Azerbaijan Journal of High Performance Computing, Vol 3, Issue 2, 2020, pp. 181-189
https://doi.org/10.32010/26166127.2020.3.2.181.189

Intrusion Detection Framework for Geo-Sensor Network

Tapalina Bhattasali

St. Xavier's College (Autonomous), Kolkata, India, tapalina@sxccal.edu

*Correspondence: Tapalina Bhattasali, St. Xavier's College (Autonomous), Kolkata,India, tapalina@sxccal.edu

Abstract

Wireless Geo-Sensor Network is suitable for critical applications in hostile environments due to its flexibility in deployment. However, low power geo-sensor nodes are easily compromised by security threats like battery exhaustion attacks, which may give rise to unavoidable circumstances. In this type of attack, the intruder forcefully resists legitimate sensor nodes from going into a low-power sleep state. Consequently battery power of compromised sensor nodes is drained out, and nodes stop working. Due to the limited capacity of sensor nodes, it is challenging to prevent a sensor node from this type of attack that appears as innocent interaction. This paper proposes a conceptual framework of secured geo-sensor network based on a dynamic load distribution mechanism for a heterogeneous environment. It includes a hybrid detection approach using three modules for detection, confirmation, and decision making to reduce the probability of false detection.

Keyword: Wireless Geo-Sensor Network, GEONET, SEGNET, Load Distribution Mechanism, Hybrid Detection Approach.

1. Introduction

Nowadays, natural hazards are increasing due to various reasons such as global warming, climate change, etc. The losses due to these hazards are increasing at an alarming rate. However, these environmental hazards are largely unpredictable and occur within brief periods. Therefore, technology has to be developed to capture relevant signals with minimum monitoring delay. Wireless geo-sensor network is one of the cutting edge technologies that can quickly respond to the rapid changes of sensed data in the surrounding environment.

Most of the deployed wireless geo-sensor networks are used to measure scalar physical phenomena such as temperature, humidity, etc. The low cost and small size of the sensors, coupled with their ability to communicate without any infrastructural support, make them necessary in crisis management. Geo-Sensor network is mainly used for environmental monitoring such as coastal monitoring, ocean exploration, flood management, forest fire detection, habitat monitoring, etc. Geo-Sensor network is useful in environmental hazard management by providing a system that will learn about the phenomena of natural hazards and provide an early warning signal (Yawut, C., & Kilaso, S., 2011, May). In this field, accuracy and response time play a significant role. Therefore, the security of sensor networks becomes very important. However, applications of geo-sensor become useless if the delay due to anomaly is too large. Incorrect or unavailable query results may cause severe damage.

Geo-Sensor network is much more vulnerable to battery exhaustion than conventional networks due to the limited capability of sensors and the lack of centralized monitoring and management in sensor networks. The target of battery exhaustion attack (Stajano, F., & Anderson, R., 1999, April) is to maximize the affected node's power consumption, thereby decreasing its battery life. Maximum security can be achieved by designing an effective intrusion detection framework (Bhattasali, 2012), whose purpose is to provide alerts about the possible intrusion, ideally in time to stop the attack or to mitigate the damage.

The remainder of this paper is organized as follows. Section II explains the problem domain. Section III consists of an outline of the proposed system model. A conclusion follows it in section IV.

2. Security of IoT

According to Marco Conti et. al. (2011) wireless sensor networks represent a particular class of multi-hop ad hoc networks that are developed to control and monitor events and phenomena where research works are still expected to address technical problems ranging from QoS to privacy, security and trust, specialized network scenarios, or the usage of sensor networks in challenging environments.

The nature of geo-sensor network deployment in severe geographical terrains makes it impossible to recharge sensor nodes' battery power. Quick battery depletion leads to sensor nodes' death, and eventual shut-off occurs in the network either fully or partially. The absence of infrastructure also makes it challenging to detect security threats, often resulting in reduced Quality of Service (QoS). If a monitoring sensor node gets affected by an intruder, then the node can behave abnormally, and alarms might be generated at the wrong times. This may lead to incorrect decisions in environmental hazard management. The transmission of critical information may get blocked or may not occur, when a relay node is affected by an attack. As a consequence, rescue operations may get delayed, and emergencies may develop.

