Identification of Packet Dropping and Modification in Wireless Sensor Networks

[1,] B.Kishore Kumar, [2,] G.K.Venkata Narasimha Reddy

[1]M.Tech (CSE), SJCET- Kurnool (Dt), Affiliated to JNTUA University, Andhra Pradesh, INDIA.
[2] Associate Professor, Department of CSE, SJCET- Kurnool (Dt), Affiliated to JNTUA University, Andhra Pradesh, INDIA.

ABSTRACT

The Packet Droppers and Modifiers are common attacks in wireless sensor networks. It is very difficult to identify such attacks and this attack interrupts the communication in wireless multihop sensor networks. We can identify the Packet Droppers and Packet Modifiers using ranking algorithms and packet marks. The Performance is represented using detection rate and false positive probability. The Proposed scheme provides an effective mechanism for catching compromised node.

KEYWORDS: **packet droppers and modifiers,** *intrusion detection, wireless sensor networks*.

I. INTRODUCTION

The Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. In a Wireless sensor networks sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards to a sink, which could be a gateway, base station or storage node. Securing the Wireless Sensor Networks need to make the network support all security properties: confidentiality, integrity, authenticity and availability. A sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward.

We expect sensor networks to consist of hundreds or thousands of sensor nodes as in Fig 1. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram individual sensor nodes. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then mount a variety of attacks.

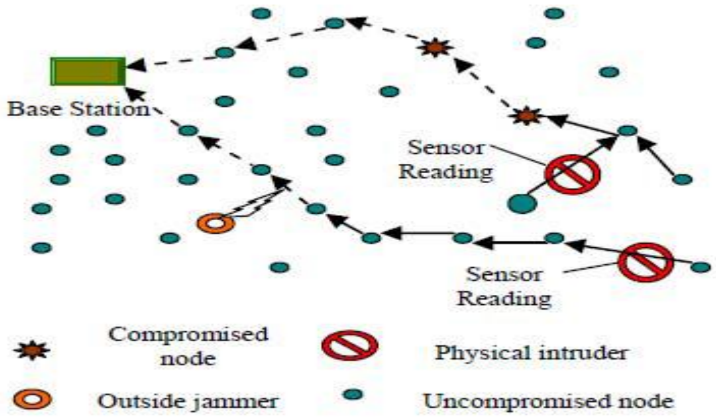

Fig 1. Sensor Network

Packet dropping is nothing but a bad node drops all or some of the packets that are supposed to be forwarded. It may also drop the data generated by itself for some malicious purpose such as blaming innocent nodes. This paper proposes a scheme to catch both packet droppers and modifiers. At first routing tree is established using DAG. Data is transmitted along the tree structure toward the sink. A packet sender or forwarder adds a small number of extra bits, which is called packet marks, is designed such that the sink can obtain the dropping ratio associated with every sensor node. Node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/ modifiers [1].

II. SYSTEM MODEL

A. Network Assumptions

We assume that a typical deployment of sensor network, as where a large number of sensor nodes are deployed in a two dimensional area. Each sensor node generates sensing data periodically and all these nodes collaborate to forward packets that contain the data hop by hop towards a sink. The sink is located at some place within the network. We assume that all sensor nodes and the sink are time synchronized, which is required by many applications. The sink is aware of the network topology, which can be achieved by requiring nodes to report their neighbouring nodes soon after deployment.

B. Security Assumptions and Attack Model

We assume that the network sink is trustworthy and free of compromise, but regular sensor nodes can be compromised. Compromised nodes may or may not collude with each other. A compromised node can launch the following two attacks:

[1] **Packet dropping:** A compromised node drops all or some of the packets that it is supposed to forward. It may also drop the data generated by itself for some malicious purpose such as accusing innocent nodes.

[2] **Packet modification:** A compromised node modifies all or some of the packets that it is supposed to forward. It may also modify the data it generates to protect itself from being identified or to accuse other nodes.

III. EXISTING SYSTEM

Existing counter measures aim to filter modified messages resend within a certain number of hopes. These measures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue the network without being caught.In existing scheme, modified packets should not be filtered out en route because they should be used as evidence to infer modified packets; hence, it cannot be used together with existing packet filtering schemes.

Disadvantages of Existing system:

- Intruders are able to collect the data while we are sending data from source to destination.
- It is not possible to send modified packets to destination.
- It cannot be easy to find what are the dropped and modified packets.
- In this system, the modified packets should not be filtered out.

