Detection of Replica Node Attack In Wireless Sensor Networks Using Hierarchical Approach

Rajashekhar V Baraker

Assistant Professor Dept of computer science

Karnatak Science College Dharwad

India

Abstract - The detection and isolation of compromised nodes in wireless sensor networks is a difficult task. However, failure to identify and isolate compromised nodes results in significant security breaches which lowers the integrity of gathered data. In this paper we propose a replica node detection scheme using a hierarchy-based framework. All the hierarchical routing protocols work on the idea of electing a cluster head. We make use of a location-aware cluster formation algorithm that detects and isolates compromised nodes. Our scheme provides a mechanism for exchanging node location in their present cluster to the base station so that base station can determine whether the nodes have been compromised, and take corrective action. Base station broadcasts the replica node information to cluster heads. The cluster heads can further eliminate the replicas by not allocating them the transmission schedule. The effectiveness of our approach in the detection and isolation of compromise nodes is validated through simulation.

Keywords- sensor networks; replica node attack; security in wireless sensor networks; hierarchical routing.

Introduction- Generally a Wireless Sensor Network (WSN) is composed of a large number of wireless sensors for monitoring a certain environment. Wireless Sensor Networks consists of very small sensors that are characterized by limited processing power and energy resources. The large number of nodes and their random placement in space offers great redundancy in data transmission. Consequently WSN are generally adaptive networks that use data aggregation and hierarchy to reduce energy consumption. WSNs are used in various domains like military applications, medical engineering, and industrial task automation.

Wireless sensor networks are emerging as very important tool in gathering and dissemination of mission critical information in real time. As a result of the importance and usefulness of the data that will traverse these networks, it is necessary that sufficient security is in place to prevent the leakage or compromise of this data. For economic viability, wireless sensor nodes are limited in power, computation capabilities and memory. The limitation of memory and processing capabilities makes public key cryptography and digital signature infeasible. In addition, the limited power of

these tiny sensor nodes makes the communication overhead of traditional security algorithms unbearable. Furthermore, the lack of infrastructure, the insecure nature of wireless communication channel, and the hostile deployment environments present additional security vulnerabilities.

Hierarchical Routing Protocols

The main idea behind hierarchical routing is to reduce the energy consumption of every node. Clusters are created and a head node is assigned to each cluster. The head nodes are the leaders of their groups having responsibilities like collection and aggregation of the data from their respective clusters and transmitting the aggregated data to the BS. This data aggregation in the head nodes greatly reduces energy consumption in the network by minimizing the total data messages to be sent to BS. Lesser the energy consumption more is the network life time. The main idea of developing cluster-based routing protocols is to reduce the network traffic toward the sink. This method of clustering may introduce overhead due to the cluster configuration and maintenance, but it has been demonstrated that cluster-based protocols exhibit better energy consumption and performance when compared to flat network topologies for large-scale WSNs.

There are different hierarchical routing protocols like, LEACH: (Low Energy Adaptive Clustering Hierarchy), Threshold sensitive Energy Efficient sensor Network protocol (TEEN), Adaptive Threshold sensitive Energy Efficient sensor Network protocol (APTEEN), Energy Efficient Clustering Scheme (EECS), Hybrid Energy-Efficient Distributed Clustering (or HEED), Power-Efficient Gathering in Sensor Information Systems (PEGASIS). All the hierarchical routing protocols work on the basic idea of electing the cluster head. These protocols only differ in the procedure followed for the election of cluster head. It is the duty of cluster heads to allocate the transmission time slots to the nodes in their cluster.

Problem statement: A replica node R1 is defined as the node having same ID and other keying materials of the node R. An attacker first compromises the node R and extracts all the information from it. Replica node R1 is created with the properties extracted from node R. There can be more than one replica with the same properties.

Goal: The model should be able to determine that both R & R1 are two separate nodes using same identity, by making use of hierarchical approach.

Hierarchical approach is used to provide the decentralization of control. This feature supports the fact that, sensor networks do not have a centralized control over the network. Once nodes are deployed, they will be working on their own without intervention. The same code will be running on all the nodes so, all nodes do have capabilities to distinguish the replica node.

DESCRIPTION OF THE PROTOCOL

The hierarchical routing protocol considered is LEACH. Leach provides many good features for the network. It provides a clustered hierarchy, localized coordination and randomized rotation of cluster head. Leach is able to increase the lifetime of the network by sending aggregate of the data. It works as both MAC layer and Network layer protocol.

It operates in two phases, a setup phase and a steady phase. The selection of the cluster heads and the formation of the cluster take place in the setup phase. In the steady phase actual data transfer to the sink takes place.

