Trust-Based Security Technique to Curb Cooperative Blackhole Attacks in Mobile Ad Hoc Networks using OTB-DSR Protocol in NS-3

Ephantus G. Mwangi[1], Geoffrey Muchiri Muketha[2] and Gabriel Ndung?u Kamau[3]

[1] Muranga University of Technology

Received: 8 December 2019 Accepted: 1 January 2020 Published: 15 January 2020

Abstract

The advent of mobile technology led to the emergence of Mobile Ad-hoc networks (MANETs). These networks have no infrastructure and central authority. Nodes in MANETs act as both routers and hosts. MANET nodes join and leave the network at will making the network topology dynamic. MANETs are prone to both passive and active security attacks. Blackhole is a denial of service attack under active attacks. Blackhole nodes work in collaboration forming cooperative black hole attacks. The attacks drop or redirecting data packets on transit. Cooperative blackhole attacks are dangerous in operations where communication is critical

Index terms— routing protocol, mobile ad hoc network, security.

1 Introduction

ANETs are wireless, with no infrastructure, and central management authority. These networks are dynamic nodes join and leave the network at will. MANETs work in areas where wired networks fail either due to destruction or natural catastrophes such as earthquakes, storms, eruptions, or terrorism [1], [2].

In MANETs, nodes communicate through special routing protocols [1], [2]. Researchers have developed several routing protocols and techniques to optimize MANETs' security [2], [6]. However, design issues are surrounding MANETs routing protocols and techniques. Some of the issues are related to the unique properties of MANETs. These issues make most of the security techniques designed for wired networks incompatible with MANETs [3].

MANETs routing protocols are grouped into three categories. The categories include; reactive routing protocols, proactive routing protocols, and hybrid protocols. Reactive routing protocols are demanddriven. They create routes whenever a source node wishes to send data packets to a destination node. This implies that nodes that actively participate in routes formation are the ones that maintain valid routing information. Some of the examples of reactive routing protocols are Adhoc On-Demand Vector (AODV), Dynamic Source Routing (DSR), and Link Aware Routing (LAR) [6]. In proactive protocols, nodes maintain complete routing information of the network. Any change of network topology due to nodes' mobility leads to automatic updating of routing tables. Some of the examples of proactive routing protocols are; Destination Sequenced Distance Vector (DSDV), Global State Routing (GSR), and Hierarchically Segmented Routing (HSR) protocols. Hybrid protocols contain blended features of both proactive and reactive routing protocols [4].

The open form of communication in MANETs paves way for an attacker to join and intercept the communication process. Further, the unique properties of MANETs have introduced an underlying complex security problem [5], [7]. Cooperation amongst nodes has made MANETs vulnerable to many network security threats. Therefore, in the design of effective security techniques secure transmission should be a key consideration [5], [7], [25].

Blackhole attack is one of the popular active attacks that endanger network integrity. Blackhole nodes drop data packets between any two communicating nodes that establish a connection [7]. For instance, a source node

can send Route Request (RREQ) packets to establish a communication with the destination node. Any node in the network that has the shortest route to the destination can respond to the RREQ packet. This open form of communication paves the way for blackhole nodes to join in the communication process. For instance, when the black hole nodes receive the RREQ packet, they masquerade as genuine nodes by sending fake RREP packets with the shortest and freshest route to the destination. This makes the source node to select the route with malicious nodes. However, when these black hole nodes receive the data packets they drop or reroute them to fake destinations. Further, black hole nodes collaborate to launch attacks known as 'cooperative black hole attacks". The cooperative black hole attacks are more harmful to a network than any other form of attack [8], [20].

Techniques such as CBDS and ECBDS suffer from security and performance issues. These issues are attributed to packet delivery ratio (PDR), end to end delays, and routing overhead. Most of the security issues arise from architecture and design considerations of the techniques. For instance, in CBDS and ECBDS techniques a source node takes some time to identify and use bait address from one of its immediate neighbours. This contributes to end to end delays. Further, these techniques do not have an effective mechanism of identifying genuine nodes in the network which leads to the incorporation of blackhole nodes in the transmission process. Additionally, genuine nodes transmit data packets without checking their energy levels. This opens an opportunity for the depleted nodes to transmit; hence acting selfishly. Selfish nodes drop data packets to save energy for their sustenance.

The study proposes a TB-RCBDT technique using the OTB-DSR protocol to identify and mitigate collaborative black hole attacks. TB-RCBDT used Resilient Cooperative Bait Detection Technique (RCBDT) which uses source node self-address as the bait address. Source node self-address saves transmission bandwidth, node's energy, and time. Further, RCBDT uses an algorithm that checks energy levels for all genuine nodes before engaging them in any transmission. In case there are nodes whose energy levels are below the threshold, it gives alerts to the source node. Additionally, TB-RCBDT uses the trust concept through the OTB-DSR protocol to identify malicious nodes in the network.

The design, implementation, and simulation of TB-RCBDT were done in a Linux environment using NS-3. Further, the technique was tested alongside CBDS and ECBDS used as benchmark techniques.

The rest of the paper is organized as follows; Section 2 presents related works, section 3 is a discussion of the methodology used. Section 4 describes the simulation environment. Further, section 5 presents the results and discussions. Finally, section 6 summarizes the study by giving conclusions and future work.

2 II.

3 Related Work

Abdelshafy and King proposed a mechanism (BRM) using the AODV protocol [6]. Its purpose was to mitigate the black hole attack. Simulation results showed that BRM-AODV was superior to AODV and SAODV routing protocols in all network performance metrics. BRM detected black hole nodes easily regardless of their number. Additionally, results showed that BRM increased the performance of AODV routing algorithms in MANETs. However, BRM-AODV failed to detect collaborative black hole attacks. Reviewed literature indicates that no enhancement of the BRM has been done.

Ukey proposed a 1-2ACK technique to curb routing attacks in MANETs [16]. 1-2ACK creates sets of three adjacent nodes for all the nodes that form routes for transmitting packets. This technique detected and mitigated black holes' attacks. However, the technique introduced extra control packets which led to routing overheads.

Hiremani and Jadhao developed a security technique using modified extended data routing information (MEDRI) using the routing table of the AODV protocol [17]. The technique was capable of detecting cooperative black hole attacks. MEDRI table maintained a record of the history of the previous malicious nodes. This record was used for the future discovery of secure paths from source to destination. However, the technique suffered from routing overhead and end to end delay.

Mistry et al. proposed a security technique that uses the source node to receive the first RREP [9]. Further, the technique waits for a specified time interval before receiving and storing the other RREPs. The source node analyses all the RREPs and rejects the ones with a very high sequence number. However, simulation results indicate that the technique increased average end to end delay.

Su et al. proposed a technique using an intrusion detection system (IDS) [10]. The purpose of IDS nodes is to detect the malicious value of nodes based on the difference between RREQs and RREPs forwarded by a node. However, if the malicious value goes beyond the threshold, the node is considered malicious. This makes the IDS node broadcasts a block message to all nodes on the network. The technique introduced extra nodes in the network. Further, IDS sniffed all the RREQs and RREPs of all nodes that led to extra overhead.

Gupta et al. proposed a technique using Ad hoc On-Demand Multipath Distance Vector (OMDV) [11]. The technique provided multiple paths during routes establishment. The source node selects only one route among available ones. The node maintains the legitimacy of all its neighbouring nodes. The technique ensures that the route selected does not include nodes with legitimacy value less than the threshold. This helps in detecting and avoiding malicious nodes. However, the technique was not able to detect cooperative blackhole nodes.

Saha et al. proposed a Two-Level Secure Rerouting (TSR) [12]. The technique uses Local Supervision (LS) and Congestion Window Surveillance (CWS) modules to detect malicious attacks. TSR addresses these attacks

using the Alternate Route Finder (ARF) module. ARF module does the work of rerouting packets at the network layer. Simulation results showed that the proposed technique is resilient against various attacks. However, LS and CWS modules introduced routing overhead.

Bhosle proposed a watchdog and pathrater mechanism [13]. The technique ensures that each node maintains a pending packet table and node rating table. Each node stores all packets forwarded in the pending packet table and overhears its neighbours. If the neighbouring node successfully forwards the packet, the value of the packet forwarded in the node rating table is incremented. However, if the packet is dropped, the value is decremented. Additionally, if the value of dropped packets gets to the threshold value, that node termed as malicious. This used extra memory space to maintain extra tables which translated to routing overhead.

