A Sequential Analysis based Approach in Wireless Sensor Networks

Punam Borah[1]

Abstract

Security is crucial for wireless sensor networks deployed in hostile environments. The selection of dropping nodes may be random. Identifying such attacks is very difficult and sometimes impossible. Selective forwarding attack is one such attack which is hard to detect. In this paper, the problem of identifying compromised and packet dropping nodes is considered. Two methodologies are presented and analyzed for this purpose. In the first method, the disconnected nodes are detected. In the second method, properly connected nodes are tested with packet transfer from source node to the destination node to identify the random dropping of nodes. Further an effective method for detecting the selective forwarding attack is proposed called the sequential mesh test which helps in the identification of nodes suffering from this attack. It is shown through experiments that this method can provide a higher detection accurate rate and a lower false alarm rate than the existing detection scheme.

Keywords : Malicious nodes, packet dropping, selective forwarding attack, wireless sensor networks.

I. Introduction

wireless sensor networks (WSN) are composed of small sensors that are able to sense some phenomenon in the environment, and communicate the sensed data. Data is wirelessly communicated between sensors until it reaches a central processing unit, referred to as the sink. The node-patterned deployment of WSNs, however, can be the focus of certain types of malicious attack. One such strategy is the selective forwarding attack. Fig. 1 shows an example sensor network under selective forwarding attack.

As shown in Fig. 1, two compromised nodes selectively drop sensitive packets. Two algorithms have been identified and analyzed for identifying the malfunctioning nodes. The first algorithm identifies the disconnected nodes in a network. The second algorithm identifies the nodes causing the random dropping of packets in the network. In selective forwarding attack, a compromised node drops some of the packets for which it needs to relay while forwards other packets.

In this paper, we propose the sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks. The sensor node will need to send the packet drop report message through another path to the cluster head if it does not observe the forwarding data message from the next hop sensor node in a fixed interval.

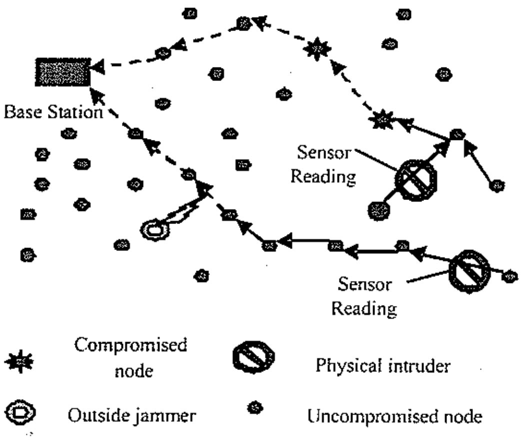

Fig.1 A sensor network under selective forwarding attack

[1] Asst. Prof, Dept. of ISE, SJB Institute of Technology, Bangalore, India. pmborah@gmail.com

The cluster head will run the sequential mesh test based detection scheme against the suspicious node after receiving the packet drop reports. We show through experiments that our scheme can provide a higher detection accurate rate and a lower false alarm rate than the existing detection scheme.

A. Related Work

Several solutions have been proposed to identify and overcome node failures and dropping of packets. One such approach as seen in [1] is based upon their dynamically measured behavior. They use a *watchdog* that identifies misbehaving nodes and a *pathrater* that helps routing protocols avoid these nodes. A lightweight solution called DPDSN [2] identifies paths that drop packets by using alternate paths that WSN finds earlier during route discovery. CHEMAS (CHEckpoint-based Multi-hop Acknowledgement Scheme) [3], is a lightweight security scheme for detecting selective forwarding attacks. Intanagonwiwat et al. [4] proposed the concept of directed diffusion data-centric in that all communication is for named data.

A countermeasure to the selective forwarding attack exists [5] in which a multidataflow topology (MDT) scheme is utilized to defend against the selective forwarding attack. Brown et al. [6] proposed the SPRT scheme for detecting selective forwarding attacks in heterogeneous sensor networks. The scheme utilizes powerful high-end sensors and is based on the sequential probability ratio test. Another security scheme for detecting selective forwarding attacks uses a multi-hop acknowledgement technique [7]. Kaplantzis et al. [8] proposed a centralized intrusion detection scheme. It suggested that the system can detect black hole attacks and selective forwarding attacks. Further [9] shows that there were several studies carried out on the attacks against sensor networks and its countermeasures.