In the setup phase the leader election takes place and the heads are changed over time. To make a decision about the cluster head formation, every node selects a random number between 0 and 1. If this number is greater than the threshold, the node is selected as the cluster head for the current round. The threshold value is calculated as,

$$T(n)=\begin{cases}\dfrac{p}{1-p*\left(r \bmod \frac{1}{p}\right)} & \text{if } n\in G\\ 0 & \text{others}\end{cases}$$

Where,

T(n) – the threshold value.

p- Fraction or percentage of number of cluster heads for the current round.

r- is the current round

G- is the set of the nodes that have not been cluster heads in the past 1/p rounds.

The protocol makes use of 3 types of messages,

1. ADVERTIZEMENT

2. JOIN REQ

3. SCHEDULE

ADV and JOIN REQ messages are used in the setup phase to form a cluster. Once a node is chosen as cluster head, it advertises itself by making use of ADV messages. A node may receive ADV messages from more than one cluster heads. Now the node verifies the signal strength of the cluster head node and sends a join request. The join request is sent only to the cluster head with higher signal strength.

To calculate the received signal strength we make use of the formula,

$$Pr=Pt*Gr*\ Gt*(1/(4*\pi*d))^2$$

where,

Gt : transmitter antenna gain (mostly 1),

Gr: receiver antenna gain (mostly 1)

Pt: transmit power,

distance : $d= (X2-X1)^2+(Y2-Y1)^2$

- A node wishing to join a cluster may do so by making use of JOIN REQ message. While sending the join request the node is forced to enter its

location information along with its node id which will be stored in the child list of cluster head node (CH). The typical format of join request sent to cluster head node will be,

- send(MAC_BROADCAST,
  currentCHMAC_,
  currentCH_,LEACH_JOIN_REQ,
  (char *) (&nodeId), sizeof(int),
  dataSize, config_.maxDist_,
  code_,
  dist_,
  loc_x,loc_y);

In the steady phase, cluster head forwards the child list to the base station.

- send(
  MAC_BROADCAST,
  destination_id_,
  LEACH_DATA,
  sensedData_,
  dataSize,
  bsDist_,
  config_.bsCode_
  child_list);

Base station receives such child list from all the cluster head nodes. All the lists received are compared with each other for presence of the replica nodes. The base station broadcasts list of replica nodes to the cluster heads. Then the cluster head creates TDMA time schedules for the nodes in the cluster and assigns the time slot. Each node waits for its turn to transmit the data. The replicas will be eliminated by not allocating them the time slot, providing a way for isolation of replica nodes. Periodically cluster head creates an aggregate packet and forwards it to the sink node. This aggregate packet is based on all the data received by the cluster member nodes.

Leach provides many good features for the network. It provides a clustered hierarchy, localized coordination and randomized rotation of cluster head. Leach is able to increase the lifetime of the network by sending aggregate of the data.

Simulation and results

The proposed model is simulated in Network Simulator-2. Temperature, Carbon monoxide, humidity, winds peed Data generators are used to provide the sensed data values to the nodes. Simulation is carried out on a set of 100 nodes and a base station. Every node runs on the same code.

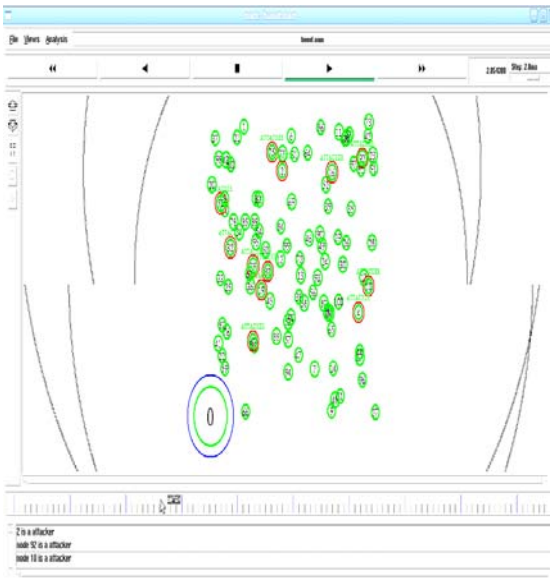

Fig 1. Replica nodes

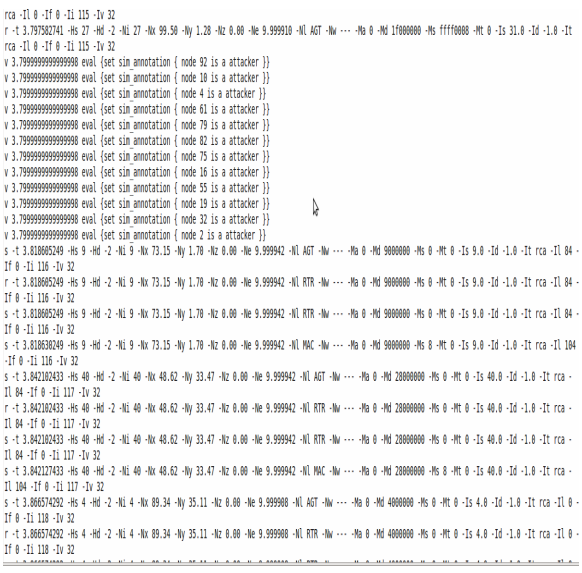

Fig 2. List of replica nodes.

