ACTM: Anonymity Cluster Based Trust Management in Wireless Sensor Networks

Shaila K.[1], Sivasankari H.[1], S.H. Manjula[1], Venugopal K.R.[1], S.S. Iyengar[2], and L.M. Patnaik[3]

[1] Department of Computer Science and Engineering,
University Visvesvaraya College of Engineering,
Bangalore University, Bangalore-560 001
[2] Florida International University, USA
[3] Indian Institute of Science, Bangalore
shailak17@gmail.com

Abstract. Wireless Sensor Networks consists of sensor nodes that are capable of sensing the information and maintaining security. In this paper, an Anonymity Cluster based Trust Management algorithm(ACTM) is proposed which enhances the security level and provides a stable path for communication. It is observed that the performance of the network is better than existing schemes through simulation.

Keywords: Anonymity, Cluster head, Trust value, subrange values, Wireless Sensor Networks.

1 Introduction

Wireless Sensor Network (WSNs) consists of a large number of tiny sensor nodes that are equipped with sensing, processing and communicating components. WSNs applications include target tracking in battle field and environmental monitoring etc.. The deployment nature of sensor networks makes them more vulnerable to various attacks. Thus, providing security to WSNs becomes very important. Traditionally, cryptography and authentication approach are used to provide security. Conventional approach of providing security is not sufficient for autonomous network, so trust-based approaches are used for providing security to the network. In order to evaluate the trustworthiness it is essential to establish the co-operation and trust between sensor nodes. Group-based Trust Management Scheme [1] uses Hybrid Trust Management and works on two topologies: *intra-group topology* and *inter-group topology*.
Motivation : During processing of data, each node forwards the trust of its neighbors to cluster head upon request. When sink sends request to cluster head, it transmits neighboring clusters trust value to the sink. So, there is a possibility of adversary performing traffic analysis during the communication between sensor nodes. Hence, security level has to be enhanced by incorporating identity anonymity feature to the existing Group-based Trust Management Scheme.

V.V. Das and J. Stephen (Eds.): CNC 2012, LNICST 108, pp. 75–80, 2012.

Contribution : In this paper, we have proposed an Anonymity Cluster based Trust Management(ACTM) algorithm to establish and maintain trust values between communicating sensor nodes. In identity anonymity, identity of the sensor nodes is hidden from the compromised sensor nodes while calculating the trust values. The adversary cannot predict other subranges of the sensor node and hence enhances the security in WSNs.

2 Literature Survey

Riaz et al., [2] proposed Group-based Trust Management Scheme which calculates trust for group of sensor nodes in each cluster. It works on intra-group topology using distributed trust management approach and inter-group topology using centralized trust management approach. Karthik et al., [3], compares various trust management Techniques for high trust values in WSNs. The trust values are maintained based on the various processes like trust establishment, trust propagation, trust metrics and Group Based Trust Management Schemes.

Efthimia et al., [4] propose Certificate-based approach mechanism for deployment knowledge on the trust relationships within a network and Behavior-based trust model views trust as the level of positive cooperation between neighboring nodes in a network. Yu et al., [5] present Trustworthiness-Based QoS Routing protocol for Wireless Ad hoc Networks.

3 System Model

Consider a static Wireless Sensor Network consisting of a large number of small devices called sensor nodes. The number of nodes in a sensor network can be of 144 sensors with 600 x 600 nodes, 225 sensors with 800 x 800 nodes and 324 sensors with 1000 x 1000 nodes. Each sensor node has its own ID. The network is divided into number of groups referred to as clusters. Cluster Head (CH) is elected for each cluster, which has more power compared to other members of the cluster. Each sensor node can communicate with all its cluster members directly. Each cluster head commu-nicates with neighboring cluster heads as well as with sink either through intermediate CH or directly.

4 Problem Definition

Consider a given grid based WSNs, in which nodes are organized in the form of clusters. The trust values are computed and communicated from the nodes to sink through the cluster head. During this process, the adversary performs traffic analysis and alters the trust values. The objective of this work is to avoid traffic analysis attack.

Assumptions: (i) Initially all nodes will be in uncertain zone. (ii) Each node has enough memory to store range of dynamic IDs. (iii) Sensor nodes have to exchange their ID ranges within a short period, to avoid the nodes compromising with an adversary. (iv) Adversary cannot attack sink.

5 Algorithm and Implementation

In order to overcome the traffic analysis attack, anonymity of the nodes and trust values are maintained during transmission. Initially, *N* nodes are generated using random function and are arranged in a grid fashion. These nodes are divided into smaller groups called as clusters and they elect their leader called as *Cluster Head* as proposed in Selection of Cluster Head algorithm in Table 1.

These cluster heads communicate with the other cluster heads and the sink. An adversary can track the information being transmitted if it is able to trace the IDs of the sensor nodes. To overcome this problem, identity anonymity is created by dividing the dynamic ID pool into number of subranges of equal size. Each sensor node is given randomly chosen subranges that are overlapping and non-contiguous from ID pool as explained in Assigning Anonymity IDs algorithm in Table 2. Map table is created at each sensor node to map true ID of sensor node with dynamic sender and receiver ID.

