# Detecting Packet Droppers and Modifiers in Wireless Sensor Network

AyushiNainwal [1], ArvindKalia [2], Jawahar Thakur [3]
Computer Science [1, 2, 3, 4], Himachal Pradesh University [1, 2, 3, 4]
Email: ayushinainwal@gmail.com [1] , arvkalia@gmail.com [2], jawahar.hpu@gmail.com [3]

***Abstract***- Wireless networks are widely used because these are very easy to install. However, there are various security issues and problems while deploying it. Two most important issues are Packet modification and dropping. These are the common attacks that can be generated by an attacker to disrupt communication in wireless sensor networks. Many schemes have been proposed to reduce or tolerate such attacks but very few can effectively and efficiently identify the intruders. This paper proposed a simple and an effective scheme, which can identify misbehaving nodes that drop or modify packets. Heuristic ranking algorithm is been used to identify the bad nodes. The alert message will be forwarded to all the users in the network if any misbehaving action occurred, so that no message will reach the misbehaved node and the node will be blocked.

***Index Terms***- *Wireless Sensor Network, Packet dropper and modifiers, Node Categorization, Heuristic ranking approach.*

*****

## 1. INTRODUCTION

A wireless sensor network (WSN) is an important and exciting new technology. With its growth the wireless security has become more important. In WSNs the wireless medium is inherently broadcasting in nature and hence is mostly unguarded. This makes wireless sensor network vulnerable to various kinds of attacks like denial-of-service (DOS) attack. Without proper security measures, an opponent can launch various kinds of attacks. These attacks can interrupt the normal working of WSNs and can even defeat the purpose of their deployment. The various types of denial-of-service attacks are packet dropping, false route request or flooding. Hence, intrusion detection mechanisms to detect various attacks are needed. Wireless sensor network (WSN) consists of three main components: the nodes interface with sensor which are spatially distributed, software, and gateways. Sensor nodes are the small devices consisting of a radio, a processor, a battery, and a memory and sensor hardware. These nodes can gather sensory information, perform processing and can communicate with other sensor nodes in the network. The acquired data is transmitted to the sink, which could be a gateway, a user, a storage node, or a base station. Sensor nodes are constrained in terms of various resources like radio range, memory size, power and processor speed. Whenever a sensor network is installed in an unsecure environment to perform the monitoring and data collection, it lacks physical protection and leads to node compromise. If one or more sensor nodes are compromised, an attacker may easily launch various attacks [4] in order to disrupt the communication within a network. Among these attacks, two common ones are packets dropping and packets modifying.To reduce the problem of packet droppers various methods can be used. First method is of multi-path forwarding [1], [9], in which each packet is forwarded along multiple alternative paths through a network. This will ensure that the packet reaches destination through some alternative path even if one or more path fails. The disadvantage of this scheme was extra communication overhead. Second method is to monitor the behavior of forwarding nodes [8]–[7]. However, this method subject to high energy cost. To deal with packet modifiers, one of the existing countermeasures [2]–[10] is to filter modified or altered messages within a certain number of hops but to make it more effective packet droppers and modifiers needs to be identify because the attacker nodes can still continue attacking the network without being caught. To identify packet modifiers probabilistic nested marking (PNM) scheme was used. This scheme was proposed by Ye [3] to identify packet modifiers with a certain probability. The only problem with PNM scheme was that it cannot be used together with the packet filtering schemes. The packet filtering schemes will remove all the modified packets which the PNM scheme needs to use as a proof to find packet modifiers. This problem reduces the efficiency of deploying the PNM scheme. In this paper a simple yet effective method is proposed to catch both packet modifier and dropper. According to this, a routing tree whose root node is sink node is first established. The data collected by sensor node is transmitted along the tree structure towards the sink in the form of packets using multipath routing approach. Each packet forwarder adds a small number of extra bits, which is called packet marks, to the packet. The format of the packet marks is carefully designed such that the sink can obtain very useful information from the marks like the dropping rate of a sensor node, and then run node categorization algorithm to identify nodes that are for sure dropper or modifiers. The structure of the tree changes dynamically after certain time interval so we can easily observe behavior of sensor nodes in different scenarios. Once the behaviors have been accumulated, the sink periodically run heuristic ranking algorithms to identify bad nodes from suspiciously bad nodes.