IV. PROPOSED SYSTEM

Our Proposed scheme consists of system initialization phase and compromised nodes identification phases.

4.1. Initialization phase:

In the initialization phase, sensor nodes form a topology which is direct acyclic graph (DAG).A routing tree is extracted from the DAG. Data reports follow the routing tree structure. The purpose of system initialization is to set up secret pair wise keys between the sink and every regular sensor node. To establish the

Each sensor node u is preloaded the following information:

- Ku: A secret key exclusively shared between the node and the sink.
- Lr: The duration of a round.

- Np:The maximum number of parent nodes that each node records during the DAG establishment procedure.
- Nsth packet is numbered Ns-1,the Ns-1th packet is numbered 0,and so on and so forth.
- Ns: the maximum packet sequence number.

4.2.Intruder Identification phase:

In each round, data are transferred through the routing tree to the sink. Each packet sender/forwarder adds a small number of extra bits to the packet and also encrypts the packet. When one round finishes, based on the extra bits carried in the received packets, the sink runs a node categorization algorithm to identify nodes that must be bad nodes and suspiciously bad. The routing tree is reshaped every round, when a certain number of rounds have passed, sink collects enough information about node behaviors in different routing topologies.

4.3.Packet Sending:

when a sensor node u has a data item D to report, it composes and sends the following packet to its node.

Pu: <Pu,{Ru,u,Cp MOD Ns,D,padu,0} Ku,padu,1>

Where Pu - parent node, Ru – receiving node, U- node, Cp – counter node, D – data ,pad u,0 –padding, Ku encryption. Puddings pad u,0 and pad u,1 are added to make all packets equal in length, such that forwarding nodes cannot tell packet sources based on packet length, Meanwhile, the sink can still decrypt the packet to find out the actual content.

4.4.Packet forwarding:

When a sensor node v receives packet hv;mi, it composes and forwards the following packets to its parent node Pv:

$<P_{v,}\{R_{v,}m\}K_v>$

Where m is obtained by trimming the rightmost log(Np) bits off m. Meanwhile , Rv, which has logNp bits,is added to the front of m.

4.5.Packet receiving at the sink:

The sink attempts to find a child node for every parent node by decrypting which results in a string. If the attempt fails the packet is modified and it should be dropped. If it succeeds the packet is forwarded from the respective node.

4.6.Algorithm 1.Packet Receipt at the Sink

```
[1] Input: packet<0;m>.
[2] if Success Attempt =false then decrypt.
[3] if decryption fails then continue, else
[4] if Success Attempt=true then record sequence.
[5] u←v, Success Attempt=false;go to line4.
[6] if Success Attempt = false then
[7] drop this packet.
```

4.7.Algorithm 2. Tree-Based Node Categorization

```
1. Input: Tree T, with each node u marked by “+” or”_,” and its dropping ratio du.
2. for each leaf node u in T find parent node until the sink node categorize the nodes.
3. consider u as positive threshold and v as negative threshold.
4. If v. mark =”_”then until v.mark=”+” or v is Sink,Set nodes from b to e bad for sure.
5. if v is Sink then Set u as bad for sure.
6. If v. mark =”+” and if v is not bad for sure then set u and v as suspiciously bad else
7. if dv – du>θ then
8. Set v as bad for sure.
9. if difference du-dv> θthen Set u and v as suspiciously bad;
```

Nu,max - most recently seen sequence number
Nu,flip - the number of sequence number flips

nu,rcv - number of received packets.

The dropping ratio in each round is calculated as follows:

$$d_u = \frac{Nu{,}flip * Ns + Nu{,}max + 1 - nu{,}rcv}{Nu{,}flip * Ns + Nu{,}max + 1}$$

To identify most likely bad nodes from suspicious nodes:

$S_i = \{ < u_j, v_j > \mid < u_j, v_j > \text{ is a suspicious pair and } < u_j, v_j > = < u_j, v_j > \}$

Ranking algorithms:

1. Global ranking based approach:

The GR method is based on the heuristic that, the more times a node is identified as suspiciously bad, the more likely it is a bad node. The node with the highest value is chosen as a most likely bad node and all the pairs that contain this node are removed.

2. Stepwise ranking based approach:

It can be anticipated that the GR method will falsely accuse innocent nodes that frequently been parents or children of bad nodes. Once a bad node u is identified, for any other node v that has been suspected together with node u,the value of node v's accused account is reduced by the times that u and v have been suspected together.