Therefore, security solutions are vital for the wider acceptance and use of sensor networks and have to be designed with efficient resource utilization. The need of the day is to design a model for detecting intrusions accurately in an energy-efficient manner. For this reason, a conceptual framework is proposed to extend the lifetime of the network, even in the face of battery exhaustion attack.

3. Proposed Model

In this section, a novel framework has been proposed for detecting intrusion in a wireless geo-sensor network. It uses a cluster-based mechanism (Chen, R. C., Hsieh, C. F., & Huang, Y. F., 2010) in an energy-efficient manner that enhances network scalability and lifetime. In this framework, energy efficiency can be achieved using a load distribution mechanism where low energy nodes are assigned sensing. Dynamic property (Huo, G., & Wang, X., 2008, June) is considered here to overcome the sudden death of sensor nodes.

In the proposed framework, nodes at different layers are categorized into three different types depending on their battery capacity; (i) Base node (ii) Intelligent node (base nodes which are not attached to micro-server),(iii) Simple node. Depending on the functionality, sensor nodes are categorized into the following designations such as Gateway Node (GN), Cluster Owner (CO), Monitor Node (MN), Zone Owner (ZO) and Sensing Node (SN). There are several types of sensing leaf nodes for sensing temperature, humidity, light, pressure, rainfall, wind speed, etc. Participant nodes in the SEGNET model are defined here, depending on their functionality.

GN: One type of base node having high capacity among other nodes.

CO: One type of intelligent node which has maximum energy level, degree (number of nodes within its coverage area), and minimum distance among all neighbors of GN. It acts as the controller of the cluster area. It is capable to take the final decision regarding the intrusion.

MN: One type of intelligent node with minimum distance from cluster owner and maximum energy among all neighboring nodes of cluster owners. It is responsible for checking data flow to analyze network traffic and to detect intrusion.

ZO: One type of intelligent node whose degree is highest among all the neighbors of CO. It can collect sensing data from SN and detect anomalous behavior if any.

SN: One type of simple node for sensing events. Its detection power is disabled.

Some of the assumptions are given below.

- The network is divided into clusters, which are again partitioned into zones.
- Gateway Node acts as an honest gateway to another network or access point.
- Energy contents EIN of intelligent nodes have μ times more energy than simple nodes.

The life-cycle of the nodes includes the following phases.

3.1. Initialization Phase

Geo-Sensor nodes are deployed. GN broadcasts HELLO MESSAGE and its node-id and designation. GN sends a query message to acquire energy status from any node N joining the network and categorizes it according to its response. GN sets the id of the node N and other parameters.

COs are selected. CO adds nodes within its coverage area into its member list. Then MNs are selected for each cluster. ZOs are selected and add nodes within its coverage area into its member list. Pre-loaded detection modules are activated according to the designation of nodes.

Candidates can be selected randomly if more than one fulfills the selection criterion.

3.2. Data Collection Phase

When a query request comes from GN (Heinzelman, W. R., Kulik, J., & Balakrishnan, H., 1999, August), the corresponding sensing node in the sleep state receives a wake-up coin (Falk, R., & Hof, H. J., 2009, June) from its ZO, which collects sensing data packets and checks anomaly. If the anomaly is detected, the corresponding packet is marked as suspected.

3.3. Data Transfer Phase

ZO sends packets towards CO. MN checks for intrusion during traffic flow from ZO to CO. If a real intrusion is detected, a warning ticket is sent to CO for each data packet. If warning tickets are generated for a packet from at least two different MNs, the fake packet is rejected. If the number of warning tickets received within a time interval is greater than the threshold, the sensing node is blocked. If no intrusion is detected, the packet is forwarded to GN.

If GN discovers any new node N in the middle of the duty cycle, it sends a sleep signal to node N.

If behaviour of any sensor node deviates from normal behavior, the reconfiguration procedure takes place, or, after a predefined time-interval, the reconfiguration procedure takes place to avoid complete exhaustion of sensor nodes. During reconfiguration, detection modules of the previously selected nodes are disabled, and currently selected nodes are enabled.

Geo-Sensor network framework is deactivated, when the network lifetime reaches below the threshold value.