Thachil presented a technique that does the overhearing of neighbouring nodes to calculate their trust value [14]. Before a node forwards the packet, it keeps a copy in the cache. Additionally, a node overhears the packets forwarded by its neighbours. If a packet forwarded by the neighbour matches with the packet in the cache, the sending node believes that the neighbouring node is genuine. However, if the packet doesn't match the trust value is decremented. If the trust value goes beyond the threshold, that node is considered malicious. The technique introduced routing overhead at a node.

Bindra et al. developed a security technique that uses the AODV protocol [15]. The proposed technique keeps an extended data routing information (EDRI) table in every node. This technique discovers secure paths by avoiding cooperative black hole nodes. However, the challenge of this technique is that malicious nodes must be contiguous to be discovered. Further, the introduction of the EDRI table led to routing overhead.

Gaikwad and Ragha developed a cooperative cluster agents (CCAs) technique to mitigate cooperative black hole attacks [18]. The technique uses DRI and SRT-RRT tables as input to CCAs. Simulation results showed that the technique detected cooperative black hole nodes. Additionally, the technique identified a secure routing path from source to destination. This technique was compared to the standard AODV protocol. Results show that the technique proved to be superior. However, CCAs technique introduced routing overhead due to the incorporation of DRI and SRT-RRT tables. Further, packet delivery ratio and throughput need further improvement to hit the desired levels.

Dumne and Manjaramkar proposed a Cooperative Bait Detection Scheme (CBDS) based upon the DSR mechanism [19]. The scheme integrates proactive and reactive defence architectures to detect malevolent nodes. Simulation results showed that CBDS using AODV was superior to DSR protocol and CBDS using DSR. Metrics used in this scheme were throughput and packet delivery ratio. However, the proposed technique was inferior to CBDS using AODV in terms of throughput and packet delivery ratio. This is a motivation for researchers to enhance the new technique. Further, the reverse tracing technique led to the end to end delay in data transmission.

Emimajuliet and Thirilogasundari proposed Modified Cooperative Bait Detection Scheme (MCBDS) based on DSDV [20]. MCBDS is a modification of CBDS. Simulation results showed that MCBDS with DSDV protocol was superior to DSR and 2ACK scheme. However, MCBDS suffered from routing overhead. Reviewed literature shows that there is a need for a hybrid technique that can combine MCBDS with other techniques to provide a resilient technique that can secure routing of data packets.

Mwangi, Meath, and Kamau proposed a Resilient Cooperative Bait Detection Technique (RCBDT) using DSR protocol in NS3 to curb collaborative black hole attacks [29]. The proposed technique used the source node address as the bait address. Further, the RCBDT used an algorithm that checks nodes' energy levels before engaging them in packet transmission. The proposed technique was compared with CBDS and ECBDS used as benchmark techniques. Simulation results indicated that the proposed technique was superior to benchmark techniques. Metrics used were packet delivery ratio, end-to-end delays, and routing overheads. The findings showed that RCBDT had the highest packet delivery Ratio of 94%, while ECBDS and CBDS had 88% and 81% respectively. Additionally, simulation results indicated that RCBDT had the lowest routing overhead of below 8% while ECBDS and CBDS had 15% and 19% respectively. Finally, results indicated that RCBDT had an end-to-end delay of 1.2 seconds while ECBDS and CBDS which had an average of 1.3 and 1.8 seconds.

Mwangi, Meath, and Kamau proposed an Optimized Trust-Based Dynamic Source Routing (OTB-DSR) protocol in NS3 [30]. The proposed protocol integrates dynamic trust and friendship functions in the architecture of standard DSR protocol. The performance of the OTB-DSR protocol was compared to standard DSR and AODV used as the benchmark protocols. Simulation results indicated that the proposed protocol was superior to standard DSR and AODV protocols used as the benchmark protocols. Performance metrics used include; packet delivery ratio, routing overhead, end to end delays, and throughput used as performance metrics. The OTB-DSR protocol had a packet delivery ratio of above 95%, routing overhead of 4.75%, an end to end delay of between 0.9 seconds and 1.65 seconds, and throughput of 95.6 Kbps.

4 III.

5 Methodology

The architecture of the proposed technique was first designed. In the next section, the architecture was translated into a flowchart. Further, in the next section, a detailed description of the proposed technique was provided. In the next section, a demonstration of how the proposed technique computes trust weights in source routes was

done. In the next section algorithms of the proposed technique and SROC were developed. Further, in the next section, the technique was implemented in NS-3 programming language. The next section was a discussion of the results of the proposed technique. Finally, the last section was the conclusion and future work.

6 a) The Architecture of TB-RCBDT Technique

The architecture is made up of integration of RCBDT and OTB-DSR. The two components interact to identify safe and resilient routes as shown in Figure 1. Further, besides the architecture combining the merits of both proactive and reactive defines architectures. It also employs the concept of trust values and energy levels of a node when selecting optimal routes from the node's cache. These factors make the selected source route stand higher chances of being free from malicious attacks during the data transmission process. The primary purpose of this component is to select the most optimal route among the prioritized routes. The selected route is marked as the backbone route for packets transmission. The other routes in the node cache are marked as secondary routes. However, in case the selected route turns out to be invalid or broken, the route refresher component in liaison with the OTB-DSR protocol refreshes the source routes. The information about the fresh source routes is circulated to all the nodes in the network so that they can update their nodes' caches. The block diagram in Figure 2 is a diagrammatic representation of the SROC module. The flowchart of the TB-RCBDT technique is shown in Figure 3. The technique comprises of integration between Optimized Trust-Based DSR protocol and RCBDT design. The primary purpose of RCBDT is to bait all the malicious nodes in the network. Further, RCBDT is also responsible for determining the energy level for all nodes to establish genuine nodes in the network. Any node with an energy level far above the expected level is considered to be malicious; hence blacklisted. Genuine nodes with energy levels above the threshold level and within the limits of acceptable nodes' energy levels are engaged in packet transmission.

7 e) Initial Self-Address Bait phase

The phase uses the address of the source node (self-address) as the bait address. This is opposed to the initial bait phase of CBDS and ECBDS which randomly chooses the address of one of its nearest hop neighbours as its bait destination address. The source node sends bait RREQ with its address as the destination address and waits for a reply from other nodes in the network. OTB-DSR protocol helps in broadcasting this self-address to all its neighbours through the flooding process. A 'Flooding Controller' is used which reduces the lifetime of RREQ packets by every hop. FC will ensure that the flooded RREQ packets automatically eliminate themselves in the network. This will lead to efficient utilization of the bandwidth and also control routing overhead. Further, the TV will help in identifying the most reliable backbone nodes as their selection will be based on the value stored in the TV packet.

Any node that sends the RREP packet is considered a malicious node in the network. The malicious nodes are the fake nodes that receive the route request packet and masquerade to be genuine nodes by sending fake RREP packets with the highest frequency. This triggers the reverse tracing program as indicated in the next phase.

Using self-address as the bait address makes the source node to save its battery power. This power could have been used when communicating with one hop step neighbour to generate the bait address. Further, this also saves time and other network resources as no engagements are involved between the source node and its one-hop step neighbours, hence improving network efficiency.

8 f) Reverse Tracing Phase

In this phase, the reverse tracing program is started to detect the routes with malicious nodes. If the routes are secure, no node send san RREP packet since the source node had broadcasted its address. When malicious nodes receive RREQ, they respond to false RREPs. This triggers the reverse tracing program which tries to identify the dubious paths and exact location of the malicious nodes through the RREPs.

The reverse tracing program then forms a set (Nd) of all the nodes that sent back the false RREPs and saves them in the malicious nodes alarmed list. The source node uses this set (Nd) to form a malicious node detected list. It then sends an alarm to all other nodes in the network about the existence of the malicious nodes. The malicious nodes detected list helps other nodes to establish temporary a set of trusted routes in the network.Nd={n1,n2,n3,?,nm}**(1)**

This phase saves a lot of node's battery power and memory space as no set difference operation is computed to identify the malicious nodes. In ECBDS, when the node received RREP, it would perform a set difference operation between the address List recorded in RREP and saved RREQ. Further, it would cache the routing of receiving nodes and consequently obtain a new list of genuine nodes. This process drained battery power and memory space, hence limiting its ability to participate in subsequent data transmission processes.

