# Saving Wireless Networks By Detecting, And Designing Efficient From Masquerade Attacks

Sonu Kumar, Anshul Anand

**Abstract :** Wireless sensor networks (WSNs) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. Wireless medium is inherently broadcast in nature. This makes them vulnerable to attacks. These attacks can disrupt the operation of WSN and can even defeat the purpose of their deployment. An adversary can launch DoS attacks without much effort (e.g. even without cracking keys used for cryptography-based solutions). Masquerade attacks can be very dangerous because adversaries can launch other attacks and can still hide and project themselves as legitimate nodes. Therefore, masquerade detection mechanisms are necessary. To be practical for real life WSN deployments techniques for detecting masquerade attacks should be lightweight. In our research, we proposed AODV routing protocol is used in detection technique. Time factors with rest of parameters are set to detect the malicious node.

**Keywords:** Wireless Sensor Network, Security, Attack, AODV Routing.

## 1. Introduction

A wireless sensor network has been a new and hot domain in computer science and technology and has a wide application future. The wireless sensor networks consists of small sensor nodes able to detect light, sound, temperature, motion, an intelligent computing devices that enables the processing of data collected from sensors, and communication capabilities with other nodes through wireless networks. Sensor nodes can self-organize to form networks and communicate with each other using their wireless interfaces and transmit to the destination as multi-hop. In large-scale sensor networks, hundreds or thousands of sensor nodes are randomly deployed into a sensing field. WSN is a very large array of diverse sensor nodes that are interconnected by a communication network. The sensing data are shared between the sensor nodes and are used as input for adistributed estimation system. The fundamental objectives for WSN are reliability, accuracy, flexibility, cost effectiveness, and ease of deployment. WSN is made up of individual multifunctional sensor nodes. Sensor nodes are especially useful in extremely hostile environments, such as near active area, inside a dangerous chemical plant, or in disaster areas with a nuclear reactor.

### 1.1 Security in Wireless Sensor Networks

Due to inherent limitations in wireless sensor networks, security is a crucial issue and a sensor network is highly vulnerable against any external or internal attack, thus the infrastructure and protocols of the network must be prepared to manage these kinds of situations. In this security problems that sensor networks face due to node resource limitations like memory and energy, sensor network constraints like unreliable communication, collisions and latency and physical limitation like unattended after deployment and remotely managed.

### 1.2 Security Challenges

WSNs have many characteristics that make them very vulnerable to malicious attacks. Some of these are :

1. A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs.
2. Due to standard activity, Most routing protocols for WSNs are known publicly and do not include potential security considerations at the design stage. Therefore, attackers can easily launch attacks by exploiting security holes in those protocols. Due to the complexity of the algorithms, the constrained resources make it very difficult to implement strong security algorithms on a sensor platform. To design such security protocols is not an easy task. A stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off must be made between security and performance. However, attackers can break weak security protocols easily.

3. A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment.

## 2. Proposed Work

Any node under attack in wireless sensor network exhibits an anomalous behavior called the malicious behavior. The most likely threats to public safety wireless deployments, especially those using 802.15.4 technologies, are passive eavesdropping, masquerading, and denial-of-service attacks. All of these are supported by widely available tools and can be difficult to detect. In addition, passive eavesdropping and denial-of-service can never be completely prevented. a. Eavesdropping attacks are designed to expose protected information. Passive eavesdropping, the most likely eavesdropping threat, can be best prevented through the use of strong encryption against these attacks and are becoming widely available.

b. Masquerading attacks involve attackers inserting themselves into the wireless network. In most of these attacks, the attacker simulates the wireless access point itself. Fortunately, the Wireless Protected Access (WPA) and 802.11i technologies are effective defenses.

Any malicious node in the network can disturb the whole process or can even stop it. To stop such malicious behavior several detection and prevention solutions have been discovered.

