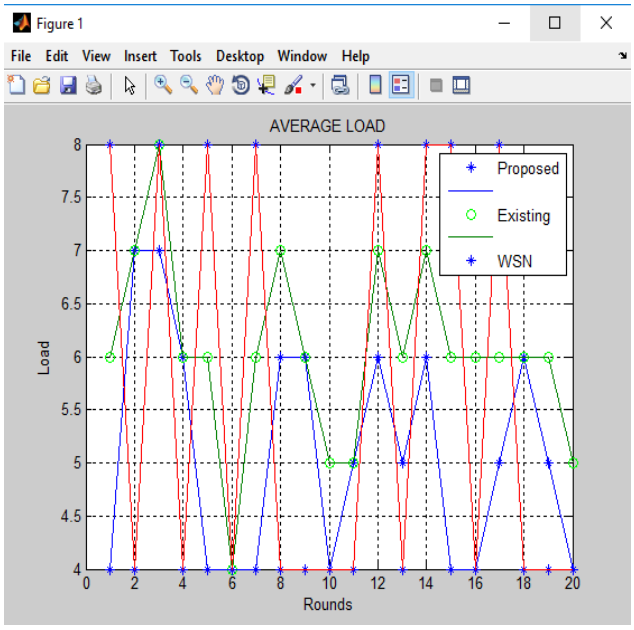

Fig.6 Average Load

LOAD: Network load balancing (commonly referred to as dual-WAN routing or multi homing) is the ability to balance traffic across two WAN links without using complex routing protocols.

Figure6 is the presentation of load against the number of rounds. This figure is a comparative study of the proposed technique and existing technique and it has been analyzed that the load is less as compared to WSN and existing ones.

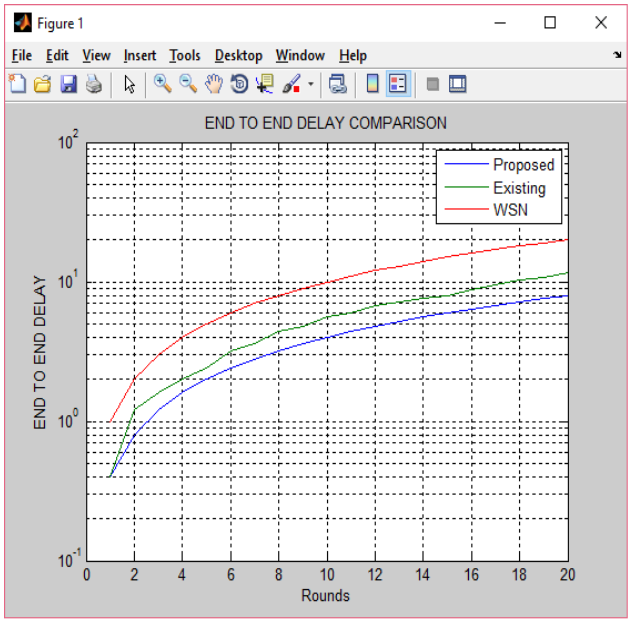

Fig.7 End to End Delay

DELAY: End-to-end delay or one-way delay (OWD) refers to the time taken for a packet to be transmitted across a network from source to destination. It is a common term in IP network monitoring, and differs from round-trip time(RTT).

Figure7 is the presentation of delay against the number of rounds. This figure is a comparative study of proposed and existing technique and it has been analysed that delay as compare to WSN and existing one is less in proposed technique.