The main issue in wireless sensor networks is node energy since nodes are discarded once they run out of energy. Nodes that had become cluster heads will consume more energy as compared to other nodes.

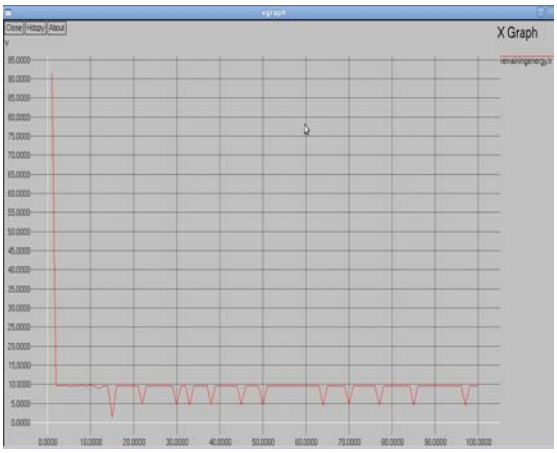

Fig 3. Remaining node energy

Fig 4. Time schedule allocation

Inference

From the above figures we can infer that, the hierarchical model can be made use of efficiently to detect the replica nodes. It can also be observed that, the number of messages exchanged, specifically to detect the replica node are less. Since leach is a hierarchical routing protocol the nodes which had become leader heads would consume more energy than the other nodes.

CONCLUSION AND FUTURE WORK

The characteristic behavior of the sensor networks is studied by making use of temperature, carbon monoxide, wind speed, humidity data generator applications and MD5 algorithm is used to provide identity based keys to the sensor nodes. An attacker model is considered to have same id and key as that of the original node but with different location.

A counter-measure to replica node attack is presented by making use of the hierarchical approach. It enhances the network lifetime by the cluster head formation. Nodes involved in the detection are cluster head nodes and the base station. This increases overall energy efficiency of the nodes. Periodically election is carried out among the nodes. Node with the higher threshold becomes the cluster head. Nodes wishing to join a cluster are made to register themselves with their location information. Each cluster head node is made to forward the child list to the base station. The nodes with same id's but different locations are marked as replica nodes. The detected replica nodes are eliminated by not allocating the time slot for transmission. The effectiveness of the model is depicted using simulation results.

Wireless sensor network applications are increasing day by day. With the constraints on battery life of nodes, the area is one of the hot research topics and needs more improvements. The replica node detection scheme can be further enhanced by making use of more levels of clusters to reduce the energy consumption.

The proposed model can be applied over all other hierarchical routing protocols with no or very less modifications. The stress is given on a framework rather on a particular protocol.

References

[1] Misic and Misic: Wireless Personal Area Networks: Performance, Interconnection, and Security with IEEE 802.15.4 , January 2008.

[2]Akyildiz I F, Weilian Su, Sankarasubramaniam Y, and Cayirci E. "A surveyon sensor networks," *IEEE Communication Magazine*, Page(s): 102 – 114. 2002.

[3] V.Manjula and Dr.C.Chellappan, "The Replication Attack in wireless Sensor Networks: Analysis & Defenses" , CCIST 2011, Communications in Computer and Information Science, Volume 132, Advances in Networks and Communications, Part II, Pages 169-178.

[4] Zubair A. Baig "Distributed Denial of Service Attack Detection in Wireless Sensor Networks", 2008, thesis.

[5] Parno B, Perrig A, Gligor V. "Distributed Detection of Node Replication Attacks in Sensor Networks" In: Proceedings of the IEEE Symposium on Security and Privacy; 2005. p. 49 – 63.

[6] T. Ghosh, N. Pissinou, and K. Makki, Collaborative trust-based secure routing against colluding malicious nodes in multi-hop ad hoc networks," AnnualConference on Local Computer Networks (LCN), pp.224-231, Tampa, USA, 2004.

[7] Hemanta Kumar Kalita and Avijit Kar, "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009.

[8] C. Karlof, and D. Wagner, "Secure routing in wireless sensor networks: Attacks and counter measures," *First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113-127,2003.

AUTHORS PROFILE

Rajashekhar V Baraker

Assistant professor

Dept of computer science

Karnataka Science College Dharwad

India

rajshekhar.baraker@gmail.com