Journal of Computer Science 10 (9): 1608-1616, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1608.1616 Published Online 10 (9) 2014 (http://www.thescipub.com/jcs.toc)

DEDICATED TRUSTEE DETECTOR OF BLACK HOLES IN MANETS

[1]J. Manoranjini and [2]A. Chandrasekar

[1]Department of the Computer Science and Engineering, Tagore Engg College, Chennai, India
[2]Department of the Computer Science and Engineering, St. Josephs College of Engg, Chennai, India

Received 2014-02-10; Revised 2014-02-27; Accepted 2014-04-10

ABSTRACT

MANET is developing the next generation wireless universe. However MANETS prove their performance only when routing is efficient. In this paper we propose a model of Dedicated Trust System (DTS) which aims in detecting the misbehaving nodes. We implement our DTD using zone routing protocol with trusted systems. We finally develop a reputation model with two new parameters trustee and bucy trustee, which aims in identifying the black holes and isolating them and show significant upgradation in the overall protocol performance. We make a comparative study of our defensive network with the zone routing protocol defenseless network. All simulations have been implemented using NS2 simulator.

Keywords: MANETS, Zone Routing Protocol, DTD ZRP, Bucy Trustee, Trustee, Trust Reputations

1. INTRODUCTION

An adhoc network in general is a self-configuring infrastructure less network of mobile devices connected by wireless. In mobile adhoc network, nodes coordinating among themselves to determine channel access. In this study we concentrate on clustered topologies where local cluster head elected and used for network control. In a dynamic environment the cluster head election process has to be re-invoked according to a suitable update policy. If the nodes coordinate well then forwarding is done to destination. But in many cases these nodes act as malicious or faulty nodes which misroute data packets and not allowing them to reach destination.

This study deals with one of the security problems in ad hoc networks called black hole problem (Jaisankar *et al*., 2010). The black hole generally exhibits itself as the node which has the shortest path to the destination node and sends its reply as early as possible than all other original nodes thereby the source node assumes this fake node as the path to destination and sends all its packets which are all drained into the fake node making an empty hollow. The network performance is greatly affected by black hole problem.

In this study we propose an trustee bucy mechanism which integrates techniques from trust management system systems and kalman Bucy filter, which to some extent help to filter out the malicious nodes (Natsheh and Buragga, 2010). This study is organized as follows. Section 2 discusses some related work. In section 3, we describe proposed approach to detect the black holes in MANET. Performance evaluation of our protocols is presented in section 4 and finally, section 5 presents conclusions.

2. LITERATURE SURVEY

Dokurer *et al*. (2007) investigated the effects of black hole attacks on the network performance. They simulated black hole attacks in network simulator 2 (ns-2) and measured the packet loss in the network with and without a black hole. They gave a solution which improved the network performance in the presence of a black hole by about 19%. Mishra *et al*. (2009) proposed a method to enhance the security of the AODV protocol and DSR protocol in the presence of Black holes with minimal additional delay and Overhead and gave an analyzes of which routing method is best for different malicious behaviors.

Corresponding Author: J. Manoranjini, Department of the Computer Science and Engineering, Tagore Engg College, Chennai, India

3. TRUSTEE BUCY MODEL

In this study we would like to consider the zone based protocol ZRP (Lee *et al*., 2011) for detection of black holes. Generally in zone topology every node is organized into several zones. For every zone a leader is elected, this leader acts as the representative for his group. In **Fig. 1**, the zone head and its group members are depicted. When a new node wants to join the group it contacts the zone leader and joins the group by updating its routing table.

When the leader leaves a group, another member is elected as a leader and announces its leadership to all other members and other group leaders and hence reconfiguration is efficiently managed in zone routing protocol. Along with the zone head routing table we are including two new parameters trustee and bucy trustee. This trustee is a value which will be calculated for every leader in the zone group. This trustee is calculated based on trust management models. Trustee has all the information about the head that includes the past and present status of the zone head and bucy trustee has all the information about the members.

Our proposed trustee model uses the zone topology where each node that is present in the network should be in one of the three states: 0-node is functioning properly; 1-node is in detection-location phase, 2-node in final phase of route discovery. Identification of the black holes perfectly or accurately is the key issue to consider while detecting black holes. In the **Fig. 2**, we have depicted our new trustee model which has a monitor which gathers all the member and leader values and sends to the detector which manipulates ensures the reliability of routing in the specified and destined route detected by our detector.