9 g) Reactive Defence Phase

In this phase, first, the reverse tracing program is terminated. Additionally, all the nodes in the malicious node detected list (blackhole list) are deactivated by setting their life-bit bit to zero (sleep mode). Further, this information is broadcasted to all other nodes in the network. Secondly, the OTB-DSR route discovery phase gets triggered. OTB-DSR ensures that Cumulative Trust Values (CTV) and Friendship Level (FL) of every node in

the network are computed before the node is engaged. The route discovery process introduces a set of special nodes known as backbone nodes which helps in the fast selection of new routes. The selection of these backbone nodes is based on factors such as; nodes' availability, nodes' signal strength, nodes' cumulative trust value, nodes' friendship level, and energy levels of nodes. The CTV and FL help in identifying reliable primary routes and backbone nodes.

The backbone address challenges of link breakages due to failure or node unreachability. These backbone nodes are reliable neighbouring nodes on standby. Further, they are closer to the optimal routing path nodes and have good signal strength and sufficient power. This improves the efficiency of the technique by guaranteeing the transmission of data packets without any transmission issues. When some of the reliable intermediary nodes get out of range a link failure can occur. In such a case, backbone nodes take charge of the process and the route is re-established without delay. The backbone nodes are selected at one hop distance from the affected node using the gratuitous technique.

10 h) Refreshing Phase

In this phase, the nodes' route caches are refreshed. Broken links are deleted and newly established temporary trusted routes are saved in the nodes caches. Further, the newly recorded routes in the cache are used to determine the optimal route based on the current status of the network. These routes remain valid as long as there are no broken links or no gratuitous routes established. Additionally, the life-bit of nodes classified as genuine is incremented by one, and information circulated to all other nodes in the network. These nodes are allowed to participate in network operations as long as their battery power is above the threshold level.

11 i) Computation of Trust Weights in Source Routes

TB-RCBDT technique uses the OTB-DSR protocol to calculate the nodes' trust values (TV) and friendship level (FL). The two parameters create an array of source routes weights 'Snaw' which are saved in the node's cache. Equation **??**.1 is an array of calculated source routes weights stored in node X's cache. From equation 6.1, 'w' is the weight of the route while '?' is a variable representing the dynamic variation of trust in nodes of a given route based state and time.

The weight of a route can be any integer value based on the node's social group level and trust recommendations (RTV) made by neighbouring nodes based on positive or negative interactions during packet forwarding. Equation **??**.2 shows how to calculate the weights of every source route. From equation 6.2, '?' is a moderating constant. This constant maps the aggregated trust weight of a source route between 0 and 1. Value '0' represents the absence of trust while value '1' represents total trust. The trust weights of routes are spread out between the two values. Source routes with most of the nodes from Most Trusted Friendship Level are the most secure routes since their route trust values are close to '1'. However, if source routes have most of the nodes from Untrusted Friends Level, they are the least secure routes since their route trust values are close to '0'.?? ?? [] = {?? 1??? , ?? 2??? , ?? 3??? , ?? 4??? , ? , ?? 5??? }**(2)**?? ??=([?????? ????] * ? ???? ?? ??=1) * ??**(3)**

The Route Selector module prioritizes the source routes based on the aggregated weights. Source routes with aggregated trust weights greater than 0.5 or equal to 1 (0.5=<Wn<=1) are considered to be more trusted. Further, source routes with aggregated trust weights less than 0.5 (0=<Wn<0.5) are considered untrusted.

The proposed TB-RCBDT technique evaluates the received packets at the destination node. Further, it determines whether they meet the packet delivery ratio threshold. If the PDR is below the threshold level, the technique triggers the destination node making it to send a Negative Acknowledgement (NACK) packet to the source node. Further, the source node redirects control to the Bait Phase where a fresh retransmission process is initiated. However, if the PDR is within the threshold level, the proposed technique triggers the destination node making it to send a Positive Acknowledgement (ACK) packet to the source node. The presence of the ACK packet at the source node end means that the handshake process was successful.

12 j) Algorithm of TB-RCBDT Technique

The TB-RCBDT algorithm describes in nontechnical terms a step by step process of the implementation of the technique. Further, the algorithm describes all the steps and processes undertaken by a node willing to send packets to the destination. Any node wishing to send data packets triggers the RCBDT algorithm which sends bait RREQ packet over the network. The purpose of the bait RREQ packet is to detect any malicious node in the MANET.

Response to bait RREQ packet indicates the presence of malicious nodes in the network. This makes the RCBDT algorithm to mark them as malicious, blacklist, and deactivate them. Further, the algorithm identifies the genuine nodes, increases their life bit. Finally, the algorithm calculates their energy levels. The algorithm triggers the source node to send RREQ which identifies a safe route to channel the data packets. When the RREQ reaches the destination node, this node sends back an RREP packet to acknowledge the receipt of the RREQ packet sent by the source node.

The OTB-DSR protocol calculates the composite trust values of all the intermediate nodes that successfully passed the RREQ packet. These composite trust values are stored in the node caches.

Further, the OTB-DSR protocol uses the composite trust values to calculate the friendship level of all the nodes. Finally, the OTB-DSR protocol uses the nodes' composite trust values and friendship level to calculate the route trust weights.

Further, the TB-RCBDT technique uses the SROC module to select the route with the highest Route Trust Value. This route is marked as the backbone route. The source node transmits the data packets to the destination through the backbone route. Finally, the TB-RCBDT technique checks whether the PDR threshold was met during the data transmission process. If yes, the data transmission process is terminated. Otherwise, the RCBDT is retriggered to restart the packet transmission process. Algorithm 1 shows a step by step procedure of the design of the proposed TB-RCBDT technique.

13 Algorithm TB-RCBDT {[Begin] Run MANET// Calling Algorithm MANET Source Node intends to send data packets to a destination node. RCBDT Algorithm triggered Through RCBDT algorithm Source node sends bait RREQ If (RREP from any node) { do { RCBDT algorithm tracks nodes that sent RREP and marks them as malicious RCBDT algorithm blacklists any malicious node. RCBDT algorithm deactivates blacklist nodes RCBDT algorithm increases life bit of genuine RCBDT algorithm calculates energy levels of genuine nodes } while (Blackhole exists in MANET) else { Source Node sends RREQ Destination node sends RREP//acknowledging to the source node OTB-DSR protocol calculates trust values for intermediates node that successfully passes RREQ packet to nexthop neighbor OTB-DSR protocol stores trust values in nodes caches OTB-DSR protocol uses cumulative trust values to calculate friendship level OTB-DSR protocol stores friendship level in nodes caches OTB-DSR protocol calculates Routes Trust Weights RCBDT algorithm and OTB-DSR protocol use the route selector module to establish the source routes from nodes cache that has the highest Route Trust Weight. Call SROC algorithm Established source route marked as backbone route Destination node sends data packets through the backbone route. while (not PDR threshold met) { go to RCBDT Algorithm triggered } End Packet transmission Release channel //bandwidth Mark route as idle } [End]}

Algorithm 1: TB-RCBDT Algorithm

15 E k) Algorithm of SROC Module

The SROC algorithm is used to select the most optimal source route. The algorithm first scans and creates an array of all possible routes in the source node cache. The routes are then compared based on their route trust values (RTVs). The source route with the highest RTV is selected and marked as the backbone route to be used for packet transmission. However, if the backbone route proves to be invalid, the SROC algorithm refreshes the

array. Further, the SROC algorithm restarts the process of selecting the backbone route afresh. The operations of the SROC algorithm are depicted in Algorithm 2.

16 Algorithm

17 Simulation Environment

To compare the effectiveness of the proposed TB-RCBDT technique, the simulation environment was setup in NS-3 Simulator. The simulation area measuring 1500 by 1000 meters was set in a rectangular pane. Additionally, fifty genuine mobile nodes were installed and configured. Further, two, four, and six blackhole nodes were installed in the three simulation scenarios. The black hole nodes used a simple attack model to entice other nodes in the network. The Channel of communication among nodes was set to User Datagram Protocol (UDP). OTB-DSR protocol was set as the routing protocol for all the nodes in the network.

For the nodes to manoeuvre within the simulation area, the propagation model was set to Radom Way Point (RWP) model. The nodes were configured using radio waves in a manner that could enable them to receive signals from all directions using an omnidirectional antenna. Constant Bit Rate (CBR) traffic model with a packet size of 512 bytes and sending rate of 4 packets per second was set to handle packet traffic. Simulation time for each scenario was set to 400 seconds. Finally, the nodes' transmission range was set to a radius of a radio range of 250 meters. Table 1 is a summary of the simulation parameters. V.