## 2. IMPORTANCE OF MULTIPATH ROUTING APPROACH IN WIRELESS SENSOR NETWORKS.

The multipath routing technique which has demonstrated its efficiency to improve wireless sensor performance is efficiently used to find alternate paths between sources and sink. This approach is considered as one of the existing solutions to cope with the limitations of routing. The benefits of multipath routing are:

- Reliability and Fault Tolerance: The multipath routing approach in wireless sensor networks provide path resilience and reliable data transmission. . Fault tolerance means if a node cannot forward the packets in the direction of the sink then available alternative paths are used to prevent packets from failures. Since many alternative paths are available from a target area to the sink node, packet transmission can be continued without any interruption even if path failure occurs. This will also increase the reliability of packet transmission. There are two ways of providing reliability in multipath routing; the first technique is by sending numerous copies of the original data across various routes to allow recovery of data from route failures. In this case the reliability of data transmission is assured when at least one route is able to forward data safely. The second technique is erasure coding, in this approach, every source node inserts extra information to the original data before distributing the packets across different routes. So in case of routes failure to send packets to the sink, data transmission can still continue by reconstructing packets from previous good routes.

- Load Balancing: Sensor nodes are constrained to resource availability, leading to congestion which further leads to degradation of network performance. To handle this problem, multipath routing approaches can provide the best solution through splitting network traffic over several paths. The main goal of load balancing is to use the available network resources in order to reduce the risk of traffic congestion. When a link becomes over-utilized and causes congestion, multipath routing protocols can be chosen to divert traffic to alternate paths to reduce the burden of the congested link. Also, the distribution of network traffic across numerous sensor nodes might contribute to equal energy consumption between the nodes and extend the lifetime of the network.

- QoS Improvement: Quality of service supported in terms of network throughput, end-to-end latency and data delivery ratio is important in designing multipath routing protocols for various types of networks. Discovered alternative paths can be used to distribute network traffic based on the quality of service demands of the application for which the multipath routing protocol has been designed

- Reduced Delay: In wireless sensor nodes if a path failure occurs when single path routing protocol is used then a new path has to be discovered which further contribute to delay of route discovery. The delay is minimized in multipath routing protocol because during route discovery many alternative paths are identified.

- Bandwidth Aggregation: Multipath routing provides bandwidth aggregation, this is beneficial when a node has multiple low bandwidth links but requires a bandwidth that is greater than the one which an individual link can provide .For example, suppose a node wants to forward large data to the same destination but the bandwidth of an individual link is small thus the large data can be split into multiple streams where each stream is routed through different path, aggregating the effective bandwidth.

## 3. THE PROPOSED SCHEME FOR INTENDED STUDY

**3.1.** ***Network Description:*** Consider sensor network, with large number of sensor nodes in a two dimensional area. Each sensor node generates sensing data after certain interval of time and all these nodes work together to forward packets containing data hop by hop towards a sink.

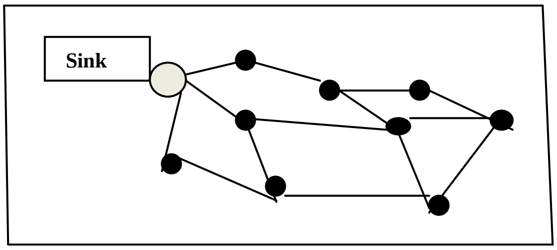

Fig1. Network System Model

All sensor nodes and the sink are time synchronized [6]. Time Synchronization in wireless networks is extremely important for secure and stable communication. It allows for successful communication between nodes on the network. In sensor networks the exact location of nodes are not known so time synchronization is used to determine their location. Time stamped messages will be send to the nodes in order to determine their relative proximity to one another. Time synchronization is also used to save energy; it will allow the nodes to sleep for a given time and then awaken periodically to receive a signal.