## Algorithm

1. If link layer reports a link failure, try to repair the link locally using buffer information.
2. Remove the lost neighbor from all the precursor lists.
3. For each unreachable destination if precursor list non-empty add to RERR (route error) and delete the precursor list.
4. If a packet is forwarded where no route exist, drop the packet and send error upstream.
5. If a valid route has expired, purge all packets from send buffer and invalidate the route.
6. Check the TTL on every node, if it is zero, and then discard to prevent from routing loop.
7. Sequence numbers is used to determine an up-to-date path to a destination.
8. Set an expiry time to the route by adding active route time to current time.

In our research, AODV routing protocol is used in detection technique. Time factors with rest of parameters are set to detect the malicious node. Many existing prevention techniques are discussed like strong encryption, Wireless Protected Access (WPA) and 802.11i technologies, backup communication mechanism etc. To implement detection technique based on time factor many prevention techniques are also described. When prevention is followed network can be cured from attacks.

## 3. Results

The analysis is being done on the basis of the results of *.nam file and the *.tr file with the help of Network Animator (NAM) and trace graph by plotting the 2D and 3D graphs. The performance of the protocol by using AWK programming is evaluated. With the help of AWK programming the results in percentage is obtained .

### 3.1 Detection technique

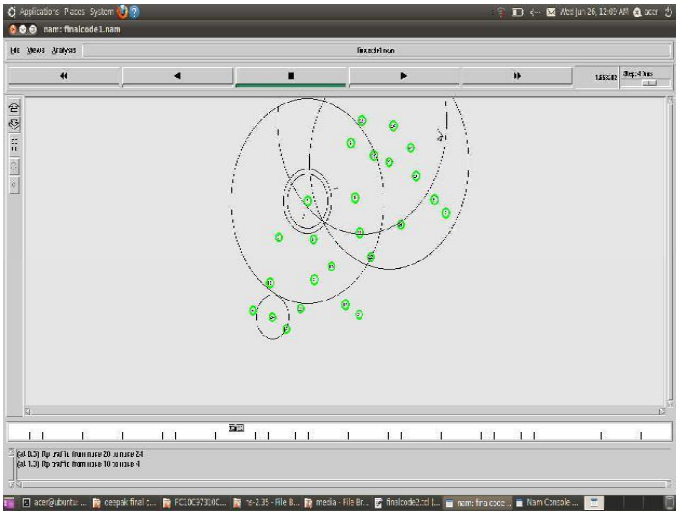
To detect malicious node timers are used with AODV protocol. AODV uses the following fields with each route table entry:

-Destination IP Address
-Destination Sequence Number- Valid Destination Sequence Number flag
- Other state and routing flags (e.g., valid, invalid, repairable, being repaired)
- Network Interface
- Hop Count (number of hops needed to reach destination)
- Next Hop
- List of Precursors
- Lifetime (expiration or deletion time of the route)

A link can break between two nodes. If the broken link is closer to the destination than source, attempt a local repair. For local repair buffer the packets in interface queue. // mark the route as under repair rt->rt_flags = RTF_IN_REPAIR; If time out in local repair attempt, route can yet to be repaired, bring down the route and send route errors upstream. This routine is invoked when the link-layer reports a route failed. This is link failure management function. In this condition, try to build route from the source. Non-data packets and Broadcast Packets can be dropped. For each valid route maintained by a node (containing a finite Hop Count metric) as a routing table entry, the node also maintains a list of precursors that may be forwarding packets on this route. These precursors will receive notifications from the node in the event of detection of the loss of the next hop link. The list of precursors in a routing table entry contains those neighboring nodes to which a route reply was generated or forwarded. Remove the lost neighbor from all the precursor lists. If the route is up, forward the packet. If it is the source of the packet, then do a Route Request. A local repair is in progress. Buffer the packet. If a packet is forwarded for someone else to which it don't have a route, drop the packet and send error upstream. Now the route errors are broadcast to upstream neighbors. If a valid route has expired, purge all packets from send buffer and invalidate the route. If the route is not expired, and there are packets in the sendbuffer waiting, forward them. If the route is down and if there is a packet for this destination waiting in the sendbuffer, then send out route request. SendRequest will check whether it is time to really send out request or not. In order to track direction of packet flow, direction_ in_hdr_cmn is used instead of incoming flag. For packet originating...* Add the IP Header ch->size() += IP_HDR_LEN; It can happen that a node received a packet that it sent. Probably it is a routing loop. Check the TTL. If it is zero, then discard. Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router whether or not the packet has been in the network too long and should be discarded. For a number of reasons, packets may not get delivered to their destination in a reasonable length of time.