3.1. Analytical Model

To apply the Kalman Bucy filter for estimation of state vector the observations are linearized as follows Equation 1:

$$a_n = (t_n^*) + H_n \Delta t_n + \psi_n \quad (1)$$

where, t_n^* is the nominal or reference vector and $\Delta t_n = t_n - t_n^*$ is the difference between the true and nominal state vectors. In the Kalman Bucy filter the nominal vector is obtained from the estimated state trajectory $\hat{t}_n$, i.e, $t_n^* = \hat{t}_n$. The matrix n H is given by Equation 2:

$$H_n = \frac{\partial_h}{\partial t}\Big| t = \hat{t}_n \quad (2)$$

The discrete command process cannot be estimated in the current framework of adhoc networks using HSMM or Bayesian based estimators due to lack of suitable observations required for these estimation processes. We use an alternate idea of dealing the discrete command as an additional noise process and using kalman filter to estimate the mobility state vector. Noise $\hat{P}$ is Equation 3:

$$\hat{P} = Q + C\ F[(u_n - F[u_n])u_n - F[u_n])]B \quad (3)$$

where, the matrix Q and covariance matrix of ω_n is given. The discrete command process u_n consists of two zero mean independent semi-Markov processes, so the covariance matrix of u_n is Equation 4:

$$F[(u_n - F[u_n])(u_n - F[u_n])^{\cdot}] = \sigma_u^2 I_2 \quad (4)$$

where, σ_u^2 is the variance of u_x or u_y.

3.2. System Normal Functioning Phase

Let us consider a reliability R of a 40-node system. The system is said to be functioning properly only if all the components or at least one route from node X to node Y are functioning properly.

We define for i = 1, 2… 40 event X_i = node I is functioning properly:

$$R_i = \text{Reliability of node i} = P(X_i)$$

Let X = System functioning properly and let R = system reliability = P(X) Equation 5 to 7:

$$R_{k/n} = P(\text{K Or more components have not failed})$$

$$= 1 - \Sigma P_{yn}(j) \quad (5)$$

$$= 1 - F_{yn}(K-1) \quad (6)$$

$$= \Sigma(n) R^i (1-R)^{(n-i)} \quad (7)$$

Reliability assures the node to be in state 0, when reliability value raises beyond the threshold value then node enters state 1 which now has to pass a preventive maintenance model. In this model we compute the steady state probabilities by first writing down the balance Equation 8 and 9:

$$\lambda_{\pi 0} = \mu_2 \pi_2, \mu_1 \pi_1 = \lambda \pi_0,\ \lambda_2 \mu_2 = \mu_1 \pi_1 \quad (8)$$

Which yield the following relations:

$$\pi_0 = \lambda / \mu_1 \pi_0 \pi_2 = \mu_1 / \mu_2 \pi_1 = (\mu_1 / \mu_2), (\lambda / \mu_1)\pi_0 (\lambda / \mu_2)\pi_0 \quad (9)$$

