An Enhanced Scheme of Excluding Compromised Nodes in Wireless Sensor Networks

Aparnaa M\textsuperscript{1}, Dhanush Krishna S\textsuperscript{2}, Sibi Amaran\textsuperscript{3}, Maheswari S\textsuperscript{4} and Soundarya R\textsuperscript{5}

\textsuperscript{1}\textsuperscript{2}\textsuperscript{3}\textsuperscript{4}\textsuperscript{5}SRM INSTITUTE OF SCIENCE AND TECHNOLOGY, CHENNAI
johnpaulreddy875@gmail.com

Abstract— Any system or network is always susceptible to attacks. If an adversary has access to the network, they may disrupt the network in several ways. Sybil attack, selective forwarding, tampering, etc., are some of the attacks that disrupt the network. If the sensor network is employed in critical areas such as warzones or border protection systems, any attack or breach of security may prove to be fatal. Therefore, proper security mechanisms have to be integrated into the system to ensure that the data remains secure. In our project, we intend to identify and isolate the compromised nodes that selectively forwards data packets. The proposed protocol uses a reputation based system to determine the integrity of the neighboring nodes. Once a compromised node has been identified, that node is excluded from further communication after verification from base station.

Keywords- CBRP-Reputation Based System-Selective Forwarding Attack-Node Revocation

1. INTRODUCTION

Wireless sensor network consists of large number of nodes that are deployed to monitor the physical or environmental conditions. The collected data is then sent to the sink or to the base station, where it is organized and used for the specified purpose. An adversary may take control of nodes and launch attacks on behalf of it, with the intent to either disrupt the working of the network or collect data. These attacks can be of two types namely Active and Passive attacks. The active attacks involve directly interacting and disrupting the network. Passive attacks involves in collecting information. Passive attacks are sometimes a preliminary phase in an active attack. Some of the active attacks that are used are black hole, selective forwarding, Sybil attack, wormhole attack, etc. Several counter measures have been developed over the years to identify the compromised nodes. To ensure that the damage caused by the attack is minimum, it is important to identify the nodes and revoke them as soon as possible.

2. RELATED WORKS

A. Detecting Compromised Nodes In Wireless Sensor Networks

Matthews, Song and Shetty proposed an algorithm that was based on identifying the compromised nodes by analyzing the time taken by the packets to arrive. Each node maintains a table that contains the node_ID and the maximum and minimum time taken by the nodes to transfer the packets. It also keeps a buffer containing the last few transaction times of the packets the node sent. When a node sends a packet to another node, it checks if the packet arrival time is between the highest and lowest arrival times of that node. If the arrival time does not fall between these two values, the node sends an alert message to the base station. The base station then requests the transmission buffer of the suspected node. If the values are found to be inconsistent, the base station labels the node as compromised and sends a broadcast message informing the nodes of the same. Once a node receives the broadcast message, it clears out all entries of that node and adds the node_ID to the compromised list.

If it is found that the node isn't compromised, then it informs the node, which then updates the time based on the value. While this algorithm produced no false positives, the time taken for detection increased with increased network size. This also places a huge load on the base station.

B. Node Compromise Detection Based On Nodetrust In Wireless Sensor Networks
Thaile and Ramaniah proposed a scheme called Node Trust. This scheme eliminated false positives with substantial reduction in detection overhead. In this scheme, each node is given a unique ID and the given area is divided into a number of zones. The deployment of sensor nodes in the zones is decided based on the results obtained by modulo of the node’s ID with the number of zones. The node with the smallest ID form each zone in the chosen as zone head and placed near the base station. Once the zone head selection is complete, each node is requested to send a packet to its respective zone head within a fixed time interval. If a node fails to send a packet within the fixed time interval, it is considered as untrust. The base station then proceeds to perform software attestation using MD-5 hash algorithm to determine the software’s integrity. If the base station finds any alteration in the integrity of the software, then that particular node is considered to be compromised. Revocation is either done manually by replacing it or re-configuring it with the help of a high computing machine or the base station.