Table 1. Data Dictionary

Parameters	Description
G_neibor {}	Set of neighbor nodes of GN.
E_N	Energy level of node N.
E_{GN}	Energy level of GN node.
Intelligent_Nd{ }	Set of intelligent nodes.
Simple_Nd{}	Set of simple nodes.
desig(N_i)	Designation of node N_i.
$Distance_{N,CO}$	Distance between node N and CO.
MIN (Dist_Cneibor{})	Minimum distance from CO among all neighbors of it.
MAX (Eng_Cneibor{})	Maximum energy level among all neighbors of CO.
degree(N)	Number of nodes within the range of node N.

MAX (Deg_Cneibor{})	Maximum degree among all neighbors of CO.
ZO_neibor{}	Set of neighbors of ZO.
MAX (Deg_Gneibor{})	Maximum degree among all neighbors of GN.
Res_Eng(N)	Residual energy of node N.
MAX (RE_Gneibor{})	Maximum residual energy among all GN neighbors.
C_neibor{}	Set of neighbors of CO.
SneiborCO{}	Set of simple node neighbors of CO.
cnt(wakup(tinter))	Number of wake-up coin received within time interval.
Th_Token	Threshold number of tokens.
Th_max	Maximum threshold number of packets.
Th_min	Minimum threshold number of packets.
Th_{ENERGY}	Threshold energy level.
cnt(Warning)	Number of warning tickets generated by one MN within specific time interval.

Procedural Logic of SEGNET

```
1   GN broadcasts its profile and starts timer T.
2   If acknowledgement from N is received within timeout
          add node N to G_ neibor{}.
3   For every N∈G_ neibor{}, GN collects energy $E_N$.
4     If $E_N$ $^1$ $(1/\mu)^*$ $E_{GN}$ then,
            $N_i$ is added to Intelligent_Nd{ }.
    Else $N_i$ is added to Simple_Nd{}.
5     CO_Select ().
6     Cluster_Form().
7     // Selection of Monitor Node
 Set desig($N_i$) as MN, if $Distance_{N,CO}$ = MIN(Dist_Cneibor{})
 and $E_N$ = MAX(Eng_Cneibor{})
8    // Selection of Zone Owner
 Set desig($N_i$) as ZO if degree($N_i$) = MAX(Deg_Cneibor{}).
9   // Zone form within coverage area of ZO
        ZO collects its neighbor ids into ZO_neibor{}.
10   Collect_Info().
11   Forward Packets to CO.
```

```
12  Confirm_Intrusion ().
13  Action().
14  ENDFOR
15  End
```

CO_Select()

```
1  Check whether neighbor node $N_i$ is type of intelligent node
     or not.
   If $N_i$ Î Intelligent_ Nd{ } then,
     $N_i$ is added to candidate_CO{ }.
    // candidate_CO{ } consists of all candidates of CO.
2  Compute degree of each neighbor node of  GN.
3  If degree ($N_i$)>= MAX(Deg_GNeibor{}) then,
     If Res_Eng(N)>=MAX (RE_GNeibor{}) then,
               prob($N_i$ ) =1.
        //$N_i$ has the probability of  becoming CO.
   Else exit.
4  If maturity of the node $N_i$ equals to 0 then,
        desig($N_i$)  is set to CO.
         //maturity→ experience level 0 or 1.
5  Set maturity of the node is to 1.
6  Broadcast profile of new CO.
```

Cluster_Form()

```
   // Procedure to form cluster within coverage area of CO.
1  CO broadcasts its profile and starts timer T.
2  Nodes that acknowledge within this period are added to
   C_neibor{}.
Simple nodes are added to SneiborCO{}.
```

Collect_Info()

```
   // Step to collect data from sensing leaf node.
 1 GN sends query for sensing data to ZO through CO.
 2  ZO sends wake-up coin to corresponding $N_i$ and
    computes current energy level of node.
 3  ZO calls Anomaly_Detec().
```

Anomaly_Detec()

```
   //  Step to detect anomaly during data transmission.
 1   /* check whether packet received from
        $N_i$ during sleep schedule of $N_i$ */
        If  $T_{SLP(START)}$ <= T1<= $T_{SLP(END)}$  then,
           /* where $T_{SLP(START)}$ and $T_{SLP(END)}$ represent
           begin and end  of sleep schedule for node
           $N_i$ and receipt time(packet($N_i$))=T1*/
 2      /*count number of wake-up coin received by
              $N_i$ within a specific time interval*/
               If count(wakeup(tinterval))> Th_Token,
                     then , anomalous event occurs.
 3        ZO sets  status(pkti)=1(suspected) to any packet from
              Ni , otherwise status(pkti)=0 (genuine).
```