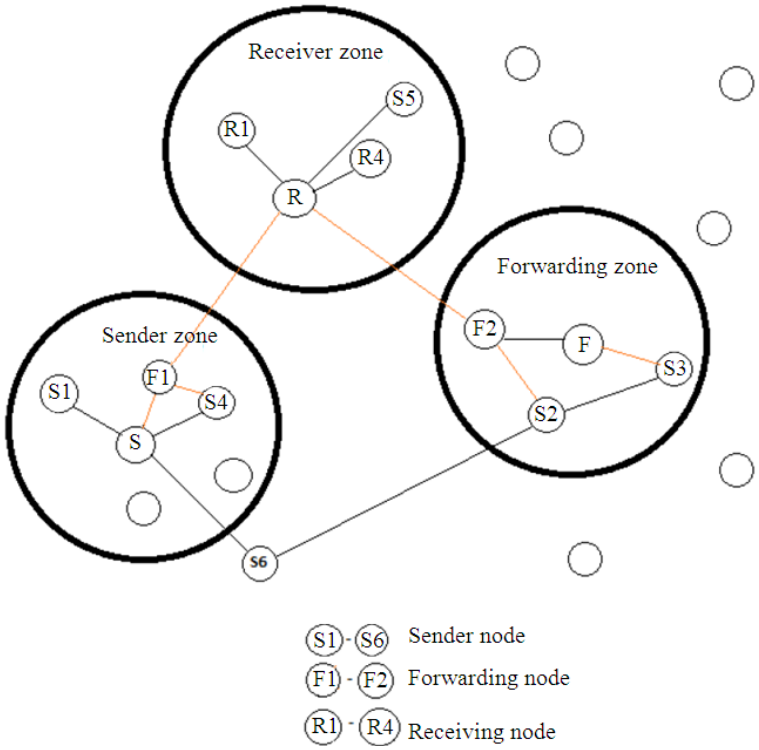

Fig 1. Zone structure in cluster topology

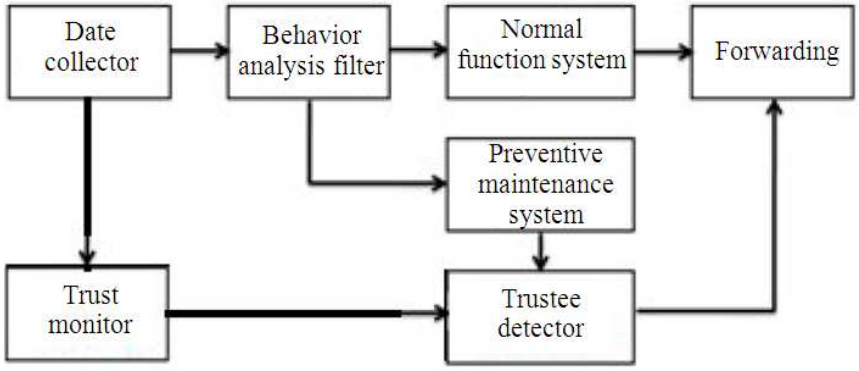

Fig. 2. Trustee detector

Since Equation 10:

$$\pi_0 + \pi_1 + \pi_2 = 1 \quad (10)$$

We have Equation 11:

$$\pi_0 = \frac{1}{1+\lambda/\mu_1+\lambda/\mu_2} \quad (11)$$

Thus the steady state availability A is given by Equation12:

$$A = \pi_0 = \frac{1}{1+\lambda/\mu_1+\lambda/\mu_2} \quad (12)$$

Reliability and availability ensures that node is consistent in its performance or not.

3.3. Preventive Maintenance System

In **Fig. 2** the preventive maintenance system in every node running as zone leader node collects the trustee and bucy trustee values for every neighbour zone head and respective members. Zone head trustee is calculated by multiplying value with the estimated maximized threshold trust value and then the average of the entire trustee values are consolidated and final value is determined Equation 13:

$$T_i = 'v_i A\omega_i + T_{i_1} \overset{p}{A} \omega_i @1^{cU} \quad (13)$$

where, ω is trustee value and v_i is bucy trustee value. These values could be moderated by Equation 14 and 15:

$$T_i = T_{i_1} \omega_i + T_i @1 \quad (14)$$

$$T_i @1 = 1@\omega_i + \omega_i + Av_i \quad (15)$$

Summarizing these two equations we can derive:

$$K_i W a_i^m \overset{d}{A} V_i^{b\cdot} a^c @ a^{@} a\theta^2 n^c$$

This value is distributed to all the neighbour cluster head nodes. Based on successful data delivery rate and successful experience rate, the initial trust value obtained from zone head on node detect K_i as trustee factor (K_i = 0 denotes malicious and K_i = 1 denotes non-malicious).

3.4. Algorithm for Detector Module

The Detector module is the heart of the system. This module inherits the functions where the node checks whether the node is malicious or not. The module computes the reliability and availability of the system. If the value exceeds the threshold value then the system is checked for its incompatibility. The algorithm for detector module as follows:

```
For every observation time
                    do
        {
            for all Node_j which is a neighbour
                if (NormalDetection() or
AutomaticDetection())
                    then Node_j is malicious
                    endIf
                endfor
            }
endevery
                        }
                    {
function NormalDetection()
  obtain observations
    compute R and A
    {
       if R and A exceeds tolerance
            then return true
            else return false
      endif
         }
          endfunction
            }
{
   function TrustDetection()
   obtain neighbourhood zone head reputations
        compute ωi and vi
          {
if relationship between ωi and vi exceeds tolerance
                then return true
                 else return false
          endif
     }
          endfunction
```