C. AICN: An Efficient Algorithm To Identify Compromised Nodes In Wireless Sensor Network

This algorithm developed by Lu,Ling, Zhang,Zhoh and Sher uses the sink to identify the compromised node. Based on trust assumptions, it is concluded that a sensor node always tells the truth and a compromised node tells the truth with half the probability. The sink first arranges the nodes in an array and asks all the nodes to report whether they think their neighbor is a compromised node or not. If a node sends a report stating that it thinks that its neighbor is a compromised node, the sink moves the pair to another set. By conducting a set of queries on the nodes in the other set, the sink identifies the compromised nodes.

An improved version of the same algorithm was used for comparison and analysis to demonstrate efficiency.

D. Compromised Sensor Nodes Detection: A Quantitative Approach

Li, Song and Alam make use of a DTQ function to differentiate the compromised and legitimate nodes. This function measures the communication quality of the node. Each node maintains a table containing DTQ values of some nodes in the group along with its time stamp. This function uses four variables as input to the DTQ function. They are: the total energy cost in transmitting a data burst, the total number of data packets that have been transmitted successfully, the expected probability of the successful data transmission and the stability of the sensor node. During communication, an ACK packet is sent by either the destination node or the node that belongs to the next group in the route to the source node. This helps in identifying the packet drop. Once the source node identifies the packet drop, it changes the DTQ values of all the nodes in that routes that belong to that particular group. If one or more nodes have DTQ values below the threshold, it is assumed that there is a compromised node in the group. A voting procedure identifies the compromised nodes. This method has a tradeoff between group size and detection performance.

3. SECURITY MECHANISM

To identify a compromised node, several schemes have been developed over the recent years. One such scheme is to identify a compromised node based on its behavior. This is achieved with the help of a reputation system. Reputation is evaluating the trustworthiness of a node by monitoring its actions. This can be done by either the neighboring nodes or separate nodes that are employed for monitoring known as watchdogs. These values decrease and increase based on the behavior of the node. These values can be used to select CH, which leads to the election of an optimal and safe CH.

4. SYSTEM MODEL

The system consists of a number of nodes distributed uniformly around the base station. The sensors have a uniform sensing range. The sensors have necessary cryptographic primitives for optimal
operation. It is assumed that the base station is the most trusted unit and cannot be compromised by any attacks.

![Network Architecture](image)

**Fig. 1 Network Architecture**

5. IMPLEMENTATION:

The proposed protocol can be divided into three phases. The three phases are as follows:
- Network Deployment
- Updating Reputation Table
- Compromised Node Isolation

![Flow Chart of protocol](image)

**Fig. 2 Flow Chart of protocol**

A. **Network Deployment**

Each node maintains a neighbor table that contains information about its neighbors obtained by sending out LIVE messages. Initially the nodes with high energy levels are elected as Cluster Heads (CH). The CHs then send out HELLO messages announcing its presence. The nodes that receive the
message send one back and become members of that cluster. If a node is part of a cluster and receives a HELLO message from another CH, it becomes a gateway. When a source node has to send data to a destination node, it first checks the neighbor table. If it is not found, it sends route request to CH. The CH checks whether the destination is a part of the cluster. If the destination is not in the cluster, the CH sends route request to the CHs in its neighbor table. When the packet reaches the destination, it sends the message of finding route in reverse. Source node updates the route once it receives.

B. Updating Reputation Table

Once the nodes start communicating, each node maintains a reputation table for each of its neighbor nodes. Nodes assign reputation to each of their neighbor based on their behavior. The values that are chosen to determine the trustworthiness of the node are totally available information to reduce computational overhead and energy loss. The proposed protocols uses the information obtained from the data packets. When the node sends a series of packets to a destination it includes the number of packets it is forwarding and the packet ID in each packet. It also includes a counter value that is updates at each node. This helps in identifying the node that caused the packet drop. If the number of packets received is less than the number of packets that are supposed to arrive, the node checks the packet ID for discontinuity. The node decreases the reputation value.