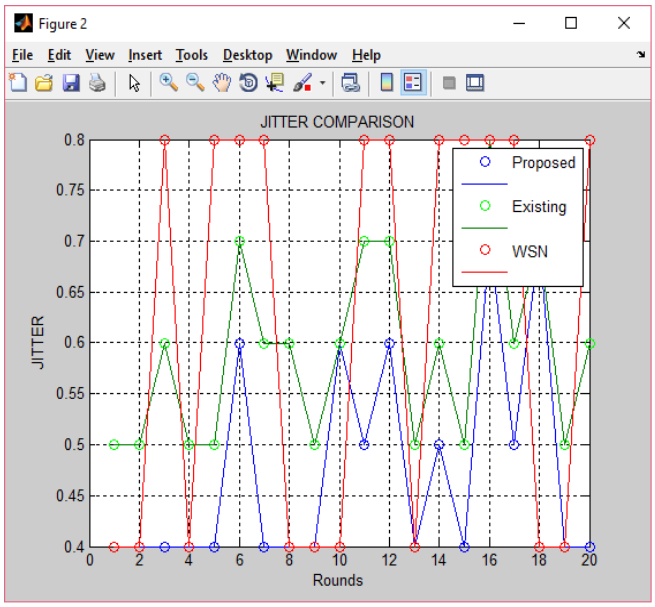

Fig.8 Jitter

JITTER: Jitter is defined as a variation in the delay of received packets. The sending side transmits packets in a continuous stream and spaces them evenly apart. Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant.

Fig 8 is the presentation of jitter against the number of rounds. This figure is a comparative study of the proposed technique and existing technique. It is clear that the jitter in proposed technique is less than that of WSN and existing technique in the network.

7. CONCLUSION

An efficient trace-back scheme is necessary to identify the sources of attacks which impose an imminent threat to the availability of Internet services. The work presented in this thesis adopted a hybrid trace-back approach in which packet marking and packet logging are integrated to achieve the best of both worlds. Therefore, at any point in the network, if there is a sudden movement in the number of packets with the same destination address and with the same group of digest marks. By using this approach to detect the source address for tracing the attacker reduce time and also memory of ours network. Memory management is done by generating a bit of RED which is inside the packet to say that if the packet is sent by the attacker or the actual node. We shall generate a bit in RED if the attacker is sending packets otherwise the bit is 0. If we talk in terms of time than the time taken to calculate or detect both the attacks is less than that of the previous approaches because we can detect both the attacks to a high extent by using our technique to mitigate attacks. Now tracing a single IP packet back to its origin is the ultimate goal of IP trace-back. Our technique illustrates the feasibility of tracing individual packets with packet logging. However, the storage overhead and access time requirement for recording packet digests are fairly high at high-speed routers.

8. REFERENCES

[1] M. M. Warrier, K. Ajay, "Efficient Energy Routing in WSN: A Survey," In the proceedings of IEEE Wisp NET conference, pp: 1987-1992, 2016.

[2] A.A. Chavan, Prof. D.S. Kurule, Prof. P.U. Dere. "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack", In the proceeding of 7th International Conference on Communication, Computing and Virtualization, Science Direct, Vol 79, pp: 835-844, 2016.

[3] M. Dharmendra, S. Deepak, P. Sunil, "A Review on Grey Hole Attack in WSN," International Journal of Computer Applications, Vol 122, No.2, pp: 33-36, 2015.

[4] Deepali Virmani, Ankita Soni, Shringarica Chandel, Manas Hemrajani, "Routing Attacks in Wireless Sensor Networks: A Survey".

[5] Pritesh Patel, Nikhil Lende, "Security in Wireless Sensor Network", International Journal of Advanced Research in Computer Engineering and Technology(IJARCET), Vol. 4, Issue 4, pp: 1322-1325, 2015.

[6] Satvir Singh and Meenaxi, "A Survey on Energy Efficient Routing in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 7, pp: 184-189, July 2013.

[7] Neeraj Kumar, Manoj Kumar, and R. B. Patel, "A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks", International Journal of Network Security, Vol 15, No.6, pp: 490-500, Nov 2010.

[8] Mohit Saini, Rakesh Kumar Saini, "Solution of Energy-Efficiency of sensor nodes in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 5, pp: 353-357, May 2013.

[9] Xun Li, Geoff V Merrett, Neil M White, "Energy-efficient data acquisition for accurate signal estimation in wireless sensor networks", Journal on wireless Communications and Networking 2013.

[10] Sanjay Eknath Gawali, Prof. D. S. Mantri, "Lifetime Energy Efficient Optimization for WSN", International Journal of Network Security, Vol 16, No.6, pp: 490-500, Oct 2012.