A Trigger Identification Service for Defending Reactive Jammers in WSN

A tracker for spanning the WSN and defeating the blockers in casting mechanism

Candidate Name: Vamsi Anush.Dakoju vamsi.anush566@gmail.com
Visakha institute of engineering and technology
Guide: Mrs Padmaja Rani padmajarani30@gmail.com

Abstract: In the wireless network normally maintaining the central base station is tedious and complicated task. So in this paper we are using and migrating from normal network to wireless adhoc network. In this network we will put base station that will not only monitor all dynamically framed sub base stations (router-*i*) but it will establish a system/architecture to enable a blocker to decrease the instant/time based jammers which will block the jammers.

Here the nodes(peers) will be added/deleted/updated in the network. Once the nodes in the network reach the threshold value the central base station will put some trusted node as sub router and starts casting the preceding added nodes. This will continues till the nodes are getting added to current network.

Modules:

- Network framing
- Spanning tree technique
- Casting nodes with sub router
- Blocker for instant/time based jammers.

Introduction:

- Normally in WSN once the network framed will be tracked by base Station. Which is total burden for base station for monitoring all the peers in the WSN.
- In this work the trigger identification service will check for the following 3 categories.
- 1. Anomaly detection 2. Jammer property estimation 3. Trigger detection.

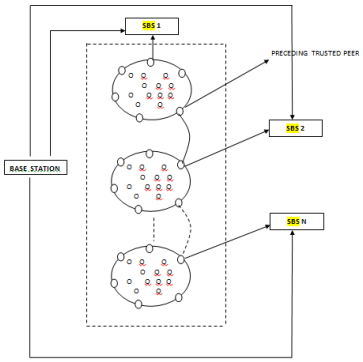
We propose spanning technique in the future work to distribute the peers in the casting way to ignore the burden on central base station. This itself is so flexible for distribution of bandwidth for more casting nodes.

The main aim of this technique is to span the peers in more casting groups which will be under supervision of sub base stations. These sub base stations will be framed by most trusted which are categorized by main base station. We have a threshold to calculate and categorize the sub base stations to establish the castings.

Once the casting nodes are framed we enable the trigger mechanism which will be under substations supervision and these triggers spans the bandwidth and have the trigger identification for third party jamming attacks. WSN will be having lot of other intrusion properties which will be easily identified by this infrastructure, reason is we are using distribution infrastructure.

The jammers in this are in this new infrastructure are the next preceding trusted nodes in the spanning distribution of casting technique.

Architectural design:



Fig(1)

Analysis:

The above picture shows our new approach where our spanned casting nodes distributively. Here in the above 3 casting nodes are shown with last one as ***n***th casting group. Normally in the previous approach whenever WSN updated the nodes they keep added to the main network and will be under supervision of super base station. This base station will have some threshold to frame casting nodes.

Once the base station frames the casting nodes as a group it checks for the trusted node in the existing nodes to put as a sub base node to supervise the framed casting group. The framed casting group will be under super vision the trusted peer(which is framed by root node).

Next the nodes are getting added and the casting nodes will be framed as grouped and preceding trusted node will be sub-base station . The reason behind this is not only to put less burden on base station but also to jamming nodes to restrict the transmission.

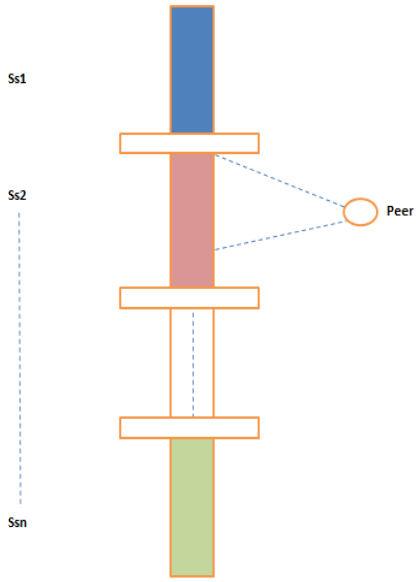
Disadvantages in existing system:

- The entire system and architecture is with regular mess networks which is complicated to resolve or track peers.
- Central base station is the main monitor which is over burden to existing network.
- The jammers are instantly generated by system. Timely generated mechanism is not available;
- Current network cannot adopt third party network and if so band width issues are raised.
- Addition of extra peers to the current network is complicated task.