C. Compromised Node Isolation

Once a node finds that one of its neighboring nodes has a reputation value lower than a particular threshold, the node sends the node ID to the CH. The CH collects the reputation value of the suspected compromised node from all its neighbors and sends it to the Base Station. The Base Station then analyze all the reputation values and considers the node as compromised if majority of the reputation values are below the threshold. If not, then the base station sends packets through several routes involving the suspected node. The Base Station then analyzes the updated reputation values and labels the nodes as compromised if there are more reputation values that have a negative change. The base station alerts the CH to add the node to the reject list. The CH sends a message to all the nodes that are neighbors of the compromised node so that they can add that node to the reject list. The other CHs and gateways are also intimated about the compromised node. The nodes reject any packet forwarded by the CH and it also refuses to forward any packets to the compromised node.

6. SIMULATION

The simulation results showed a significant decrease in packet drop ratio when the proposed scheme was applied.

| Number of sensor nodes | Packet drop ratio |
|------------------------|-------------------|
|                        | Without Scheme    | With Scheme      |
| 10-20                  | 0.02-0.033        | 0.01-0.02        |
| 20-40                  | 0.026-0.056       | 0.015-0.03       |
| 40-60                  | 0.040-0.05        | 0.018-0.025      |

Table 1: Packet Drop Ratio
7. CONCLUSION
We have presented an innovative approach to exclude compromised nodes involving in selective forwarding attacks in a wireless sensor network. The approach makes use of an reputation based system to identify the compromised nodes and then prevents the remaining nodes from communicating with it once the base station verifies the genuineness of the node.

8. REFERENCES
[1] Rongxing Lu, Xiaodong Lin, Chenxi Zhang, Haojin Zhu, Pin-Han Ho and Xuemin (Sherman) Shen, "AICN: An Efficient Algorithm to Identify Compromised Nodes in Wireless Sensor Network", Proceedings of IEEE International Conference on Communications, ICC 2008, Beijing, China, May 2008.
[2] Mary Mathews, Min Song, Sachin Shetty, Rick McKenzie, "Detecting Compromised Nodes in Wireless Sensor Networks", Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Norfolk, VA, Aug 2007.
[3] Tao Li, Min Song, Mansoor Alam, "Compromised Sensor Nodes Detection: A Quantitative Approach", The 28th International Conference on Distributed Computing Systems Workshops, Toledo, June 2008.
[4] Manyam Thaile, O.B.V. Ramaiah, "Node Compromise Detection Based on Node Trust in Wireless Sensor Networks", International Conference on Computer Communication and Informatics (ICCCI -2016), Coimbatore, India, Jan 2016.
[5] Alma Oracevic1 Serkan Akbaş, Suat Özdemir, Mladen Kos”, Secure Target Detection and Tracking in Mission Critical Wireless Sensor Networks”, Macao, China, Dec. 2014.
[6] Mohamed-Lamine Messai,”Classification of Attacks in Wireless Sensor Networks”, International Congress on Telecommunication and Applications, Setif, Algeria, 2014
[7] Waldir Ribeiro Pires Júnior, Thiago H. de Paula Figueiredo Hao Chi Wong, Antonio A.F. Loureiro,’Malicious Node Detection in Wireless Sensor Networks’, 18th International Conference on Distributed Computing Systems, Santa Fe, NM, USA, April 2004.
[8] Mary G Baker, Sorav Bansal,”Observation-based Cooperation Enforcement in Ad Hoc Network”, Networking and Internet Architecture (cs.NI), Stanford, CA, USA, July 2013
[9] P.Parvathi,”Comparative Analysis of CBRP, AODV, DSDV Routing Protocols in Mobile Ad-hoc Networks”, 2012 International Conference on Computing, Communication and Applications, Dindigul, Tamil Nadu, India, Feb. 2012.
[10] Udaya Suriya Rajkumar.D, Rajamani Vayanaperumal,”Detecting and Revocation the Compromised Node in Zone - Based Wireless Sensor Network Using a Two Stage Approach”, Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, August 2014