3. Hybrid Ranking-Based(HR) Method:

The GR Method can detect most bad nodes with some false accusations while the SR method has fever false accusations but may not detect as many bad nodes as the GR method. After a most likely bad node has been chosen, the one with the highest accused account value among the rest is chosen only if the node has not always been accused together with the bad nodes that have been identified already.

4. Packet Modifiers:

Modified packets can be detected with the afore-described scheme. Modified packets will be detected by sink and it will be dropped and hence packet modifier can be identified as packet dropper .To enable en-route detection of modifications, the afore-described procedures for packet sending and forwarding can be slightly modified as follows. When a node *u* has a data item *D* to report , it can obtain endorsement message authentication codes (MACs) from its neighbors, which are denoted as *MAC(D)*, following existing en-route filtering schemes such as the statistical en-route filtering scheme (SEF)[3] and the interleaved hop-by-hop authentication scheme[4].

V. SIMULATION RESULTS

5. IMPACT OF ROUND LENGTH

Considering the delay for transmitting a packet from a source node to the sink, the round length effects number of packets received at the sink in each round, which in turn affects the detection performance. It can be seen that round length mainly affects the false positive probability. it is shown in fig. 2(a),2(b).

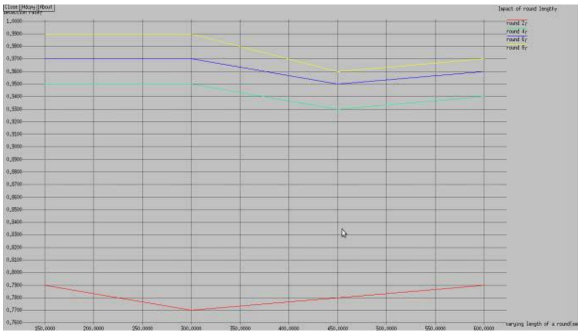

Fig 2a. Detection Rate

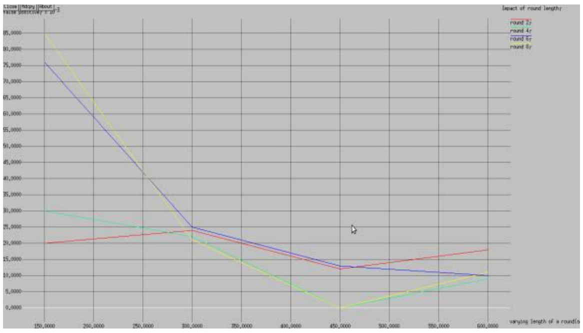

Fig 2b. False positive

5.2.IMPACT OF DROPPING PROBABILITY

Fig.3 shows the performance sensitivity to bad node’s dropping percentage (i.e., the percentage of packets that will be dropped if a bad node decides to drop packets to drop packets in a round). We vary the dropping probability between 20% and 80%.From Fig.3(a),3(b). We can see the all the three ranking algorithms have similar sensitivity to the dropping probability. In addition, with a high dropping probability, all the three algorithms achieve a higher detection rate in the early rounds, which means they can detect bad nodes quicker, and can achieve a lower false positive generally. This is because frequent misbehaviors can quickly distinguish bad nodes from innocent nodes.