Confirm_Intrusion()

```
//  During transmission, MN monitors traffic whether
       intrusion occurs or not.
1  If Th_max <count($p_i$ from $N_i$ )< Th_min then,
       check , if Res_Energy($N_i$) <$Th_{ENERGY}$ then,
           Warning ticket generated by MN to CO.
```

Action()

```
1  If any packet is received by CO, whose status is set to 1,
      but no warning is generated then,
         packet is erroneous but no intrusion.
2  If CO receives warning tickets (WT) from more than one
      MN for the same packet then,
           CO ignores corresponding fake packet irrespective
           of its status field.
3   Related valid data packets are aggregated and forwarded
     to GN.
4   If  count (Warning)> Threshold then,
           $N_i$ is blocked for further communication.
   Else
        $N_i$ remains under observation.
```

Although the procedure focuses on intrusion detection at low capacity sensing nodes, detection can also be possible at other nodes.

i) If ZO repeatedly sets valid packets as suspected, i.e., when counting (false detection) > threshold, it is considered compromised, and MNs send warning tickets to CO. Then the old one is blocked, and new ZO is selected.

ii) If the warning ticket rate (the ratio of the number of reported warning tickets from distinct MNs to the total number of MNs in the cluster) exceeds a predefined threshold within a time interval, then the compromised MN is blocked, and a new one is selected.

iii) If MNs (more than one) detect CO's abnormal flow volume, they send warning tickets to GN. Then compromised CO is blocked, and the new one is selected.

4. Conclusion

Wireless geo-sensor networks are susceptible to various security threats due to its deployment in the open and unprotected domain. As battery exhaustion attacks can quickly cut off parts of the geo-sensor network by exhausting compromised nodes' energy levels, early detection is essential. In this paper, an effort has been made to propose a collaborative model capable of detecting intrusion. The proposed SEGNET model aims to save the power consumption of sensor nodes from extending the network's lifetime, even in the face of attack. The proposed model virtually eliminates the probability of phantom detection (Chaki, R., & Chaki, N., 2007, June) by using three-step processes. The SEGNET model's workload is distributed among the components according to their capacity to avoid complete exhaustion of battery power. More studies are being undertaken to analyze the proposed model's performance and will be compared with other existing models.

References

Chaki, R., & Chaki, N. (2007, June). IDSX: a cluster based collaborative intrusion detection algorithm for mobile ad-hoc network. In *6th International Conference on Computer Information Systems and Industrial Management Applications (CISIM'07)* (pp. 179-184). IEEE.

Chen, R. C., Hsieh, C. F., & Huang, Y. F. (2010). An isolation intrusion detection system for hierarchical wireless sensor networks. *J. Networks, 5*(3), 335-342.

Conti, M., Chong, S., et al. (2011). Research challenges towards the Future Internet. *Computer Communications, 34*(18), 2115-2134.

Falk, R., & Hof, H. J. (2009, June). Fighting insomnia: A secure wake-up scheme for wireless sensor networks. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies* (pp. 191-196). IEEE.

Heinzelman, W. R., Kulik, J., & Balakrishnan, H. (1999, August). Adaptive protocols for information dissemination in wireless sensor networks. In *Proceedings of the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking* (pp. 174-185).

Huo, G., & Wang, X. (2008, June). DIDS: A dynamic model of intrusion detection system in wireless sensor networks. In *2008 International Conference on Information and Automation* (pp. 374-378). IEEE.

Stajano, F., & Anderson, R. (1999, April). The resurrecting duckling: Security issues for ad-hoc wireless networks. In *International Workshop on Security Protocols* (pp. 172-182). Springer, Berlin, Heidelberg.

Yawut, C., & Kilaso, S. (2011, May). A wireless sensor network for weather and disaster alarm systems. In *International Conference on Information and Electronics Engineering, IPCSIT* (Vol. 6, pp. 155-159).

Submitted: 31.07.2020
Accepted: 20.11.2020