18 Results and Discussions

The proposed TB-RCBDT technique was simulated in NS-3. Data generated by the Simulator was saved as text files of extension ".dat". The text files were then executed using Gnuplot software to generate the output. The generated output was compared to the CBDS and ECBDS technique used as chosen benchmarks. Packet delivery ratio, end-to-end delay, routing overhead, and energy consumption were the performance metrics in the experiment. Figure 4 shows the simulation environment of the RCBDT technique. The dots in red show the distribution of mobile nodes across the simulation area. The study comprised of four different simulation scenarios. Six simulation experiments were conducted in each scenario. The chosen scenarios represented real communication environments faced with security challenges. In each of the scenarios nodes' energy, nodes' speed, and the number of malicious nodes were varied and the performance of the proposed technique was observed. In the first scenario, the network had fifty genuine nodes. Further, one source node and one destination node were selected randomly. The source node was configured in a manner that it could request for packet transmission to the destination node through the proposed technique. The initial energy of nodes was set to 60 joules. Nodes' speed was set to 5 m/sec. Simulation time was set to 400 seconds while the traffic generation interval was set to 10 seconds. Further, the proposed technique was simulated in an ideal environment. In this experiment, two malicious nodes were introduced into the network. The performance of the proposed technique was evaluated against the three metrics in all the six experiments. An average of each metric in the six experiments was taken.

In the second scenario, one source node and two destination nodes were selected. The purpose of increasing the destination nodes was to increase the degree of transmitted packets to black hole nodes. Further, four blackhole nodes were introduced in the simulation environment. The blackhole nodes represented adversaries in emergencies that thwart the communication process. In our experiment, blackhole nodes were used to lure the source node to channel packets through them during simulation experiments. The blackhole nodes would then drop the data packets. The nodes' speed was set to 10 m/sec. The initial energy of nodes was varied from 60 joules to 80 joules. Traffic generation was set to 20 seconds. Six simulation experiments were conducted in this scenario in the presence of two blackhole nodes. Further, the performance of the proposed technique was evaluated in the presence of the two blackhole nodes. The results of the three metrics were recorded. The effect of the two malevolent nodes was evaluated based on recorded results for each simulation experiment. Finally, an average of each metric in the six experiments was taken and compared to the results of scenario one.

In the third scenario, one source node and four destination nodes were selected randomly. Nodes' speed was set to 15 m/sec. Traffic generation was set to 30 seconds. The black hole nodes were increased to five. The initial energy of nodes was varied from 80 joules to 90 joules.

Finally, in the fourth scenario, one source node and six destination nodes were selected randomly. Node speed was set to 20 meters per second, traffic generation was varied from 30 to 40 seconds, and black hole nodes were increased to six. The initial energy of nodes was varied from 90 joules to 100 joules.

19 b) Analysis of Simulation Results

20 i. Packet Delivery Ratio

Results from the simulation scenarios show that the packet delivery ratio of the proposed TB-RCBDT technique was superior compared to the benchmark technique. A summary of the packet delivery ratio simulation results of the proposed technique is illustrated in Tables 2. The minimum packet delivery ratio of the TB-RCBDT technique was 94% which was recorded in scenario 1. This was attributed to the low energy levels of the nodes in the network. When the energy levels of some nodes went low, they behaved selfishly by not forwarding some

packets to their intermediate nodes in the route. The selfish act made these nodes to save energy to extend their lifetime in the network.

The proposed technique recorded a higher packet delivery ratio of 99% in scenario 1 as indicated in Figure 5 despite the presence of cooperative blackhole nodes. In this scenario nodes' speed was 5 meters per second. However, scenario 4 had a lower packet delivery ratio despite higher energy levels. This implies that the higher the nodes speed, the more the energy it consumes during its mobility hence making it behave selfishly as the battery depletes. Although scenario 4 had enough energy to sustain packet transmission in the network, most of the energy was used in mobility due to high speed. This explains why the packet delivery ratio of scenario 1 was higher than that of scenario 4.

On average in all the four scenarios, TB-RCBDT had a higher packet delivery ratio than ECBDS and CBDS used as benchmark techniques. This was attributed to the fact that the proposed technique uses the concept of trust among intermediate nodes to determine which nodes are genuine in the network. Nodes that have successfully passed data packets to their immediate neighbours in the past are regarded as 'trusted'. The trusted nodes are the ones that form source routes in the proposed technique. This implies that despite the higher numbers of malicious nodes in the network, the TB-RCBDT technique is resilient enough to transmit data packets with minimal loss and at a percentage of over 95%. The results of all simulation experiments in the four scenarios were captured in Table 3. As indicated from the table, the end-to-end delays gradually increased from experiment one to experiment six for all the simulation scenarios. The end-to-end delay is a product of turnaround time. Turn-around time is the time taken between the request of transmission by the source node and the grant of the request by the destination node.

The gradual increase of end-to-end delay was attributed to increased nodes in packet transmission.

Hence a lot of time was used in making forwarding decisions. However, generally, on average, the end-toend delay reduced from scenario one four. This was attributed to the fact that as the nodes energy increased from scenario one to four, very few nodes were willing to act selfishly during packet transmission. This reduced the time taken during the establishment of source routes. For instance, in scenario one the minimum end-to-end delay was 0.3332 seconds in experiment one while the maximum was 0.3529 seconds in experiment six. The proposed technique had the lowest end-toend delay of 0.35 seconds as indicated in Figure 6. On average, in all the simulation scenarios the benchmark techniques ECBDS and CBDS had minimum end-to-end delays of 0.58 and 0.61 seconds respectively. Further, it was observed that as the number of nodes increased in the network; there was a proportionate increase of end-to-end delay in all the techniques. The proportionate increase of end-to-end delay was attributed to the fact that every node took some time to make a routing decision. However, since in the proposed TB-RCBDT technique nodes had already been prequalified based on Composite Trust Values (CTV) and social groups, there was a negligible time used on every node in the selected source route. This implies that the proposed TB-RCBDT had the shortest turn-around time. Routing overhead is a ratio that represents the number of controls packets versus the number of data packets sent in every data frame. Table **??** represents the summarized results of the routing overhead for the four simulation scenarios. The columns in the table represent the simulation scenarios while the rows represent the number of experiments per scenario. Simulation results show that the routing overhead of the TB-RCBDT technique increased gradually from scenario one to scenario four. For instance, scenario, one had an average of 3.965% while scenario four had an average of 5.549 %. However, it was observed that the TB-RCBDT technique had the lowest routing overhead of between 4 and 5.5% as indicated in Table 4. This was significantly small compared to the benchmark techniques. ECBDS had a minimum of 5% and a maximum of 15%, while CBDS had a minimum of 5.55 and a maximum of 17%.

It was noted that in all the scenarios, as the number of cooperative blackholes increased, routing overhead proportionally increased for the three techniques. An increase in routing overhead was attributed to the increase in cooperative blackhole nodes. The extra overhead requires the routing technique to make informed decisions when selecting nodes to participate in packet routing. This translates to an increased number of control packets.

However, the proportionate increase in routing overhead for the proposed TB-RCBDT was small in all the cases as indicated in Figure 7. This was attributed to the fact that the proposed technique only selected the highest priority source route. High priority source routes

21) Energy Consumption

As opposed to wired networks, nodes in MANETs are always in motion. This means that at any given time a node keeps on changing its geographical location. These nodes have inbuilt rechargeable batteries in their architecture. The batteries enable them to supply energy as they manoeuvre across the network. However, the depletion of energy levels in the batteries is directly to nodes' mobility and the levels of engagement in packet transmission.

As nodes transmit packets and manoeuvre through the network, they consume a lot of energy. In this study, the consumption of energy by nodes was captured in all the simulation scenarios. Table 5 is a summary of the results of the nodes' final energy in the four simulation scenarios. The initial nodes' energy for the four scenarios was 60 joules, 80 joules, 90 joules, and 100 joules respectively. In scenario one, on average the nodes' battery depleted by 11 joules; that is from 60 joules to 49.356 joules. Further, in scenario four on average the nodes' battery depleted by 26 joules; that is from 100 joules to 73.94 joules. The increase in battery energy depletion was noted across the four simulation scenarios. This was attributed to the increased number of cooperative blackhole

nodes in the network. Table 5 shows that there is a direct correlation between the increase in the number of black hole nodes and the increase in depletion levels of nodes' battery power. This is an indication that the cooperative blackhole nodes constantly drain nodes' battery energy to bring down the network. However, it was observed that the proposed TB-RCBDT technique had the lowest energy consumption levels of between 49 and 73.9 Joules as indicated in the table.