4. PERFORMANCE EVALUATION

We have implemented our automatic detector as a network simulator 2 (ns-2) to the ZRP protocol to get the result for our analysis. In our case we have selected our campus as our network scale. **Table 1** employs the simulation setup comprising of 50 mobile nodes moving at a variable speed. Simulation area taken is 1200×1200 m. Packet inter-arrival time (sec) is taken exponential (1) and packet size (bits) is exponential (1024). The data rates of mobile nodes are 10 Mbps with the default transmitting power of 0.010 watts. Random waypoint mobility model is selected with constant speed of 10 m/sec and with pause time of contact 5 to 10 sec. The number of multicast group is 1. The period of sending RREQ packet is 2 s. The ratio of nodes to be included into a zone is 0.8 which means at least 80% of the nearest nodes are included in the zone.

Maintaining the detector to behave consistently is a key issue when detecting black holes, the DTD works well as far as the node speed was concerned.

4.1. Simulation Results

In our simulation let us first examine our node's trust table given in **Table 2** where we have mentioned a sample of two nodes where ω_i and v_i are the two new trust parameters we have introduced in our ZRP and the detected list is maintained by ϖ our detected list. Based on our trustee values which fall between 0 and 1 our detected list is maintained.

Table 1. Simulation parameters

Examined protocols	ZRP
Simulation time	1000 sec
Simulation area (m×m)	1500×1500
Number of nodes	18 and 50
Traffic type	TCP
Performance parameter	Packet delivery ratio, data and control packet transmitted
Pause time	5-10 sec
Mobility (m/s)	10 m/sec
PacketInter-Arrival time (s)	Exponential (1)
Packet size (bits)	Exponential (1024)
Transmit power (W)	0.010
Date rate (Mbps)	10 Mbps
Mobility model	Random waypoint

Table 2. Node's trust table

Node	ω_j	v_j	Detected list ϖ
N_1	0.95	0.97	No
N_2	0.75	0.20	Yes

Table 3. Value setting

N	T	Δt	ω_j	v_j	K_i	ϖ
50	250(s)	25(s)	0.9	0.5	0.7	0.4

Futhermore we also set our basic parameters which is given in the following **Table 3** where N is the no. of nodes we have taken, T is the time interval and Δ_t is the timestamp, ω_i and vi are our new trustee parameters with which we calculate the threshold value K_i finally the detected list of nodes are indicated by the ϖ value.

Based on these values we have obtained the following **Fig. 6** which gives the performance between the standard ZRP and our DTD ZRP. We have drawn our results based on three important performance parameters the packet delivery ratio, packet loss ratio and the total packets transmitted.

Figure 3 shows the packet delivery ratio of the standard ZRP and DTD ZRP as a function of node speed and **Table 4** illustrates the values obtained. Packet Delivery Ratio is the number of data packets delivered to multicast receivers over the number of data packets supposed to be delivered to multicast receivers. We assumed 20 multicast receivers exist among the 50 network nodes. As confirmed by **Fig. 3**, packet delivery ratio decreases as nodal speed increases. This is due to the higher probability of link breakage and topology change, which cause more multicast control packets to be transmitted, lowering the overall data delivery ratio. As the nodal density doubles, the packet delivery ratio only lowers slightly, indicating the good scalability of the DTD ZRP scheme. Overall, a relatively high packet delivery ratio can be obtained.

4.2. Number of Control and data Packets Transferred

Figure 4 shows the average number of total packets transmitted per data packet delivered. Total packets include data and control packets. Since most Medium Access Control (MAC) schemes used in MANETS are contention-based, it is crucial to be able to send one data packet with as less control packets as possible.

4.3. Packet Delivery Ratio for Varying Node Speed

When nodes contend less for the channel access, the probability of successful delivery of packets in a short time becomes higher. As suggested by **Fig. 4**, the average number of packet transmitted per data packet delivered maintain relatively in the range of 1.2-1.5, although it climbs up as the node mobility increases. Total packets sent in the network with DTD ZRP scheme are a little more than in the network of Standard ZRP nodes. Therefore, the control packet overhead introduced by the standard ZRP is overcome by DTD ZRP scheme showing good scalability (**Table 5**).

