Black Hole Combat Using Node Stability System in MANET

Ranajoy Chatterjee[1] and Mukti Routray[2]

[1] Faculty of Computer Science and Engineering, Indic Institute of Design and Research, Bhubaneswar, Orissa, India
[2] Faculty of Computer Science and Engineering, Silicon Institute of Technology, Bhubaneswar, Orissa, India
{ronychatterjee,muktiroutray}@gmail.com

Abstract. MANET (Mobile Ad hoc Network) is a form of ad hoc network consisting of mobile nodes. The behavior of such network is autonomous and it gets connected to several types of network by using wireless connection. As no nodes in this network infrastructure are stationary, nodes link each other to participate in transmission. However nodes in the family may turn bad (malicious) or external attacking nodes disrupt secured routing bringing instability to network and sometimes increasing threat to applications of importance for e.g. both military and civilian applications. In both the above cases the nodes needs to be punished. In this paper we use a Node Stability System (NSS) to propose methods of identification of singular and co-operative Black hole nodes and provide steps to recover the network from such vulnerabilities.

Keywords: DTMS, Black Hole Attack, Node Stability System.

1 Introduction

One of the major characteristics of a Mobile Ad hoc network is the absence of a fixed infrastructure (no access points or base stations) or centralized administration. A group of wireless nodes(mobile computers) which may directly co-operate with each other by transmitting packets and from a network or sometimes collecting data or information from various sensors and then connecting to the network to distribute the data among several nodes for distributed processing forms an ad hoc network. The network should be much more adaptive since unlike wired transmission the nodes are often significantly mobile thereby inducing a significant topological change. [7]The attacker[10] sometimes prevents the useful packets from reaching the destination by use of Rushing Attacks[2][1][8][9] ARIADNE ensures limiting the attacking power by preventing the attacker form injecting packets resulting in routing loops. [5]. A DTMS [6] based DSR (Dynamic Source Routing) is empowered to detect and eliminate any kind of malicious packet dropping. [6][7]Therefore our major aim by developing this system infrastructure is to combat such intrusions[4] and devise strategies using the proposed system.

V.V. Das, E. Ariwa, and S.B. Rahayu (Eds.): SPIT 2011, LNICST 62, pp. 249–254, 2012.

2 Node Stability System

As mentioned earlier, we propose a NSS as an efficient and robust defense mechanism for MANETs where we go for reliability based calculation and reserve it for further interpretation.We allot FID to each and every participating node in the network before forming the network. We assume that this id is intended only for the members of the network and this FID is hidden from any outsider, passerby or intended hackers.

We represent the initial Node Security Value to be

$$NSV=N/X^2$$

Where, 'X' is the total number of nodes having FID, and 'N' is the total number of good nodes in the network after time Tk. Therefore at the time of initialization the nodes are set with an initial Node Security Value of 0.5. This NSV is broadcasted to several other nodes at periodic intervals for regular update to the Node Security Table. When any node xi is added then there is to be an authentication check whether the node can be a member of the family. If found good a family id is generated for this new node and the NSV for all the nodes are set once again in the next time interval after new node xi joined the network.At its stability of NSV=0.5, each node builds up its own Node Security Table where the participating node is assigned a Node Security Level which is given negligible weightage of c as a knowledge parameter, where the total NSL for a node xi is calculated by node xj which can be given as

Current $NSL=c\ NSL_{prev} + (1-c)\ NSL_{Tk}$
Where $NSL_{Tk}=NSV * NSL_e$

Where $NSL_e= 1-[1/(\{(S/(S+U))*Wis\}+2)]$, When $S\geq U$

And $NSL_e= [1/(\{((U-S)/(S+U))*Wiu\}+2)]$, When $S<U$

Here, S represents the number of successful interactions, U represents the number of unsuccessful interactions, Wis and Wiu represents the weight of net successful and unsuccessful interactions respectively, chosen arbitrarily depending on the number of interactions taking place.This Node security level determines the stability of each node. In case the level of any node drops to zero it is termed to be as a 'Black hole' and further marked as a bad node.The source node transmits a Route Request packet to all the family members. Then it randomizes a timer to collect the Route Replies. In each Route Reply the Node Security level of the responding node to it and also the node of its next hop's level is checked. On getting routes having the same NSL, the routes having least hop counts is taken if not then the route with the node having highest NSL is selected.Good nodes are awarded and bad ones are punished. When the destination sends acknowledgement on receiving data packets it goes on incrementing the NSL en route all the nodes to the source. In absence of acknowledgement the intermediate node's NSL will be decremented.

A proper check has to be maintained to see the Node Stability Point of NSV=0.5. When NSL falls to 0 then the node is termed as a bad node and NSV of each and

every node becomes less than the Node Stability Point. It is now an alarming situation. Each and every node should now no longer select the above detected node for routing, and hence the node is identified as bad node and eliminated from the network. Trial for recovery of such node can be ttaken up periodically. On the contrary NSV is also considered to be instable in the range of $0.5 \leq NSV < 1$, as the value rises with the event of addition of unauthenticated nodes (nodes without family id). In the above range there must be a periodic attempt by the nodes not in the family to get itself identified and all other nodes too should advocate the same cause so that NSV once again must tend to gain the Node Stability Point. When NSV reaches 1 it means the network has grown to the size where non family members are of the same size of the present family members. This is now a critical situation where the nodes must stop sending any packets and generates a massive alarm before shutting themselves down.