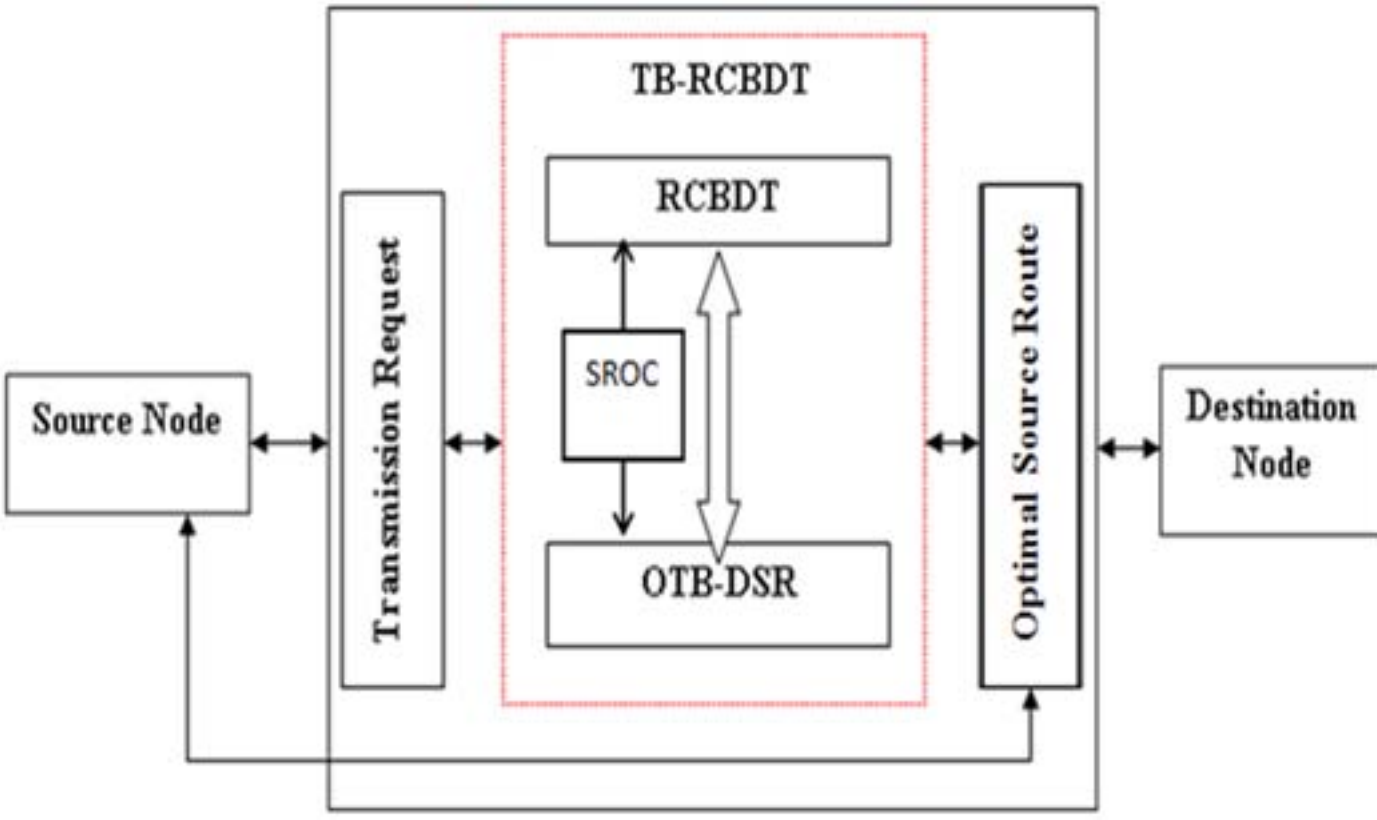
Figure 8 is a graph of nodes' energy versus simulation time (in seconds) for the four simulation scenarios. In the four simulation scenarios, the nodes' initial energy was set to 60 joules, 80 joules, 90 joules, and 100 joules respectively as indicated in the figure. The energy consumption of the proposed TB-RCBDT is indicated in green colour while that of ECBDS and CBDS are indicated in blue and red colour respectively.

The results of the four simulation scenarios indicate that is an inverse correlation between nodes' energy and the simulation time for the three techniques. As the simulation time increases, the nodes' energy levels decrease proportionally. However, from the figure, it can be noted that the proposed TB-RCBDT technique had the lowest nodes' energy utilization levels compared to CBDS and ECBDS techniques. This is an indication that the TB-RCBDT technique is more efficient in terms of energy consumption.

22 Conclusion and Future Work

MANETs are wireless networks that have attracted attention from various domains due to their flexibility and ease of deployment. However, MANETs are prone to a range of security threats. Security is a key concern in any communication system. Guaranteeing security in MANETs is today's one of the biggest challenges. The study proposed a TB-RCBDT technique against cooperative black hole attacks in MANETs. Simulation results indicated that the proposed TB-RCBDT technique is superior to both CBDS and ECBDS used as benchmark techniques. Performance metrics used include; packet delivery ratio, end-to-end delay, routing overhead, and energy consumption. This implies that the proposed TB-RCBDT technique is resilient and robust in mitigating cooperative black hole attacks in MANETs. TB-RCBDT technique has the capability of maintaining better performance through the transmission process as compared to benchmark techniques.

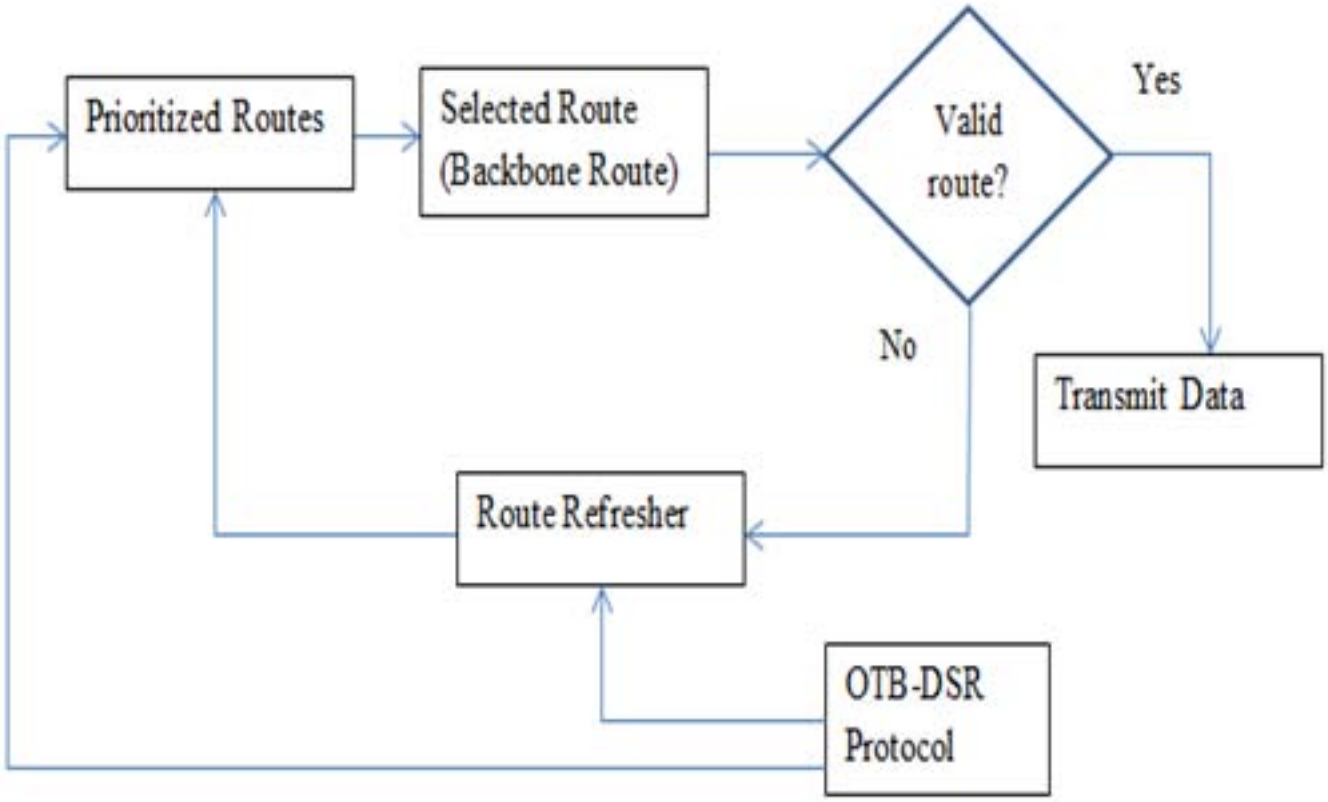
As part of our future work, we intend to improve the TB-RCBDT technique by incorporating an element of artificial intelligence using fuzzy logic. This will improve the effectiveness and efficiency of the technique in mitigating cooperative black hole attacks. [1]