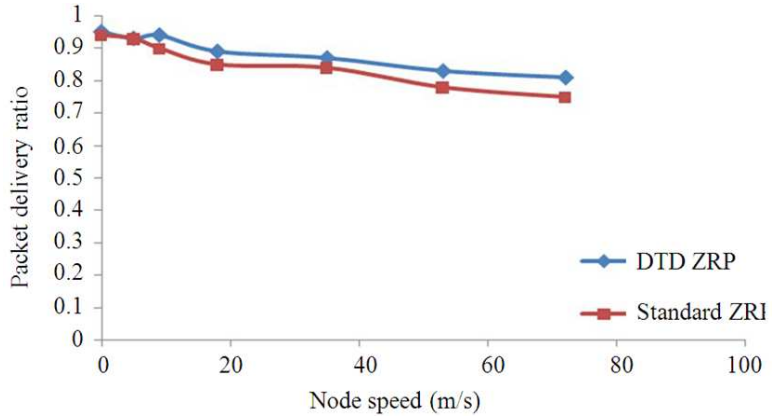

Fig 3. Packet delivery Ratio

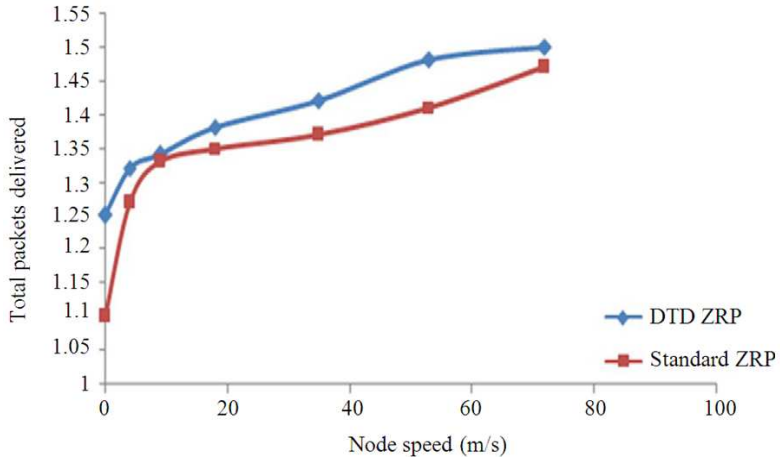

Fig 4. Total Packets Transmitted

Table 4. Packet Delivery Ratio

	Pkts delivery ratio	
Node speed (m/s)	DTD ZRP	Standard ZRP
0	0.95	0.94
5	0.93	0.93
9	0.94	0.90
18	0.89	0.85
35	0.87	0.84
53	0.83	0.78
72	0.81	0.75

Table 5. Total Packets delivered

	Total packets delivered	
Node speed (m/s)	Standard ZRP	DTD ZRP
0	1.10	1.25
4	1.27	1.32
9	1.33	1.34
18	1.35	1.38
35	1.37	1.42
53	1.41	1.48
72	1.47	1.50

4.4 Number of Control Bytes Transmitted

4.1.1. Number Black Holes Detected

The average number of control bytes transmitted per data byte delivered is shown in **Fig. 5** and the values are given in **Table 6**. Here, we choose to use a ratio of control bytes transmitted to data byte delivered to investigate how efficiently control packets are utilized in delivering data. To deliver packets reliably to the destination, some control packets have to be sent. Protocol design has to make some compromise between efficiency and reliability. **Fig. 5** shows that DTD ZRP gets high reliability with relative low control overhead.