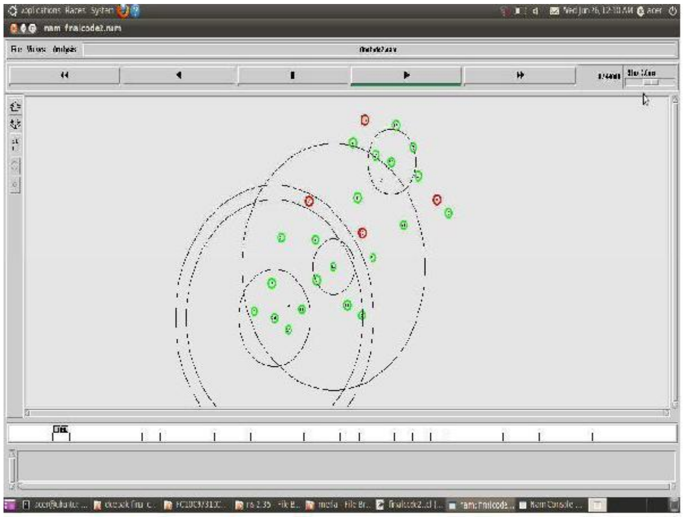
### 3.2 AODV Simulation

In the simulation of simple AODV, experiment is carried over 25 nodes. In the ns2-allinone package NAM is a build-in program. NAM helps us to see the flow of route request (RREQ) and route reply (RREP). It also shows the packets are dropping or reaching to the destination properly. When the TCL file is written, NAM is invoked inside that file. Figure1 and figure 2 are animation capture of WSN with 25 nodes. The source is broadcasting RREQ message to all its neighbors and destination node, is sending RREP (route reply) back to the source. All nodes will receive the message and forward it to its neighbor, except the malicious node, which drop the packets.



```
(at 0.3) ftp traffic from node 20 to node 24
(at 1.3) ftp traffic from node 10 to node 4
```

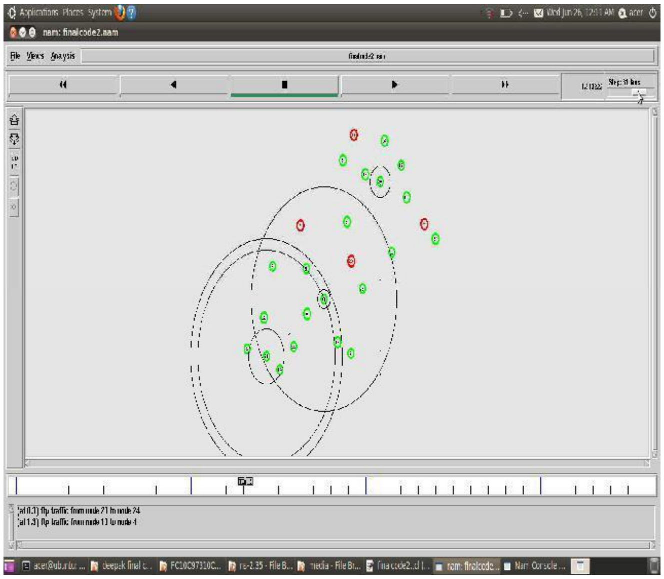
**Figure1: Simple AO**



DV simulation with 25 nodes

**Figure2:** Malicious node implementation

Here figure2 is showing the malicious nodes over the network. The malicious nodes are defined in red color. These nodes are not able to provide the effective communication as the nodes are attacker nodes



```
(at 0.3) ftp traffic from node 21 to node 24
(at 1.3) ftp traffic from node 13 to node 4
```