1

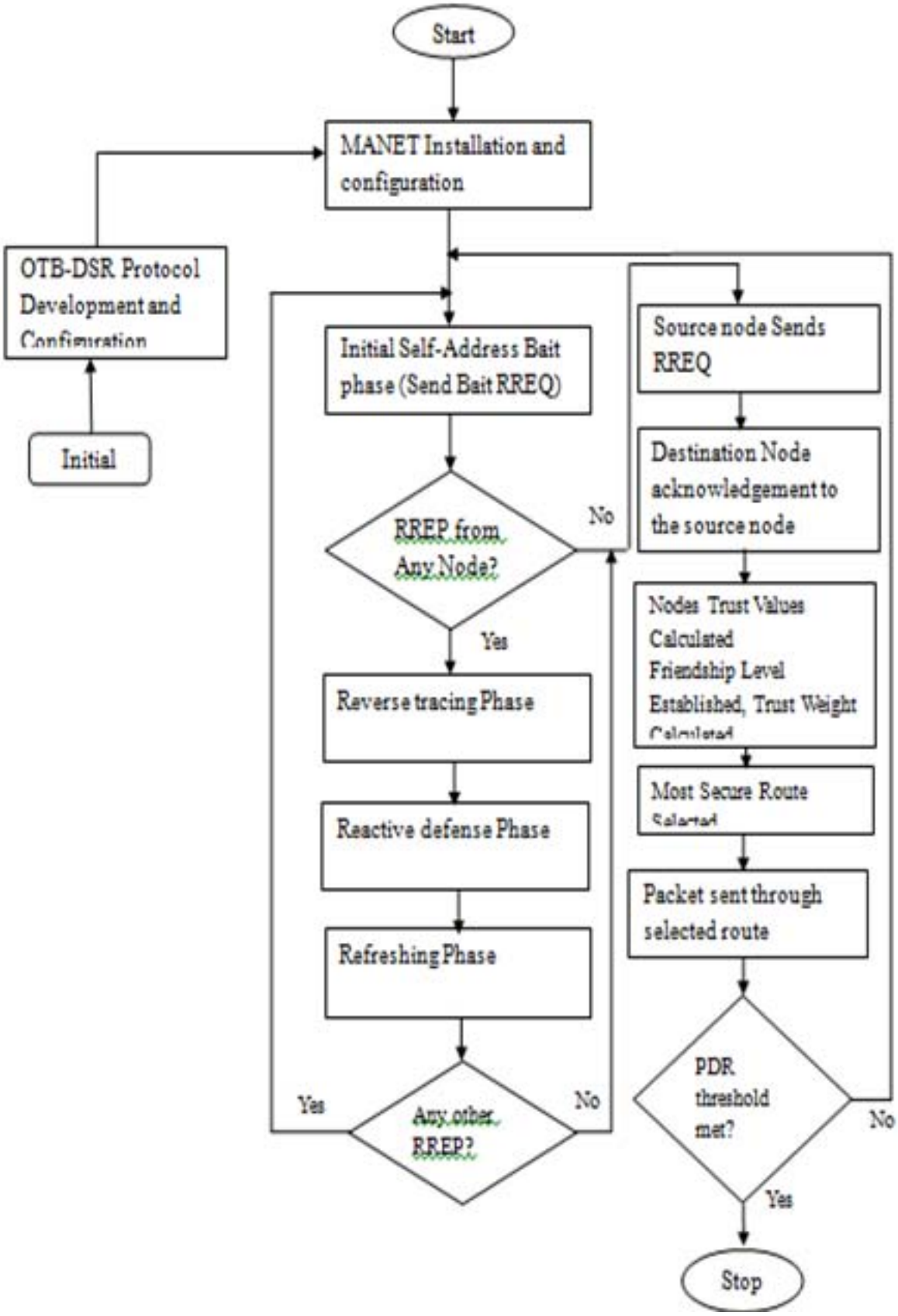
Figure 1: Figure 1 :

[1] © 2020 Global Journals



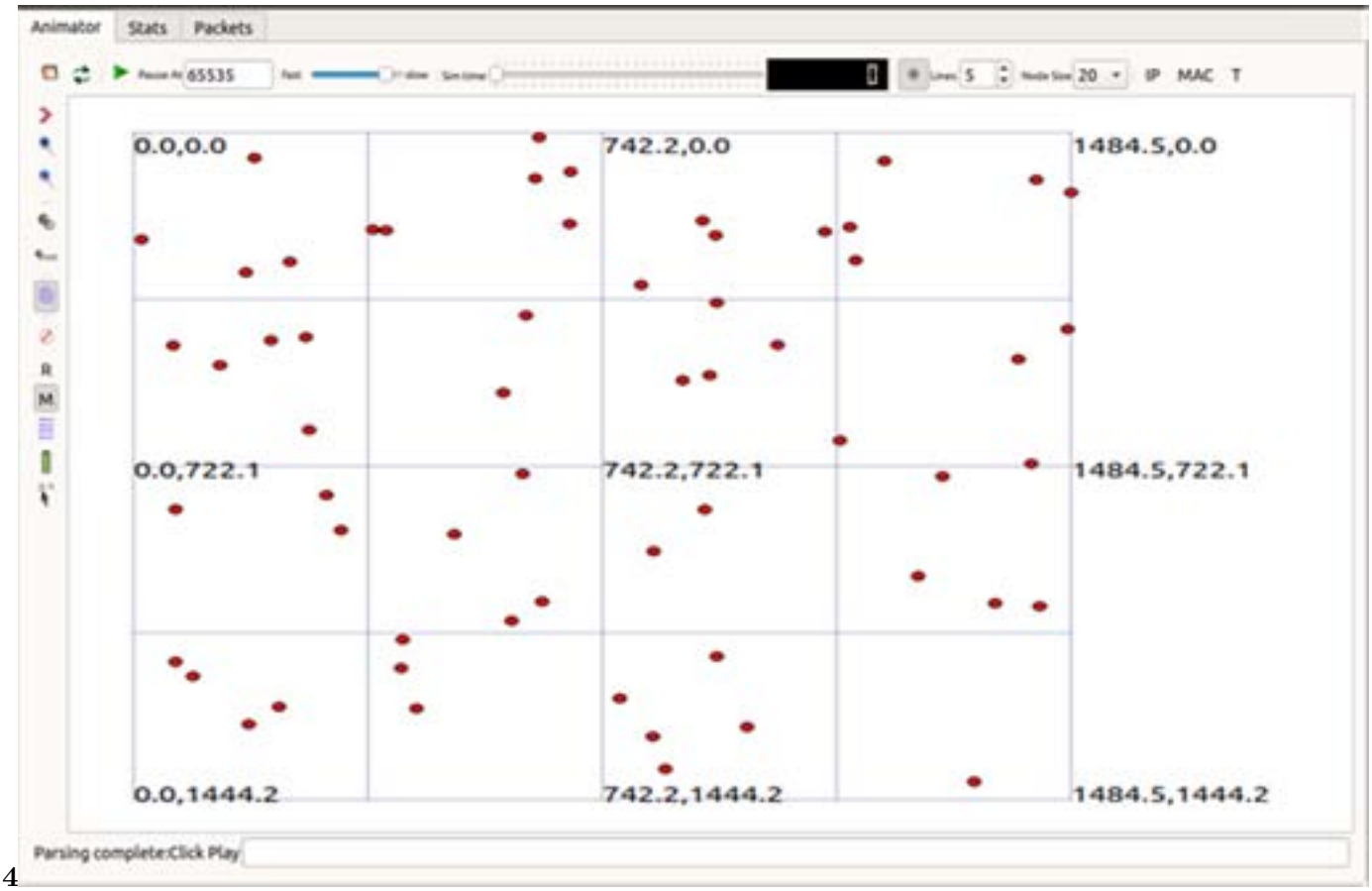
2

Figure 2: Figure 2 :