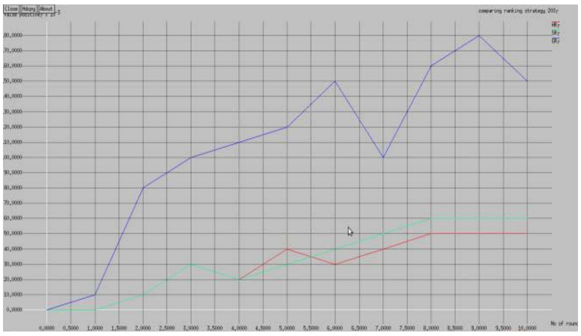

Fig 3a. Dropping probability 20%-False positive

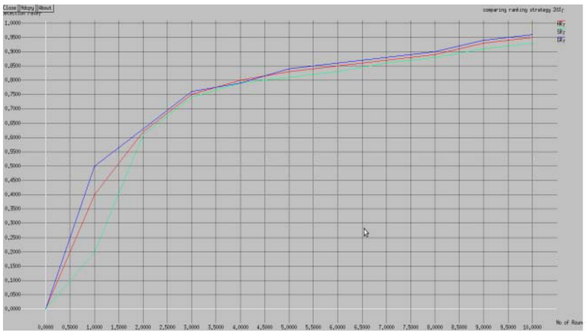

Fig 3b.Dropping probability 20%-Detection Rate

5.3.IMPACT OF THRESHOLD

Threshold for Differentiating “+” Nodes and “-“ Nodes. In order to tolerate incidental packet loss, we use a threshold θ when marking each node with “+” or “-“. Fig.3 shows the impact of this threshold on the detection performance. As depicted in Fig. 4(a), the larger is the threshold, the lower is the detection rate. This is because, fewer nodes will be marked as “-“ as the threshold increases. Hence, a part of bad nodes may escape from being detected.

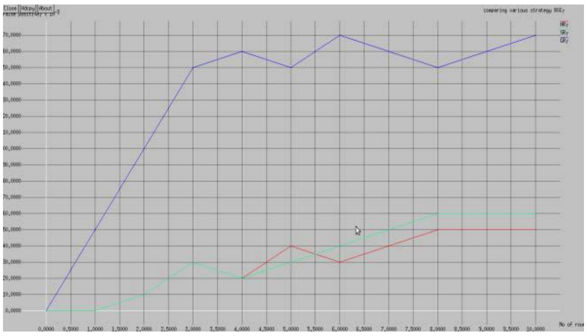

Fig.4a. Dropping Probability 80%-False positive

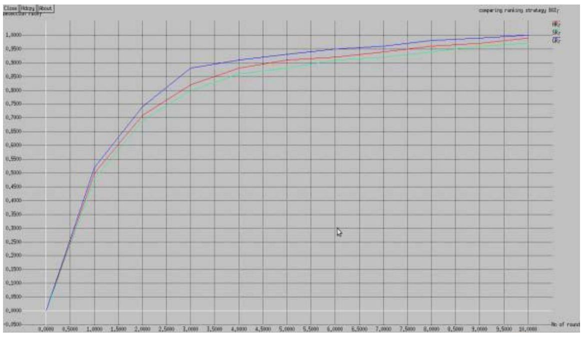

Fig. 4b. Dropping Probability 80%- Detection Rate

As shown in Fig. 4(b), when the threshold increases , the false positive probability increases first and then decreases after the threshold reaches a certain value (turning out).

Advantages of the system:

- A simple effective is used to catch both packet droppers and modifiers.
- While we are sending the data from source to destination, the node categorization algorithm finds the dropped and modified packets.
- Using sink node it is possible to resend the dropped and modified packets from source to destination.
- The sink can figure out the dropping ratio associated with every sensor node.
- The heuristic ranking algorithms identifies most likely bad nodes from suspiciously bad nodes.

VI. CONCLUSION

The Proposed Scheme is effective in both defecting and filtering packet droppers and modifiers. The bad nodes can be identified by the suspiciously bad nodes. The node categorization and heuristic ranking algorithms are used for this purpose. Extensive simulations have been done to prove the effectiveness of our scheme.

VII. REFERENCES

[1]. Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang and Wensheng Zhang, Catching Packet Droppers And Modifiers In Wireless Sensor Networks, ieee transactions on parallel and distributed systems,vol.23, no. 5,may 2012..

[2]. Bhuse, A. Gupta, and L.Lilien,"DPDSN: Detection of Packet Dropping Attacks for Wireless Sensor Networks," *Proc . Fourth Trusted Internet Workshop*,2005.

Z. Yu and Y. Guan , "A Dynamic En-route Scheme for Filtering False Data in Wireless Sensor Networks,"Proc. IEEE INFOCOM,2006.

[3]. F.Ye,H.Luo,S.Lu,and L.Zhang,"Statistical En-Route Filtering of Injected False Data in Sensor Networks,"Proc.IEEE INFOCOM,2004.

[4]. S.Zhu,S. Setia,S.Jajodia,and P.Ning,"An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data in Senso Networks,"*Proc.IEEE Symp.Security and privacy* ,2004.

[5]. Issa Khalil,Saurabh Bagchi, "MISPAR: Mitigating Stealthy Packet Dropping in Locally–Monitored Multi-hop Wireless Ad Hoc Networks.

[6]. Marti, S.,Giuli, T. J., Lai ,K.,and Baker ,M., Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,. Proc.6th Annual Intl.Conf.on Mobile Computing and Networking (MobiCom.00),Boston,Massachusetts,August 2000,pp 255-265.