Table 1. Algorithm: Selection of Cluster Heads (SCH)

```
Begin: Algorithm SCH
Generate: N nodes using rnd function.
 for i=0:T_i:N do
 for j=0:T_i:N do
      Assign the nodes in grid pattern.
   if(n(i).neigh(1, 1))then
       Form Clusters of p nodes each.
   endif;
 endfor;
 endfor;
  for i=T_i:p:N do
  for j=T_i:p:N do
  for k=1:n_d
     if(n(k).x==i)&&(n(k).y==j) then
           Elect the Cluster Head
     endif;
  endfor;
  endfor;
  endfor;
end;
```

Table 2. Algorithm: Assigning Anonymity IDs (AAI)

```
Begin: Algorithm AAI
 for i=1:n_dxnumber of nodes in cluster.
      Calculate the anonymity IDs.
 endfor;
 for k=1: n_d;
 for i=1:length(n(k).neigh)
      Create map table-determine subrange
IDs
      of sender and receiver.
 endfor;
 endfor;
  for i=T_i:p:N do
  for j=T_i:p:N do
  for k=1: n_d
    if(n(k).x==i)&&(n(k).y==j) then
         Randomly assign subrange IDs from
          map table to sender and receiver.
    endif;
  endfor;
  endfor;
  endfor;
end;
```

The trust of any node indicates its ability to provide the required service. Based on the trust value, the nodes can be categorized as trusted, uncertain or untrusted nodes. If the node is malicious it is categorized as untrusted or uncertain node. Trust value is calculated first at Node level, then at Cluster head level and finally at sink level based on number of successful and unsuccessful interaction between the nodes using sliding window [2] for every *r* iterations. Similarly, the trust values are computed at cluster heads.

Table 3. Algorithm:Calculation of Trust Values (CTV)

```
Begin: Algorithm CTV
  k=find(n(i).sw(:, 14)==2);
   if ~ isempty(k)
     for l=1:length(k);
       Calculate average trust values using
           n(i).h=(SM/2)*length(k));
     endfor;
   else k=find(n(i).sw(:, 14)==0);
  if ~ is empty(k)
   for l=1:length(k);
     Calculate average of 1/2nd of all untrustful
     node using (n(i).g=[1-n(i).h]/2_length(k));
   endfor;
 endif;
endif;
  for j=1:length(n(i).sw(:, 1))
    if (100-h ≤ trust value ≤ 100) then
       node is trusted; so assign trust state.
    else node is uncertain or untrustful.
       Check if any past interaction occurred
       between node i and j, then node i
takes
       peer recommendation about node j.
    endif;
  endfor;
end;
```

Table 4. Algorithm: Anonymity Cluster based Trust Management (ACTM)

```
Begin: Algorithm ACTM
input: global n_d, N, M, i_1=k_2, j_1, k_1,a, r, u, h,
h_i, p, SM=0, d=0, w=0;
initialize : trust value of each sensor node.
Set T_i=50, k=1, initial=0;
begin
 for (a = 1 to r)
     Phase 1: Call Algorithm SCH;
     Phase 2: Call Algorithm AAI;
 for j=1:length(n(i) : sw(:, 1))
    if j=~r_d(i) then move the window using
       (100*S^2)/(S + U)*(S+1);
    endif;
  endfor;
    Aggregate the trust values from all its
    neighbors and store in matrix form.
  Phase 3: Call Algorithm CTV;
  h_i=find(n(i).neigh(:, 2)==1);
      if (j=~h_i cluster head row) then
         assign trust value to the nodes.
  else
       assign trust value to cluster head.
   endif;
  endfor;
end;
```

Table 5. Map Table: Dynamic ID range for node 1

Neighbor ID	**Sender ID range**	**Receiver ID range**
2	26000-26025	26026-26050
3	15500-15525	15526-15550
13	1190-11925	11926-11950
14	27000-27025	27026-27050
15	58450-58475	58476-58500
25	31800-31825	31826-31850
26	21850-21875	21876-21950
27	23900-23925	23926-23950

Table 6. Trust Value for Each Cluster

CN	Trust Value
1	4480.846941
2	4465.164315
3	4424.981300
4	4372.324430
5	4067.457464
6	4353.610797
7	4105.167300
8	4219.229978
9	4077.384847
10	4427.832076

The trust values of the cluster members and cluster head is communicated to the sink. Finally, the sink allocates trust values to all the nodes in the network (Table 3). The nodes with values greater than 50 are trusted, while nodes with values less than 50 are untrusted and those with value exactly 50 are termed as uncertain. Next, verify if any past interaction had taken place between the communicating nodes. If there is no past interaction experience then node will go for peer recommendation evaluation. Here, the node takes recommendation from trusted and uncertain nodes. So, malicious nodes cannot send false recommendation to trusted nodes. The sender and receiver in different cluster head receive the trust value through the sink. Cluster heads and its trust values are changed after every *r* iterations (Table 4, ACTM Algorithm).