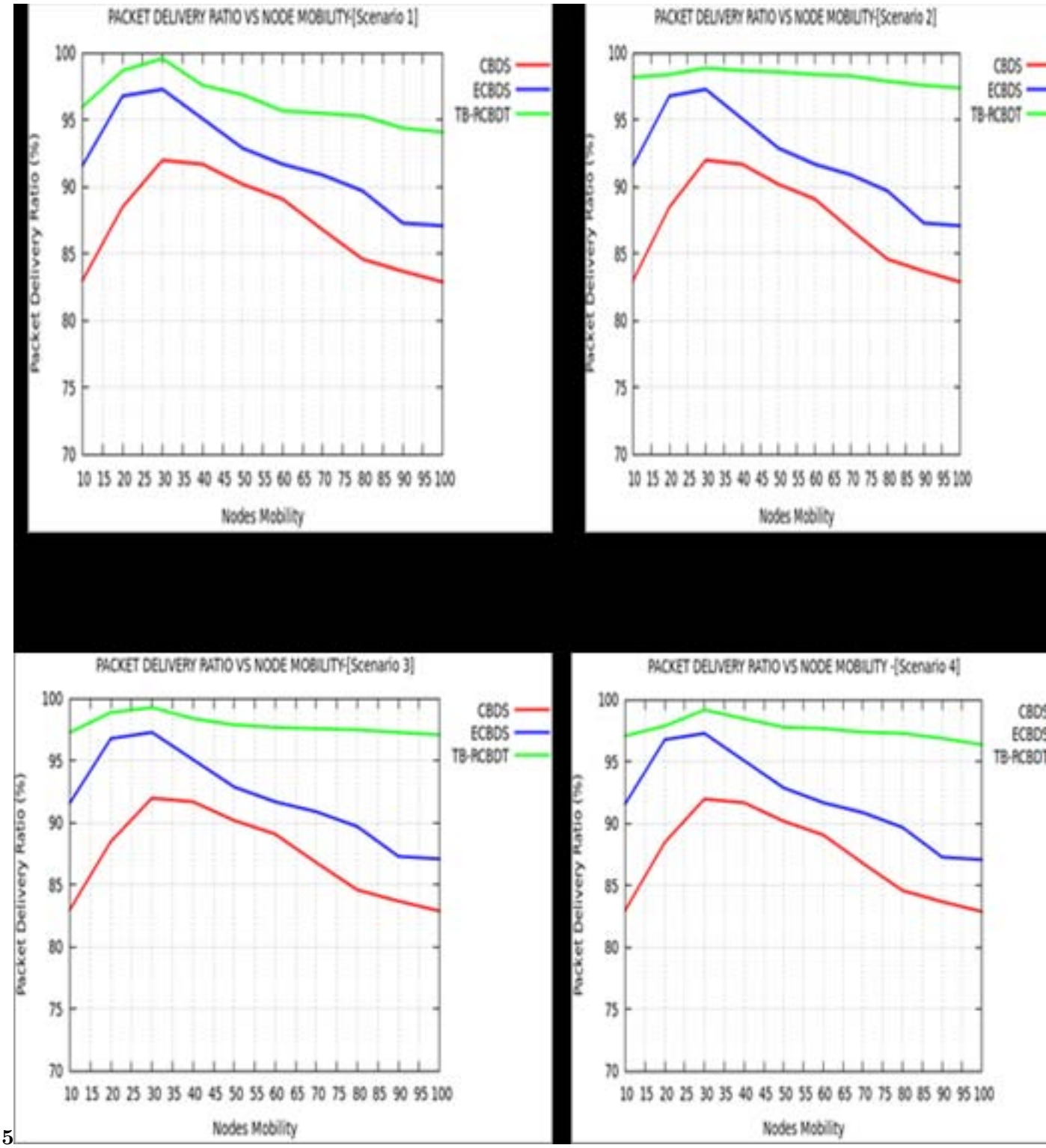
3

Figure 3: Figure 3 :



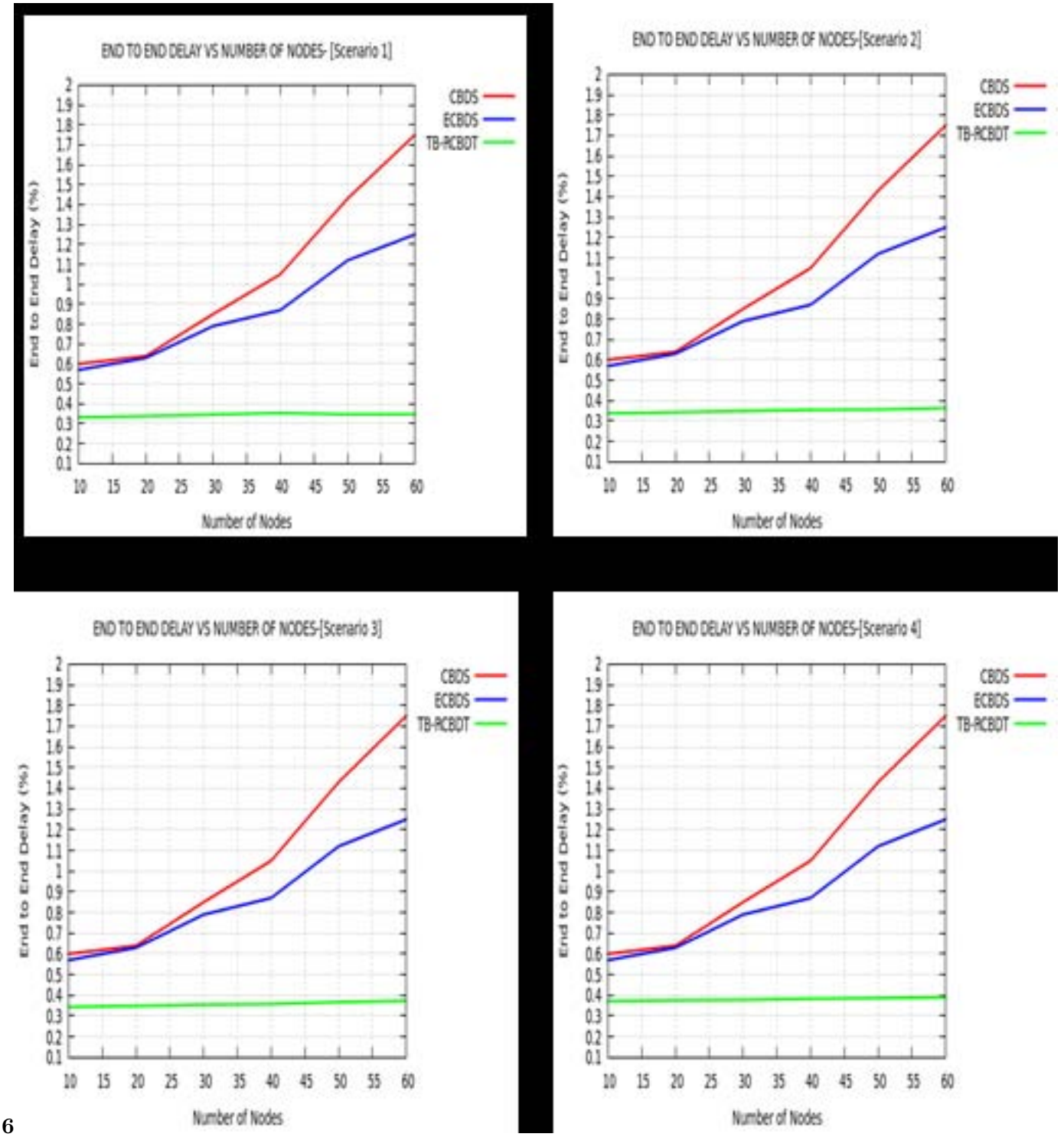
4

Figure 4: Figure 4 :



5

Figure 5: Figure 5 :



6

Figure 6: Figure 6 :