**Figure3: Detection of malicious node**

In simple AODV not much packet drop because there is direct peer to peer communication and network is free any malicious injection.In malicious code packet drop rate is very high because malicious node only creates link with legetimate nodes but does not receive the packet. In this proposed work, the loss rate is decreased as shown in figure 4

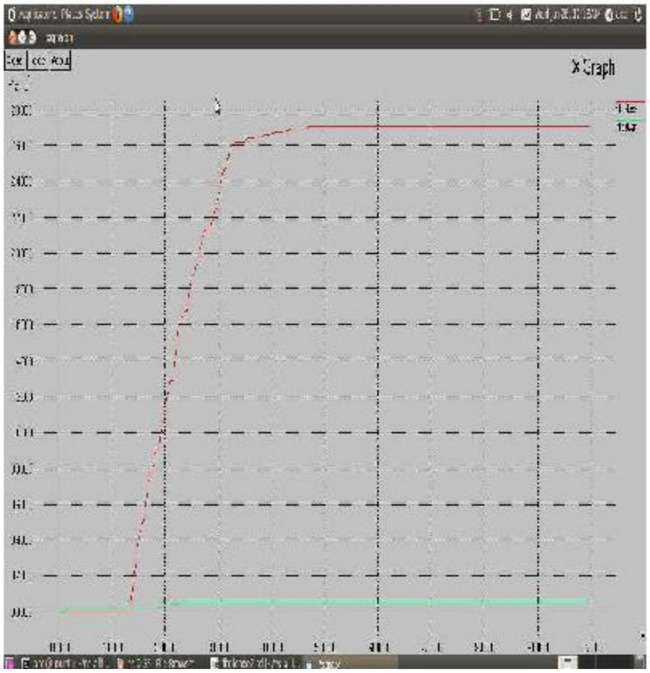


**Figure4**: Dropped packet v/s Simulation Time

Malicious nodes are dropping the packet so there is less packet transmission over the network and packet transmission ratio is low. Shown in Figure5 is showing the results in terms of packet transmitted ovre the network and the proposed work provides the higher transmissin rate