6 Simulation and Performance Evaluation

The simulation is performed using MATLAB. Static sensor nodes organized in grid fashion are deployed in 1000m x 1000m area and the distance between the node is 50m. Cluster size in each network is equal, which consists of σ nodes. Each network comprises of one sink located at the middle of the terrain. Maximum trust value of the node is 100. Initially, all sensor nodes are in uncertain state, i.e., the trust value is 50.

Let the average size of the cluster be σ and the number of nodes in the network be *N*. So the total size of the dynamic ID pool should be $N*\sigma$. Each sensor has got equal number of neighboring nodes of size σ-1. Each sensor node randomly selects σ-1 subranges from the ID pool and cluster head selects σ subranges to communicate with its cluster members and as well as neighboring cluster heads. When node receives any packet, its sender ID is compared with receiver ID in the Map table. Compute dynamic subrange IDs and consider only the integer values. The random assignment of IDs to the nodes are clearly illustrated in Table 5. *For example*: Let us consider the neighbor nodes 13 and 14 in Table 5. The sender ID range is between 1190-11925 and the receiver ID range is 11926-11950 for node 13. But node 14 sender ID range is 27000-27025 and receiver ID range is 27026-27050. This shows that though the nodes have consecutive node numbers, still the subrange IDs are different. When a cluster head wants to communicate with its neighboring cluster, then it uses different ID compared to the ID it uses for communicating with its neighbors.

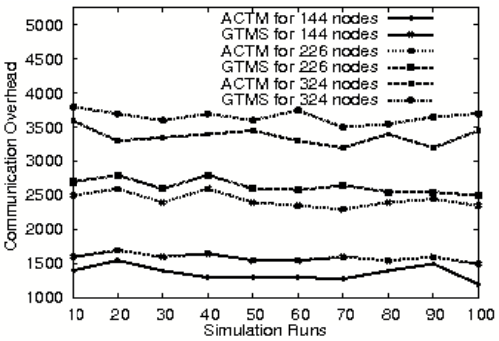

Fig. 1. Comparison of ACTM with GTMS for Communication Overhead

The trust value is generated for each of the node separately. The trust value obtained for each cluster during simulation is tabulated in Table 6. For accuracy purpose the fractional value upto six points is considered. The trust value zero is assigned directly if the nodes have not been communicated for more than two sliding time window period instead of taking peer recommendations.

The communication overhead is plotted for 100 simulation runs for 144, 225 and 324 nodes as shown in Figure 1. The graph shows that the communication overhead is less compared to GTMS. The communication overhead varies depending on size and number of nodes in the network. If the number of iterations is increased, communication overhead reduces because transfer of nodes changes the position of nodes. Still each node possesses past recommendation values in the trust table even if their positions are changed and does not calculate the trust values from beginning. This reduces the communication overhead exponentially. The anonymity IDs are calculated initially and are just assigned to the nodes for every *r* iterations. With low communication overhead it is still able to provide enhanced security as it is using anonymity of IDs.

7 Conclusions

Security is an important issue in Wireless Sensor Networks. We propose an Anonymity Cluster Based Trust Management (ACTM) algorithm to maintain security and avoid traffic analysis attack for WSNs. The proposed approach includes inclusion of anonymous IDs and assignment of trust values to each node. The concept of anonymity is introduced to hide the identity of the sensor nodes from the compromised nodes whereas anonymity of node IDs are not maintained in GTMS. The cluster head and its members are regularly reorganized randomly within the network and hence, the chance of early node failure is reduced. Thus, enhanced security, longer lifetime and reduced communication overhead is achieved in our algorithm.

References

1. Ganeriwal, S., Balzano, L.K., Srivastava, M.B.: Reputation-based Framework for High Integrity Sensor Network. ACM Transaction on Sensor Networks 4(3), 15:1–37 (2008)
2. Shaikh, R.A., Jameel, H., d'Auriol, B.J., Lee, H., Lee, S., Song, Y.-J.: Group-based Trust Management Scheme for Clustered Wireless Sensor Network. IEEE Transactions on Parallel and Distributed Systems 20(11), 1698–1712 (2009)
3. Karthik, S., Vanitha, K., Radhamani, G.: Trust Management Techniques in Wireless Sensor Networks: An Evaluation. In: Proceedings of IEEE Conference on Communications and Signal Processing (ICCSP), pp. 328–330 (2011)
4. Aivaloglou, E., Gritzalis, S., Skianis, C.: Trust Establishment in Sensor Networks: Behaviour-Based, Certificate-Based and a Combinational Approach. International J. System of Systems Engineering. 1(1/2), 128–148 (2008)
5. Yu, M., Lueng, K.K.: A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks. IEEE Transactions on Wireless Communication 8(4), 1888–1898 (2009)