AN INTRUSION DETECTION MECHANISM FOR WIRELESS SENSOR NETWORKS

Allen M. Mathew[1], Anita K.A[2], Christy Thomas Mathew[3], Jeleena Joseph[4]
Department of Computer Science and Engineering, Amal Jyothi College of Engineering, Kottayam, Kerala

Abstract: Wireless sensor networks are very prone to attacks both physically and logically, since it is usually used in hostile places that needs constant surveillance against intruders. Using several existing techniques, we have ways to tolerate or mitigate packet dropping or packet modification attacks however, they do not give an idea of where the attack occurs. In this paper, we propose an intrusion detection mechanism which describes the key sharing process and how it is possible to deal with such attacks and be able to track the position of the intrusion.
Index Terms: Packet dropping, packet modification, intrusion detection, wireless sensor networks.

I. INTRODUCTION

Sensor nodes are used to collect data from areas where manual collection of data is not possible or difficult. In a wireless sensor network, sensor nodes monitor the environment variables, detect events, produce data and collaborate with other sensor nodes in getting the information to reach the sink, which acts like a gateway, base station, storage node or simply a querying user. These sensor nodes are usually easy to deploy and has the capability of self-organization which can be used in an unattended and hostile environment to perform the monitoring and data collection functions. However, these sensor nodes lack physical protection and can easily be compromised by an intruder. After compromising one or more multiple sensor nodes, the intruder can launch several attacks and ultimately cause havoc. The two most common attacks in wireless sensor networks are dropping packets and modifying packets. By dropping packets and modifying packets sent by a sensor node, an adversary can compromise the system integrity and the adversary can infiltrate the base without being detected. A widely adopted counter measure to deal with packet droppers is multipath forwarding [2], [3], in which each packet is forwarded along multiple redundant paths, so that we have multiple copies of the same data from a single node and hence even if packet dropping occur in some nodes, the true data is not lost completely. However, the same property of multipath forwarding can be used by an adversary if they have compromised two or more nodes and the malicious data packets outnumbers the no. of packets containing true data.To deal with packet modifiers, most of the existing countermeasures [4], [5], propose to filter the modified messages within a certain number of hops. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and we have no way of identifying just where the infiltration has taken place. To deal with the problem of locating the intrusion point, it has been proposed in [6], that nodes must continuously monitor the message forwarding behaviors of their neighbors to determine if their neighbors are misbehaving, and the approach can be extended by using the reputation based mechanisms to allow nodes to infer whether a non-neighbor node is trustable or not [7]. However, this method may cost high energy requirement by the promiscuous operating mode of wireless interface. The reputation mechanisms have to be used with cautions to avoid or mitigate bad mouth attacks and similar attacks. In this paper, we proposean intrusion detection mechanism for wireless sensor networks which when used in conjunction with the node categorization algorithm and ranking system as described in [1], we can make the communication among the nodes secure and resilient to most of the common attacks.

II. SYSTEM MODEL

A. Network Assumptions

Consider awireless sensor network consisting of a large number of sensor nodes that are randomly deployed in a two dimensional area, distributed non-uniformly. Each sensor node generates data packets periodically and all of them collaborate to forward the packets towards the sink, which is located within the network. We assume all sensor nodes and sink are loosely time synchronized. The sink is aware of the network topology, which can be achieved by requiring nodes to report their neighboring nodes right after the deployment.

B. Security Assumptions and Attack Model

We assume that the sink in the network is a highly secured system which can be trusted and is free of compromise. It is assumed that the adversary cannot successfully compromise the sensor nodes during the topology establishment phase shortly after the network is deployed. Compromised nodes may or may not collude with each other. A compromised node can launch the following two attacks:

- Packet Dropping: A compromised node may drop 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 framing innocent nodes.
- 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. PROPOSED SCHEME

In this scheme, first of all a routing tree rooted at the sink is established. The sensor nodes communicate sensor data with its parent node only and follows a single direction of transmission. Each sensor node collects data and forwards the message in the form of packets toward the sink. Each sender or forwarder has its own private key which it uses to encrypt the message and forwards it. The collection of public keys of all nodes installed is stored at the sink only. This makes it very difficult to perform a masquerade or packet modification attack. Packets that cannot be decrypted using the sender's public key is regarded as bad packets. Such bad packets are dropped and the dropping ratio associated with every sensor node are calculated. Then the node categorization algorithm as proposed in [1], can be used to identify nodes that are droppers/modifiers for sure or are suspicious ones. Over time, the tree structure dynamically changes every time interval and behaviors of sensor nodes can be observed in a large variety of scenarios. As the information of node behaviors has been accumulated, the sink periodically runs the proposed heuristic ranking algorithms to identify most likely bad nodes from suspiciously bad nodes. This way, we can get an accurate rating for a node based on its behavior with small false positive.

The three main stages in the proposed system for intrusion detection are: DAG establishment and Initialization, Data Exchange and, Node categorization and ranking.

3.1 DAG Establishment and Initialization

On deploying the wireless sensor nodes, the first thing for these nodes to do is to identify a path toward the sink. The nodes look for the shortest route towards the sink, using any of the shortest path algorithms. However, a change in this conventional method is that we consider two or more alternate paths other than the shortest path and call them alternate paths. These alternate paths are chosen at random after every time interval, which makes it difficult for the intruder to guess and attack a specific node to cause a complete blackout in one of the tree structure of the sensor network. Next step is to exchange keys and let the sink know the public key of all the nodes. For this, we need to send an initialization message from each node to the sink. The initialization message consists of the initialization code and an encrypted block of data which consists of the sending node's identification and its public key, encrypted using a highly secure 256-bit key known as the initialization key. The pair of public key and private key of each node is generated randomly and prepared before the next initialization message is to be sent. So after all the nodes have sent initialization message to the sink, the sink will have the public keys of all the nodes. All the public keys are stored in the sink simply because, it is the most secure place to unpack and process data in the wireless sensor network. During this process, the tree topology of the sensor network can also be resolved at the sink, by tracing the intermediate nodes to the sender node.