B. Paper Organization

The remainder of this paper is organized as follows. Section 2 gives the overview of the system, showing the various modules that the entire system is made up of. Section 3 outlines the scheme used for generating and reporting packet drops. The Sequential mesh test scheme is presented in Section 4. Performance evaluation is discussed in Section 5. We present our conclusions and future work in Section 6.

II. Overview of System

The important issues in the sensor network are the coverage problem and the successful transmission of data to the base station [16]. The sensors send the collected data within their communication range to the base station without failure. But the base station may not receive all data sent by these nodes due to transmission problems or node malfunctions. Therefore, it is our duty to identify and report the malfunctioning nodes. Fig. 2 shows the overview of the entire system. The system proposed here consists of four basic modules:

Determination of disconnected nodes: The nodes which are compromised and always lead to dropping of packets are identified.

Identification of random packet drops: Apart from the disconnected nodes. There can be several other nodes causing random dropping of packets. These nodes are identified here.

Generation of packet drop reports: For the base station to run tests on accused nodes, nodes causing suspicion needs to be identified. This is done by a source sensor node, which after detecting a suspicious node informs the base station through the packet drop reports.

Sequential Mesh Test: After receiving packet drop reports, the base station runs the sequential mesh test to confirm the accusations and determine whether the node has undergone the selective forwarding attack or not.

A. Determination of Disconnected Nodes

The determination of disconnected nodes helps in the identification of nodes which are compromised and drop all packets that it receives. The identification of these disconnected nodes is accomplished through the use of Algorithm-H. This algorithm is run from the base station which sends broadcast packets to all the nodes. The nodes receiving this packet send an acknowledgement back to the base station. The nodes from which the base station receives acknowledgements are the connected nodes, otherwise they are considered to be disconnected nodes.

Pseudocode for Algorithm-H:

Objective: Determines which sensor nodes in the field are not connected to the sensor network i.e., it finds the holes.

```
Algorithm-H (graph, base)
{
 disconnectedNodes ← empty list
    for each node in graph
      do
          if (node not connected to base station)
          then
              disconnectedNodes←disconnected
               Nodes+node return disconnected
}
```

B. Identification of Random Packet Drops

The identification of random packet drops helps in determining the nodes which are not fully compromised but at times result in dropping of packets randomly [10]. The identification of these random dropping of packets is facilitated through the use of Algorithm-F. The algorithm begins at the source sensor node which needs to send number of packets to the base station. Each time a packet is sent, the counter value is increased. A mismatch of this value between the current node and the previous node at any point of time indicates a random drop of packet in the path.

Pseudocode for Algorithm-F

Objective: Detects if packets were dropped during transmission from a node A to the base station.

```
Algorithm-F (node A, path)
{
        transmit packets from node A to base station
along path
                if (number of packets received !=
packet_count at current node)
        then
return True
        else
return False
}
```

III. Generation Of Packet Drop Reports

For identification of nodes suffering from selective forwarding attacks, the sequential mesh test needs to be executed on the accused nodes [11]. Therefore, the first step here is determining the accused node. The packet dropping reports are generated by the source sensor node, which observes the network closely after sending a packet to its neighbors.

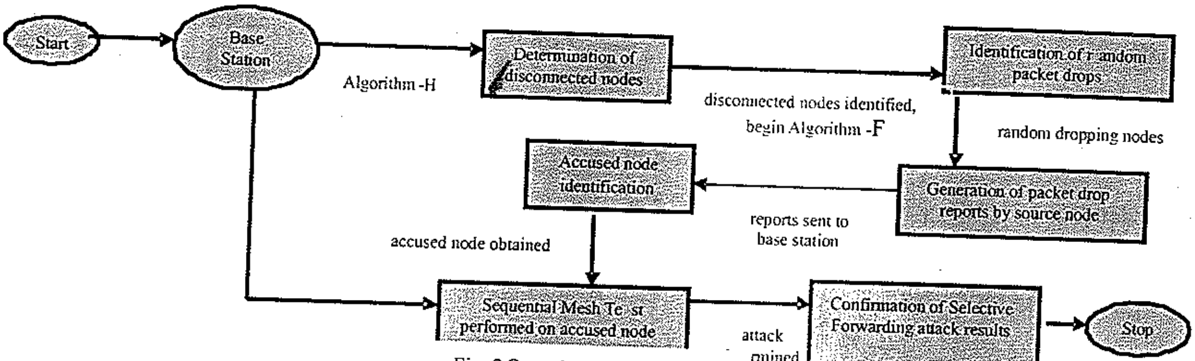
Start
Base Station
Algorithm -H
Determination of disconnected nodes
Identification of r andom packet drops
disconnected nodes identified, begin Algorithm -F
random dropping nodes
Generation of packet drop reports by source node
reports sent to base station
Accused node identification
accused node obtained
Sequential Mesh Te st performed on accused node
attack mined
Confirmation of Selective Forwarding attack results
Stop