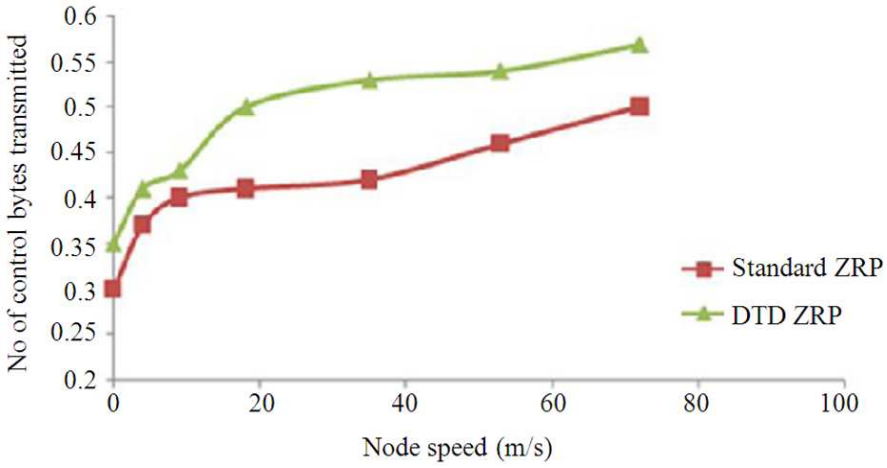

Fig. 5. No of control bytes transmitted

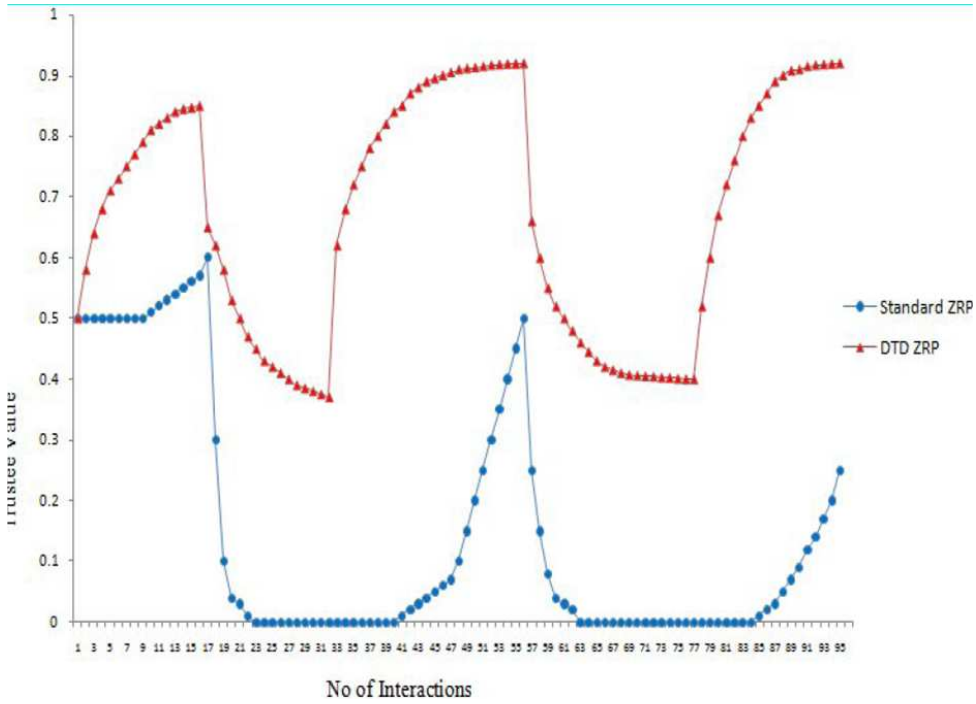

Fig. 6. Comparison of Std ZRP and DTD ZRP detections

Table 6. No. of control Bytes delivered

	No of control bytes transmitted	
Node speed (m/s)	Srandard ZRP	DTD ZRP
0	0.30	0.35
4	0.37	0.41
9	0.40	0.43
18	0.41	0.50
35	0.42	0.53
53	0.46	0.54
72	0.50	0.57