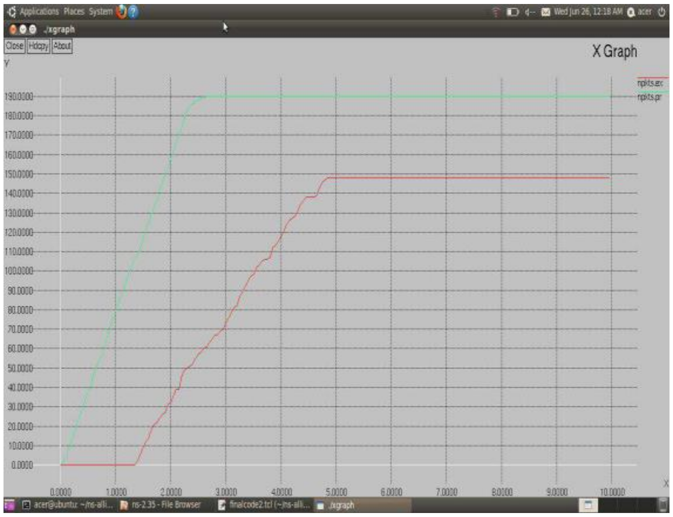


**Figure5** Packet Transmission v/s Simulation Time

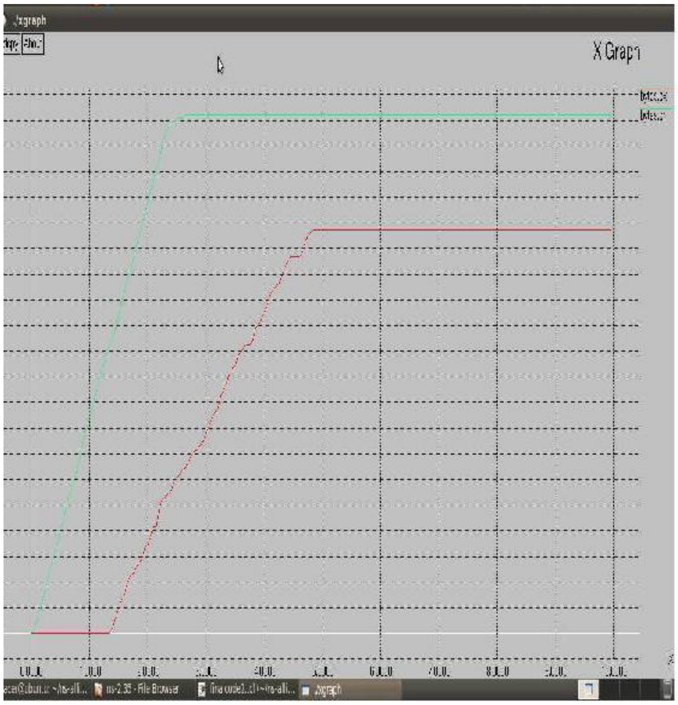


**Figure6**: Bytes Transmitted v/s Simulation Time

Here figure 6 is showing the analysis in terms of bytes transmitted. As we can see, In this work the total bytes transmission over the network is increased respective to time

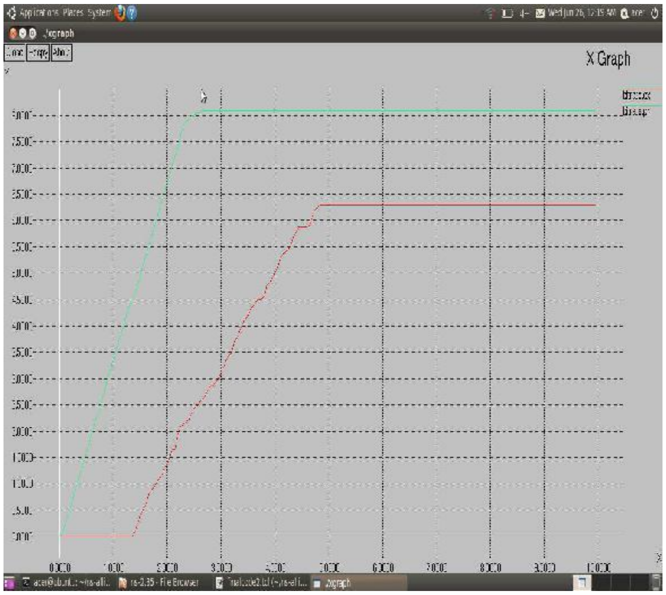


**Figure7**: Bitrate v/s Simulation Time

Here figure7 is showing the analysis in terms of bitrate over the transmission. As we can see, In this work the total bitrate of transmission is improved over the network.

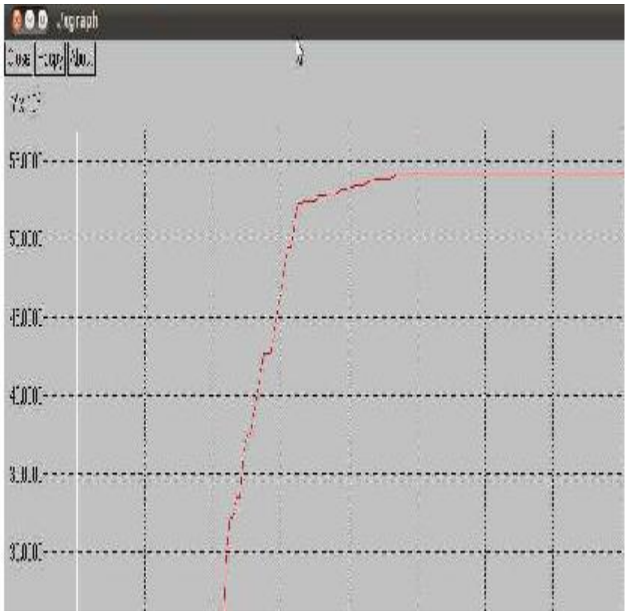


**Figure8**: Packet Loss rate v/s Simulation Time

Here figure 8 is showing the analysis in terms of loss rate over the transmission. As we can see, In this work the total loss rate of transmission is decreased over the transmission