Fig. 2 Overview of the system

Alternate paths are selected when a node becomes suspicious and reports of it dropping a packet, is sent to the base station by the source node. These reports are called as the packet dropping reports. Here, the wireless sensor nodes should listen promiscuously to the network after sending their data packets. If the sender node has not observed the forwarding message after a fixed period of time, it can suspect that the intermediate relay node has dropped its packet [12]. Then the sender node will report packet dropping event to the cluster head through another route. Consider the sample scenario shown in Fig. 3.

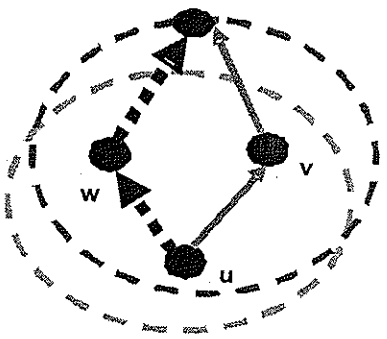

Fig. 3.Monitoring neighbor transmissions

Here, node 'u' is the original sender of the data packet to the base station 'C'. Sensor node u sends data packet to C through intermediate node 'v'. If, after certain interval of time, 'u' does not observe the message to have been forwarded, then it assumes 'v' to be the accused node then it will report this packet dropping event to the base station C through another path u->w->C. Node 'u' now needs to send the ID of the accused node (i.e., node 'v') as well as the packet which was dropped to the base station [13]. The following steps are followed to encrypt the data along with the accused node ID and sent to the base station.

a. Generate key K_{Cu} which is the key shared between node 'u' and the base station 'C'.

b. Encrypt data and ID of 'v' with K_{Cu}, to give $K_{Cu}(data||v)$.

c. 'seq' used is a newly generated sequence number.

d. Encrypted result of step 'b' concatenated with 'seq', to give $K_{Cu}(data||v)||seq$.

e. Resend message obtained in step'd' to 'C' through node 'w'.

f. At node 'w' concatenate the message sent at step 'e' with the ID of the last hop sensor, this gives $seq||K_{Cu}(data||v)||u$.

g. Node 'w' encrypts the message obtained at step 'f' with K_{Cw}, where K_{Cw} is the key shared between node 'w' and C, this gives $K_{Cw}(seq||K_{Cu}(data||v)||u)$.

h. Message obtained at step 'g' sent out until it reaches C.

i. C decrypts the packet drop report obtained layer by layer by using the keys.

j. The included node ID indicates the suspicious selective forwarding attack node.

IV. Sequential Mesh Test

Sequential Mesh Test (SMT) is used to confirm the accusations made on a node under suspicion. After receiving the packet drop reports, the base stations needs to verify whether the accused node has undergone the attack or not [12]. For this purpose the sequential mesh test is used which is a form of statistical analysis wherein based on a predefined rule,

results are obtained. The variable 'p' is used to denote the probability that a node drops a packet. The interval [p_1, p_0] denotes the acceptable probability interval of dropped packets [15].

After the base station receives the packet drop reports, it is able to identify the accused node and hence runs the sequential mesh test on this node to confirm the attack. To perform the sequential mesh test, the following steps are carried out:

a. A number of samples containing the status of packet forwarding need to be collected; this is represented as 'm' samples.

b. A variable 'x' is used where x=1 indicates a successful packet forwarding and x=0 denotes packet drop.

c. Variable 'p' denotes the probability of dropped packets among all forwarding packets.

d. The range specified as [p_1, p_0] denotes the acceptable probability interval of dropped packets.