Advantages in proposed system:

- The entire architecture migrated to wireless adhoc with spanning tree model.Which is easy to monitor and manage by central base station.
- Spanning tree technique helps proposed system to frame casts with dynamically added nodes.
- Central base station will calculate nodes for trusted vector formation.
- A blocker system will established to decrease the jammers if the current network bandwidth matches to other network if that network is adapted to existing one.

Algorithms:



Fig(2) *λ = 14(threshold for per casting segment)*

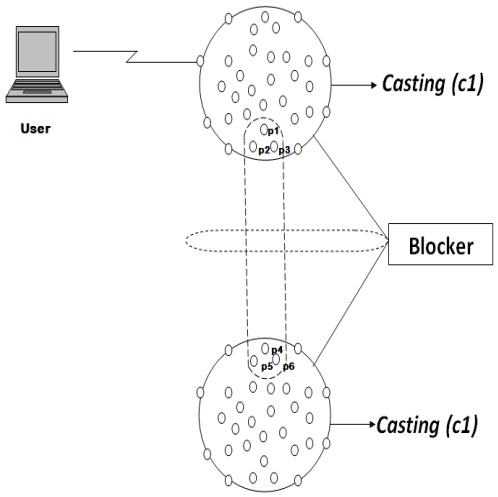
- ***Spanning tree***: The spanning tree is a dynamically generated vector for wireless sensor network. Once this vector is initiated ,Central base station will give an unique identifier to all generated nodes. All the peers will be in this vector with the id, transmission ,casting group ,sub station id etc information. Once the peers keeps getting added to existing network spanning tree will add the nodes to vector (logically) and to network physically. Fig2 contains n segments in node vector. These segments will be generated according to the total number of nodes. Once nodes keep

getting added, based on threshold value substation segments will be added and nodes will be added to *ssi*. Once the peer is added spanning tree will frame substations segments.

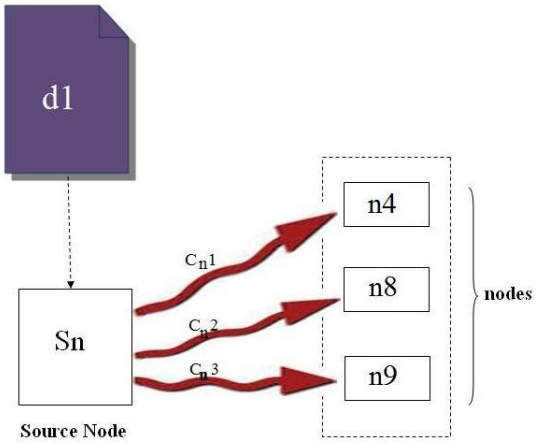
Initialization block:

∑N ← Nodes
∑Ss ← Spanning tree vector
n←0 //node initialization
I ← 0

ST(spanning tree framing)
for each node m in N
loop start
Ssi ε m
If value=n%10 ==0
I = I+1;
End loop;
End for;



- ***Casting technique***: Once the transmission happened for selected destination nodes all the nodes which are with data junks will be casted. If the document d1 is selected for transmission for selective nodes say {n4,n8,n9} among n available nodes these 3 will come under casting c1 and other nodes will be ignored for this transmission. So if the data is framed up with 3 junks which are with {n4,n8,n9} as 3 individual copies. These copies are saved at nodes permanently and logged for central server monitoring. At any time log will be having



{c1 U c2 U c3}=d1

Conclusion:

Hence in this project we have established the overall base station to monitor the wireless nodes that are in the adhoc network. Therefore we can add or delete those nodes that block the jammers. To overcome the burden over the base station we are having three techniques to trigger identification like anomaly detection, jammer proper estimation and trigger detection.

Reference:

1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002.

[2] P. Albers and O. Camp. Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches. In First International Workshop on Wireless Information Systems, 4th International Conference on Enterprise Information Systems, 2002.

[3] R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, 1996.

[4] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In IWSP: International Workshop on Security Protocols, LNCS, 1997.

[5] T. Aura, P. Nikander, and J. Leiwo. Dos-resistant authentication with client puzzles. In Revised Papers from the 8th International Workshop on Security Protocols, pages 170–177. Springer-Verlag, 2001.

[6] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 2(1):46–55, 2003.

[7] P. Bose, P. Morin, I. Stojmenovi´c;, and J. Urrutia. Routing with guaranteed delivery in ad hoc wireless networks. Wirel. Netw., 7(6):609–616, 2001.

[8] D. Braginsky and D. Estrin. Rumor routing algorthim for sensor networks. In WSNA ’02: Proceedings of the 1st ACM international workshop on Wireless