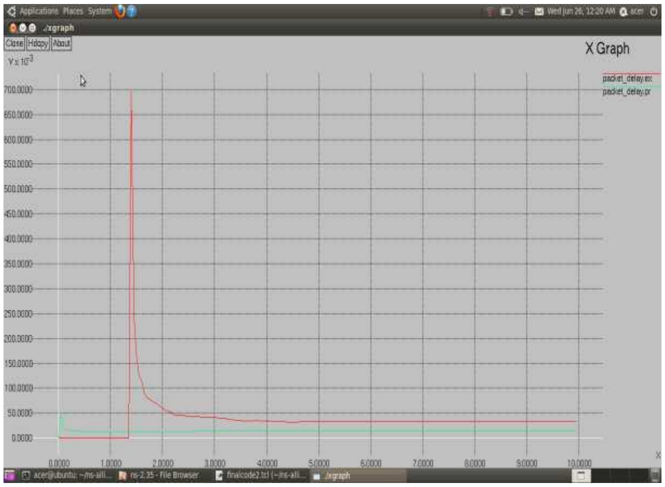


**Figure9:** Transmission Delay v/s Simulation Time

Here figure 8 is showing the analysis in terms of transmission delay over the network. As we can see, in this work the packet delay of transmission is decreased over the transmission. So that the throughput is improved. Performance measurement is done on the basis of dropped packet, packets transmission, packet loss rate, bitrate, number of bytes transmitted, packet delay.

## 4. Conclusion

Security is a significant issue in Wireless Sensor Networks. Intrusion of malicious nodes may cause serious impairment to the security. In the presented work, all the modes of AODV (simple mode and malicious node) have been discussed. This work can help in the area of security based systems. In this research work, AODV over WSN is simulated with different operation modes. An important contribution of this dissertation is the AODV with and without malicious node. As the malicious node enters into the network, it tries to capture the network. The performance of the network is affected badly. The parameters measured are number of packet send, and number of packet received, packet delivery ratio and number of packet dropped. But, after detecting the malicious node, performance of the network increase. Malicious node drops the entire packet but IDS again increase the packet delivery ratio and decrease the packet drop rate. In future work other parameters can also be considered like energy consumption, overload, throughput etc.

## References

[1] F. Akyildiz and W. Su and Y. Sankarasubramaniam and E. Cayirci, “Wireless sensor networks: a survey", Computer Networks, Vol.38, pp. 393{422, March 2002.

[2] Jangra1,A. Goel and N. Priyanka and Bhati,K. “Security Aspects in Mobile Ad Hoc Networks (MANETs)” A Big Picture”, International Journal of Electronics Engineering, pp. 189-196, 2010

[3] K. Jones and A.Waada and S. Olaniu and L.Wison and M. Eltoweissy, “Towards a new paradigm for Securing Wireless Sensor Networks”, New Security Paradigms workshop 2003, Ascona, Switzerland.

[4] Vijay Bhuse and Ajay Gupta and Ala Al-Fuqaha “Detection of masquerade attacks on Wireless Sensor Networks” , Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008 2 Institute of Security Technology Studies, Dartmouth College, Hanover, NH 03755

[5] Security Goals By PFleeger http://www.cis.temple.edu/~jfiore/2012/spring/4378/handouts/pfleeger/ch01/ch01.pdf

[6] Yinfei Pan “Design Routing Protocol Performance Comparison in NS2: AODV comparing to DSR as Example”, Department of Computer Science SUNY Binghamton Vestal Parkway East, Vestal, NY 13850.