- If $p>p_0$: Accused node is a selective forwarding attack node.
- If $p<p_1$: Accused node is not a selective forwarding attack node.
- If p1<p<p0: More samples having the status of packet forwarding are required to be collected.

e. The symbol 'α' denotes the acceptable missed detection rate.

f. The symbol 'β' denotes false alarm rate.

g. Further, the detection of selective forwarding attack is transformed into the following hypothesis test:

i. Null hypothesis H_0: $p=p_0$.

ii. Alternative hypothesis H_1: $p=p_1$.

iii. Sequential Mesh Test (SMT) splits the above hypothesis test into two pairs of hypothesis test:

- Null hypothesis H_{01}: $p=p_2$, Alternative hypothesis H_{11}: $p=p_1$.
- Null hypothesis H_{02}: $p=p_0$, Alternative hypothesis H_{12}: $p=p_2$.
- Here $p_2 = 1-((\log(p_0/p_1))/(\log[(p_0(1-p_1))/(p_1(1-p_0))]))$.

h. Let $S_n = \acute{O}^{n}{}_{i=1}\, x_i$ be the times of successfully test until 'n'.

i. Then,

- $a_1 = \log(\beta/(1-\alpha))$, $b_1 = \log((1-\beta)/\alpha)$
- $h_1 = b_1 / \log[(p_2(1-p_1))/(p_1(1-p_2))]$
- $S_1 = [\log((1-p_1)/(1-p_2))]/[\log((p_2(1-p_1))/(p_1(1-p_2)))]$
- $h_2 = b_1 / [\log(p_0(1-p_2))/(p_2(1-p_0))]$
- $S_2 = [\log((1-p_2)/(1-p_0))]/[\log((p_2(1-p_0))/(p_0(1-p_2)))]$

j. SMT starts from n=1 (where 'n' is the number of samples collected, i.e., n = 1....m).

Communications, May 2008.M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science. 1989.

[7] Bo Yu and Bin Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks", Proceedings of the second international workshop on security in systems and networks, IPDS 2006. S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," *IEEE Trans. Neural Networks*, vol. 4, pp. 570–578, July 1993.

[8] Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani and Ahmet Sekercioglu, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Support Vector Machines", 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP).Dec 2007.S. P. Bingulac, "On the compatibility of adaptive controllers (Published Conference Proceedings style)," in *Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory*, New York, 1994, pp. 8–16.

[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", in *Ad Hoc Networks, Vol.* 1, *No.* 2, 2003.W. D. Doyle, "Magnetization reversal in films with biaxial anisotropy," in *1987 Proc. INTERMAG Conf.*, pp. 2.2-1–2.2-6.

[10] Reddy, Y.B, "A Game Theory Approach to Detect Malicious Nodes in Wireless Sensor Networks", Third international conference on Sensor Technologies and Applications, 2009. SENSORCOMM' 09.

[11] Pandarinath P, "Secure Localization with defense against selective forwarding attacks in wireless sensor networks" in 3rd International Conference on Electronics Computer Technology (ICECT), 2011.

[12] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, Wang Liang-min. "Lightweight defense scheme against selective forwarding attacks in wireless sensor networks" in 2009 International Conference on Cyber enabled distributing computing and knowledge discovery.

[13] Lazos, L., Krunz, M., "Selective jamming/ dropping insider attacks in wireless mesh networks", in Network, IEEE, Volume 25, Issue 1, January-February 2011.

[14] Chong Eik Loo, Mun Yong Ng, Christopher Leckie & Marimuthu Palaniswami, "Intrusion Detection for Routing Attacks in Sensor Networks", in International Journal of Distributed Sensor Networks, Volume 2 Issue 4.

[15] A. Wald, Sequential Analysis, Wiley, 1947.

[16] http://www.sensor-networks.org/

[17] http://www.wsn-security.info/

Author's Biography

Punam Borah received his Bachelor of Engineering degree in Electronics and Instrumentation Engineering from Annamalai University in Chidambaram, Tamil Nadu and Master of Engineering in Information Technology from Rajiv Gandhi Technical University in Bhopal, Madhya Pradesh in 2002 and 2006 respectively. He is currently working as an Asst. Professor in the Department of Information Science and Engineering, SJB Institute of Technology in Bangalore, Karnataka. His research interests include Security Issues in Wireless Sensor Networks and Cloud Computing. He has participated and presented technical papers in various national and international level conferences.