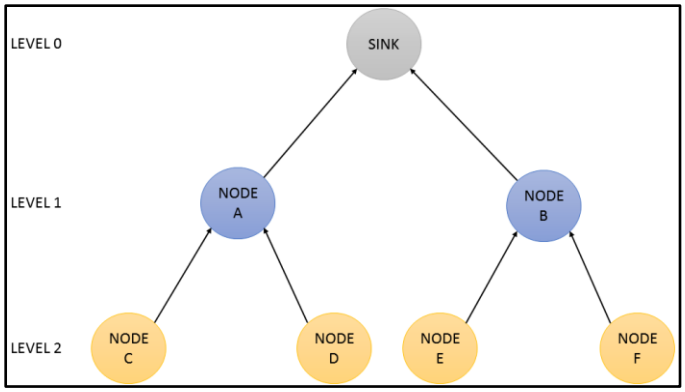

Fig. 1: Tree Topology of a simple wireless sensor network.

3.2 Sender Node

The primary function of a sensor node is to work as a sender node i.e., collect data, pack it and forward the packet toward the sink. Its secondary function is to act as an intermediate node i.e., receive an incoming packet and send it toward the sink. As a sender node, the node encrypts the collected data using its private key and pack the message in an IP packet whose header consists of the sender's ID and other details. Every node will have only one parent at any given time and it will forward all message packets to their parent. Since the parent node changes on every periodic initialization, even if one of the path is blocked for a node, the node can overcome this by using one of the alternate paths.

3.3 Intermediate node

As an intermediate node, the node receives an incoming packet and then encrypt the whole packet using the intermediate node's private key. The encrypted packet is then encapsulated in another IP packet with the header containing the intermediate node's ID. The encapsulation is done so that the data sent by the sender remains intact, such that no manipulation is done by the intermediate node. The same procedure is followed at each of the following intermediate nodes. A point to be noted is that the intermediate nodes do not perform any encryption on the received initialization message packets but simply encapsulates it in another packet with the header containing the intermediate node's ID and forwards it directly to its parent.

3.4 Sink

When the sink receives a packet, it first looks at the IP header to identify the sender. The public key of that sender is used to decrypt the message. There are two possibilities, either the decrypted message contains sensor data or contains another packet containing yet another encrypted message. The above steps are done repeatedly until we can recover the sensor data. While unpacking a message from a packet, if the decryption process fails, then we can say the packet we received from that sender is a bad packet. Bad packets are those packets that cannot be used to recover data using the sender's public key, probably because the data had been corrupted or manipulated by an adversary.

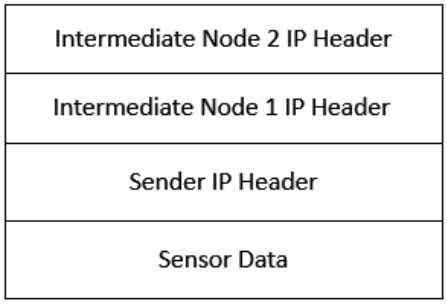

Fig. 2: An example of how sensor data is packed after passing through two intermediate nodes.

Dropped packets can be easily recognized by keeping track of the sequence number of packets received and the no. of flips in the sequence numbers of these packets. At the end of each round, the sink calculates the dropping ratio for each node u. Suppose$n_{\mathrm{u,max}}$ is the most recently seen sequence number, $n_{\mathrm{u,flip}}$ isthe number of sequence number flips, and $n_{\mathrm{u,rcv}}$ is thenumber of received packets. The dropping ratio in thisround is calculated as follows:

$$d_u = \frac{n_{u,flip} * N_s + n_{u,max} + 1 - n_{u,rcv}}{n_{u,flip} * N_s + n_{u,max} + 1} \quad (1)$$

3.5 Node Categorization and Ranking

Based on the dropping ratio of every sensor node and thetree topology, the sink identifies the nodes that are droppersfor sure and that are possibly droppers.The categorization of nodes can be done using the algorithm described in [1] by Chuang et. al. They also propose an algorithm for ranking the suspiciously bad nodes according to the dropping ratio.With this information, we can say which node has been compromised and be able to send warning to the concerned people.

IV. CONCLUSION

The use of wireless sensor networks can be for a wide variety of applications. When it comes to applications where sensor node security is vital, we need to implement the best suite of security mechanisms. Using the mechanism proposed in this paper, we would be able to effectively detect and identify nodes that have been compromised by an intruder in a wireless sensor network, which is the main advantage of the system. Inter-node communication overhead is minimum and involves a simple pack and forward manner. Packing packets at each nodes makes the message more secure and difficult to crack. Also it helps the sink identify the path through which the original packet has travelled.

Acknowledgment

We would like to express our sincere gratitude towards Prof Ashji S Raj, CSE dept., Amal Jyothi College of Engineering, Kottayam, who guided us throughout this project.

REFERENCES

[1] Chuang Wang, Taiming Feng, Jinsook Kim and Guiling Wang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 5, May 2012.

[2] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003.

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

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

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

[6] R. Roman, J. Zhou, and J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks," Proc. IEEE Third Consumer Comm. Networking Conf. (CCNC), 2006.

[7] S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation- Based Framework for High Integrity Sensor Networks," ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, 2008.