3 The Defense Mechanism

3.1 Related Works

Cases for elimination of collaborating black hole have also been dealt [11] with PCBHA [3] with modifications to AODV protocol. Also modification to DSR has enabled a Trust Based Scheme wherein a Trust factor is induced with a greater stress on the recommendation factor.In the method of route selection, a second chance is given to the nodes that were misbehaving previously to operate so that they have to work good to be trusted.[12]

3.2 Working of NSS

3.2.1 Response Collection

The incoming responses are collected in the Response table . The fields would be source address, destination address, next hop, hop count, TTL, destination sequence number, source and destination header addresses. The collection will be done till timer expires.

3.2.2 Choosing a Route

A valid route is selected from the method as under.A Node Security table is maintained which holds the NSL of the participating nodes. NSL for the responded node and also the next hop would be recorded. If the mean M of their levels is found to be above the specified threshold then the node is considered to be reliable. On receipt of the RREPs the one with the highest NSL is taken into consideration and the route is selected. If Nodes are found of same NSLs the one with minimum hop count is selected.

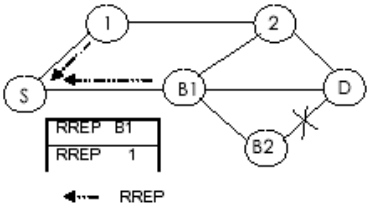

Fig. 1. Response Collection

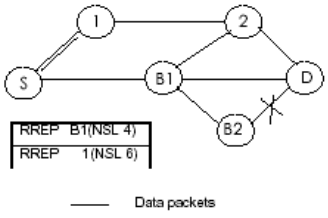

Fig. 2. Response Selection on the basis of NSL for a route to forward data

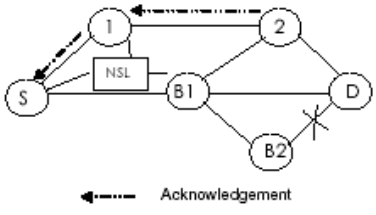

Fig. 3. Receipt of Acknowledgement and updating of NSL

As shown in the above figures the source S chooses RREP-1 after checking the NSL values

3.2.3 NSL Updating

On receipt of data packets every destination nodes sends an acknowledgement. On receipt of acknowledgement the Source node S increments the NSL of the Next node and awards it to be a good node. On the contrary if within the expiry of the timer the intermediate node fails to give any acknowledgement (In the above Figure B1 and B2 acts as the co-operative Black holes) then it decrements the NSL Value of that node and also the next hop of the intermediate node to identify the collaborating attack. And the rest nodes are informed in the network. Periodically the NSL value is shared among the participating nodes.

3.2.4 Eliminating Black Hole

When NSL drops to 0, it proves that it has dropped all the packets forwarded to it and we call this node as the bad node. This simultaneously decrements the NSV to form instability in the network. Alarm packets are sent across all the nodes in the network and the node is eliminated.

Algorithm for the above system is as follows.

```
RREP: Route Reply
NEXT : Next Node
NSL refers to the current NSL computed above.

On receipt of RREP
Mean NSL = NSLNext + NSLNext Hop
Route with highest Mean NSL is selected
NSLNext> THRESHOLD and NSLNext hop >
THRESHOLD
        {
            send data packets
         }
else
       {
           repeat till a max TTL.
          Still if not done then declare the route invalid.
         }
On Timer EXPIRY
                    if Data ACK is received
               {
                   Next NSL is incremented
                   NSL packets broadcasted for other nodes information
               }
                       if Data ACK is not received
                 {
                  Next NSL and Next Hop NSL is decremented
                  NSL packets broadcasted for other nodes information
                 }
if (NSL = 0)
       {
          Node is eliminated from the NS Table
          NSV of Sender is checked for Node Stability.
         }
```

4 Conclusion and Future Work

In this paper we have presented an effective method to combat with misbehaving nodes in MANET. And also we have given stress on maintaining stability in such a network. Not a massive change in the existing protocol structure is appreciable. But for stability of these networks NSS might prove to be a road to further solutions in this area.Our future work aims at probing more into the structure of MANETs with elimination of further adversities regularly.

References

1. Nguyen, H.L., Nguyen, U.T.: A study of different types of attacks on multicast in mobile ad hoc networks. In: Proceedings of the ICNICONSMCL 2006 (2006)
2. Mölsä, J.V.E.: Increasing the dos attack resiliency in military ad hoc networks. In: Proc. IEEE MILCOM, Atlantic City, New Jersey, USA (2005)
3. Tamilselvan, L., Sankaranarayanan, V.: Prevention of Blackhole Attack in MANET. In: The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. IEEE (2007)
4. Aad, I., Hubaux, J.-P., Knightly, E.W.: Impact of Denial of Service Attacks on Ad Hoc Networks. IEEE Transactions on Networking, Reference: LCA-ARTICLE-2007-011
5. Hu, Y.-C., Perrig, A., Johnson, D.B.: Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks. In: Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, MobiCom 2002 (2002)
6. Choudhury, S., Roy, S.D., Singh, S.A.: Trust Management in Ad Hoc Network for Secure DSR Routing. In: CISSE 2007, December 3-12 (2007)
7. Johnson, D.B., Maltz, D.A.: The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF (October 1999)
8. Hu, Y.-C., Perrig, A., Johnson, D.B.: Rushing Attacks and defense in Wireless Ad Hoc Network Routing Protocols. In: ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, pp. 30–40 (September 2003)
9. Choudhury, S., Roy, S.D., Singh, S.A.: Countering Sinkhole and Black hole attacks on Sensor Networks using Dynamic Trust Management System. In: CISSE 2008 (2008)
10. Wood, A.D., Stankovic, J.A.: A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks
11. Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J., Nygard, K.: Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks
12. Bansal, S., Baker, M.: Observation-based cooperation enforcement in ad hoc networks (July 2003), http://arxiv.org/pdf/cs.NI/0307012