***3.2 Security and Attack Modes:*** The sink node is trustworthy and will not compromise, but all other regular sensor nodes in a network can be compromised. Compromised nodes may collude with each other in order to accuse some innocent node. A compromised node can generate the following two attacks:

(1) Packet dropping: a compromised node drops the packets that it is supposed to forward. It may also drop the data generated by it in order to accuse some innocent nodes.
(2) Packet modification: a compromised node alters the packets that it is supposed to forward. It may also alter the data it generates to accuse other nodes.

The proposed scheme consists of several equal-duration rounds of intruder identification phases as shown in figure 2.In the initialization phase sensor nodes form a topology which is a Tree on Directed Acyclic Graph. The data is transferred through the routing tree to the sink node in form of packets. Each packet forwarder adds some extra bits to the packet which is called packet mark. When one round is over, based on the packet mark carried in the received packets, the sink node will run a node categorization algorithm to identify nodes that are packet droppers (bad for sure), suspected to be packet droppers (suspiciously bad) and no packet droppers (good for sure).The routing tree is reshaped at every round providing different topology. After certain number of rounds, the sink node collects the information about node behavior in different routing topologies. The information collected helps to identify which nodes are bad for sure, suspiciously bad, and good for sure.

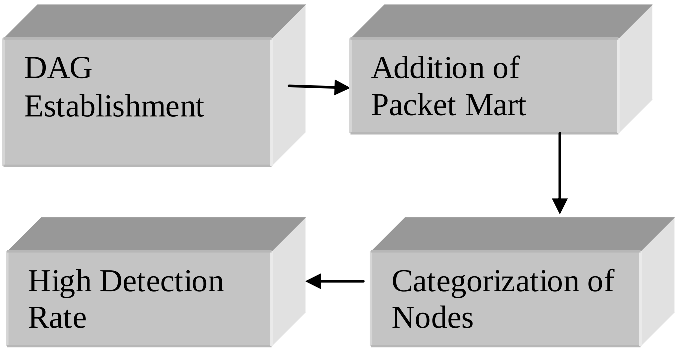

Fig.2. Flow diagram for intruder identification

Detailed description of each phase is as given below…

***(1) Initialization phase:*** In the starting of the initialization phase, a directed acyclic graph (DAG) is formed that represent the topology followed by all sensor nodes. A routing tree is extracted from the directed acyclic graph. Data to be forwarded follow the routing tree structure. In this phase a secret pair of key is set up between the sink and all the other remaining nodes in graph. Each sensor node u is provided the following information

a) Ku: is a secret key specifically shared between the node and the sink.
b) Lr: The duration of a round.
c) Np:The maximum number of parent nodes that each node records during the tree establishment procedure.
d) Ns$^{th}$ packet is numbered Ns-1, the Ns-1$^{th}$ packet is numbered 0, and so on and so forth.
e) Ns: the maximum packet sequence number.

**(2).** ***Intruder Identification phase:*** In each round, data is transferred through the routing tree to the sink. Each packet sender/forwarder encrypts the packet by adding a small number of extra bits to it. As one round finishes, the sink runs a node categorization algorithm which categorize the nodes as bad nodes and suspiciously bad. The routing tree is reshaped every round, after certain number of rounds, sink collects enough information about node behaviour in different topologies.

***(3)Packet Sending:*** Suppose a sensor node (u) has certain data (D) to send. It will create a packet (Pu) and send it to other node,
Pu:<Pu,{Ru,u,Cp MOD Ns,D,padu,0}Ku,padu,1>here Pu denotes parent node, Ru is a receiving node, Cp is a counter node, pad u,0 and pad u,1 are padding, Ku is an encryption key. Padding is added to make all packets equal in length, so that forwarding nodes cannot identify packet sources based on packet length. The sink can decrypt the packet to find out the actual content.

***(4). Packet forwarding:*** As the node v receives packet <v,mi>, it creates and forward the packets Pv to its parent node where Pv: <Pv,{Rv,m}Kv>. The value of m is obtained by removing the rightmost log(Np) bits of m. To keep the length of the packet same Rv having log(Np) bits, is added to the front of m.

***(5) Packet receiving at the sink:*** Sink tries to find a child node for each parent node by performing decryption which results in a string. If the packet is modified the attempt fails else it succeeds and the packet is forwarded from respective node.