Table 7. DTD ZRP and Standard ZRP detections

	Trustee value			Trustee value	
No of interactions	Standard ZRP	DTD ZRP	No of interactions	Standard ZRP	DTD ZRP
01	0.50	0.050	49	0.15	0.9120
02	0.50	0.580	50	0.20	0.9130
03	0.50	0.640	51	0.25	0.9150
04	0.50	0.680	52	0.30	0.9170
05	0.50	0.710	53	0.35	0.9180
06	0.50	0.730	54	0.40	0.9190
07	0.50	0.750	55	0.45	0.9195
08	0.50	0.770	56	0.50	0.9200
09	0.50	0.790	57	0.25	0.6600
10	0.51	0.810	58	0.15	0.6000
11	0.52	0.820	59	0.08	0.5500
12	0.53	0.830	60	0.04	0.5200
13	0.54	0.840	61	0.03	0.5000
14	0.55	0.845	62	0.02	0.4800
15	0.56	0.847	63	0.00	0.4600
16	0.57	0.850	64	0.00	0.4450
17	0.60	0.650	65	0.00	0.4300
18	0.30	0.620	66	0.00	0.4200
19	0.10	0.580	67	0.00	0.4150
20	0.04	0.530	68	0.00	0.4100
21	0.03	0.500	69	0.00	0.4070
22	0.01	0.470	70	0.00	0.4060
23	0.00	0.450	71	0.00	0.4050
24	0.00	0.430	72	0.00	0.4040
25	0.00	0.420	73	0.00	0.4030
26	0.00	0.410	74	0.00	0.4025
27	0.00	0.400	75	0.00	0.4010
28	0.00	0.390	76	0.00	0.4005
29	0.00	0.385	77	0.00	0.4000
30	0.00	0.380	78	0.00	0.5200
31	0.00	0.375	79	0.00	0.6000
32	0.00	0.370	80	0.00	0.6700
33	0.00	0.620	81	0.00	0.7200
34	0.00	0.680	82	0.00	0.7600
35	0.00	0.720	83	0.00	0.8000
36	0.00	0.750	84	0.00	0.8300
37	0.00	0.780	85	0.01	0.8500
38	0.00	0.800	86	0.02	0.8700
39	0.00	0.820	87	0.03	0.8900
40	0.00	0.840	88	0.05	0.9000
41	0.01	0.850	89	0.07	0.9080
42	0.02	0.870	90	0.09	0.9100
43	0.03	0.880	91	0.12	0.9150
44	0.04	0.890	92	0.14	0.9170
45	0.05	0.895	93	0.17	0.9180
46	0.06	0.900	94	0.20	0.9190
47	0.07	0.905	95	0.25	0.9200
48	0.10	0.910			

The final indication of the performance of a DTD ZRP scheme is its detection of black holes at a consistent level a good multicast scheme should scale well even if a wide range of number of receivers “tap” to the multicast group. We present our simulation results of the DTD ZRP scheme in this respect in **Fig. 6** and the values in **Table 7**.When the receiver number equals to 1, it ensure trusted path and high packet delivery ratio is assured. In standard ZRP the results are shown where the detections are not given so the packet loss occurs frequently.

5. CONCLUSION

This study is an improvisation of my previous work on Black Hole attack with cluster topology, where different scenarios with respect to zones where analyzed. Based on the introduction of the new trustee parameters we have drawn a conclusion that new approach identifies the black holes and maintains the consistency in routing. More study is suggested to implement this mechanism to scale for a larger group of networks.

6. REFERENCES

Dokurer, S.Y., M. Erten and E.A. Can, 2007. Performance analysis of ad-hoc networks under black hole attacks. Proceedings of the SoutheastCon, Mar. 22-25, Richmond, pp: 148-153. DOI: 10.1109/SECON.2007.342872

Jaisankar, N., R. Saravanan, K.D. Swamy, 2010. A novel security approach for detecting black hole attack in MANET. Proceeding of the International Conference on Recent Trends in Business Administration and Information Processing, Mar. 26-27, Springer Berlin Heidelberg, India, pp: 217-223. DOI: 10.1007/978-3-642-12214-9_36

Lee, E., S. Park, J. Lee, S.H. Kim, 2011. Geographic multicast protocol for mobile sinks in wireless sensor networks. IEEE Commun. Lett., 15: 1320-1322. DOI: 10.1109/LCOMM.2011.102611.111565

Mishra, D., Y.K. Jain and S. Agrawal, 2009. Behavior analysis of malicious node in the different routing algorithms in Mobile Ad Hoc Network (MANET). Proceedings of the International Conference on Advances in Computing, Control and Telecommunication Technologies, Dec. 28-29, IEEE Xplore Press, Trivandrum, Kerala, pp: 621-623. DOI: 10.1109/ACT.2009.158

Natsheh, E. and K. Buragga, 2010. Density based routing algorithm for spare/dense topologies in wireless mobile ad-hoc networks. Am. J. Eng. Applied Sci., 3: 312-319. DOI: 10.3844/ajeassp.2010.312.319