***(6) Node Categorization Algorithm:*** In every round sink node(s) needs to keep track of number of packet sent from node u and number of packets received by node s. Then the sink node s calculates for every round the dropping ratio for each node u. Let us suppose that Nf is the number of transmitted packets and Nr is the number of received packets. The dropping ratio (du) is calculated as follows:
$du= ( Nf-Nr *Nf) /( Nf+Nr +(Nf*Nf-Nr ))$
By calculating the dropping ratio of every sensor node, the sink categories the sensor nodes as bad nodes, suspiciously bad nodes or good nodes. A threshold θ is used which determines the maximum value for dropping ratio.

```
Input: Tree T, with node u, sink node s and
dropping ratio du, threshold value θ
for each sink node in tree T do
    find dropping ratio du;
    if du<θ then
        Set u as good for sure or suspiciously
        bad
        if du = 0 then
            Set u as good for sure
        else if du >0
            Set u as suspiciously bad
        else
            break
    else
        Set u as bad for sure
repeat
```

## 4. RANKING ALGORITHMS

**(1) Global ranking based approach**: The Global ranking method is based on assumption that if a node is identified as suspiciously bad then there are more chances that the node is a bad node. The node with the highest value of accused account is chosen as a bad node for sure and all the pairs that contain this node are removed.

**(2) Stepwise ranking based approach**: It may happen that the GR method falsely accuses innocent nodes that were parents or children of bad nodes. So to remove this problem if a bad node u is found and there is a node v that is been suspected together with node u, the value of node v account is reduced by the times u and v have been suspected together.

***(3) Hybrid Ranking-Based (HR) Approach***: The GR Method and the SR method detect bad nodes with some false accusations so hybrid ranking method is used. The HR approach also considers accusation account value as GR and SR but it checks if an innocent node is not being framed by previously identified bad nodes. In this method first all the likely bad node are identified, then the one with highest account value is chosen only if the node has not always been accused together with the bad nodes that were identified before.

## CONCLUSION

Various techniques for detection of packet- dropping nodes in ad hoc networks incur heavy costs and are not suitable for resource-constrained wireless sensor networks. This new scheme detects whether a path is dropping packets without incurring extra cost because the alternate path, established during route discovery, is ready for the response.

## REFERENCES

[1]. C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” *the First IEEE International Workshopon Sensor Network Protocols and Applications*, pp. 113–127, May 2003.

[2]. F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical En-route Filtering of Injected False Data in Sensor Networks,” *IEEE INFOCOM*, March 2004.

[3]. F. Ye, H. Yang, and Z. Liu, “Catching Moles in Sensor Networks,” *IEEE International Conference on Distributed Computing Systems (ICDCS)*,June 2007.

[4]. H.Chan and A. Perrig, “Security and Privacy in Sensor Networks,” *IEEEComputer*, October 2003

[5]. Md. AtiqurRahman, Shahed Anwar, Md. I1eas Pramanik, Md. FerdousRahman, “A Survey on Energy Efficient Routing Techniques in Wireless Sensor Network”, In Proc. Of Advanced Communication Technology (ICACT), 15th International Conference on, pp.200,Jan 2013.

[6]. Singh Satvir, Meenaxi, “A Survey on Energy Efficient Routing in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and SoftwareEngineering,Vol.3,Issue 7,pp.184-188,July 2013.

[7]. S. Lee and Y. Choi, “A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks,” *Proceedings ofthe fourth ACM workshop on Security of ad hoc and sensor networks(SASN)*, pp. 59–70, 2006.

[8]. S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehaviorin Mobile Ad Hoc Networks,” *ACM MobiCom*, August 2000.

[9]. V. Bhuse, A. Gupta, and L. Lilien, “Dpdsn: Detection of packet-dropping attacks for wireless sensor networks,” *In the Trusted Internet Workshop, International Conference on High Performance Computing*, December 2005.

[10]. Z. Yu and Y. Guan, “A Dynamic En-route Scheme for Filtering FalseData in Wireless Sensor Networks,” *IEEE Infocom 2006*, April 2006.