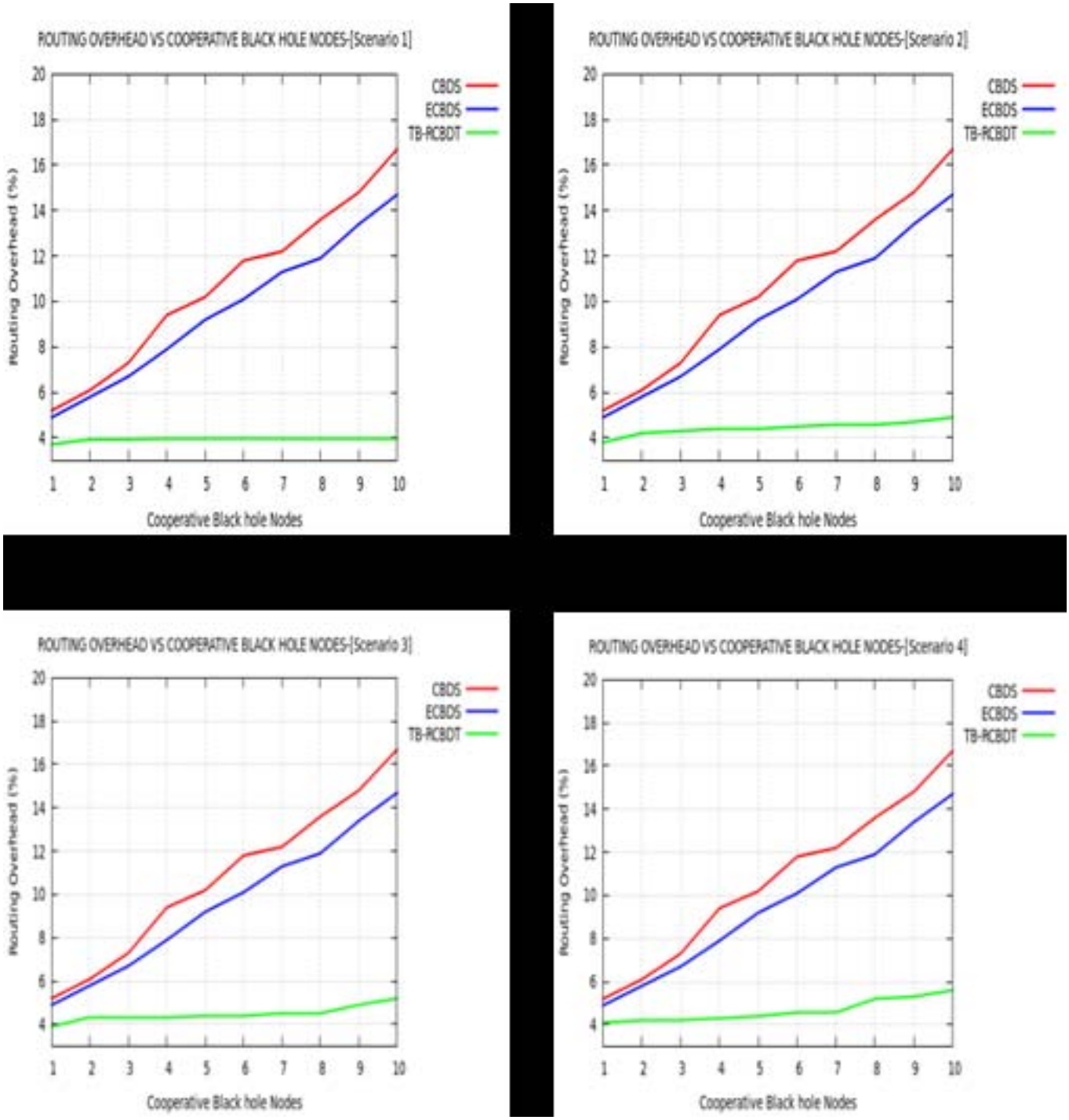
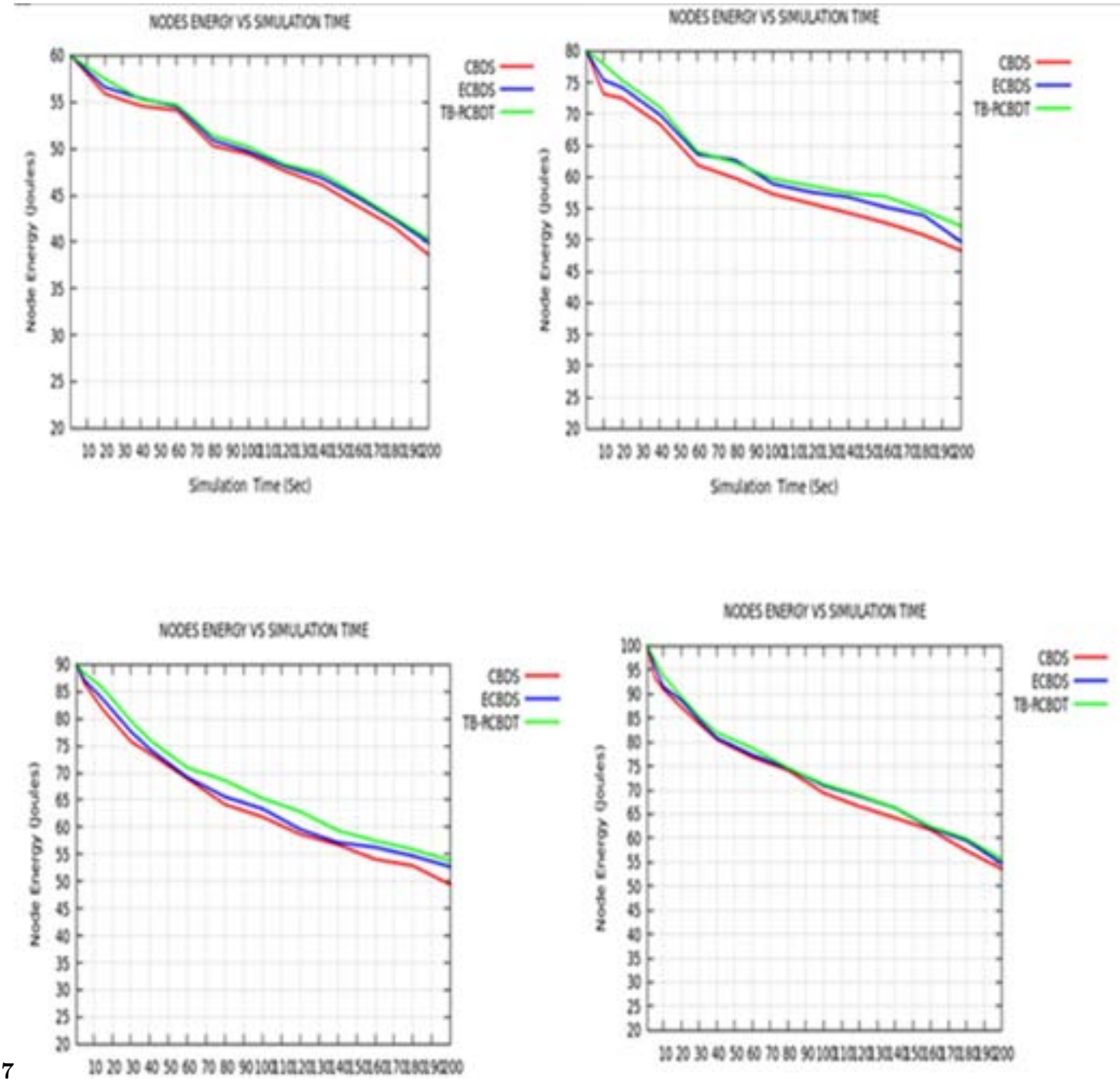


Figure 7: Global



7

Figure 8: Figure 7 :

1

Year 2020
46
Volume XX Issue III Version I
( )
Global Journal of Computer Science and Technology

Parameter	Value
Channel Type	Wireless Channel
Simulation Time	400 seconds
Number of nodes	50
MAC type	802.11 IEEE
Routing Technique	TB-RCBDT
Routing Protocol	OTB-DSR
Movement Model	Random Way Point
Traffic model	Constant Bit Rate (CBR)
Receiving Antenna	Omnidirectional Antenna
Transport layer protocol	User datagram protocol
Radio Transmission range	250 meters

Figure 9: Table 1 :

2

Simulation Experiment	Scenario 1 Packet Delivery Ratio (%)	Scenario 2 Packet Delivery Ratio (%)	Scenario 3 Packet Delivery Ratio (%)	Scenario 4 Packet Delivery (%)
1	99.88	98.81	97.65	97.37
2	99.88	98.55	97.34	98.08
3	99.88	99.08	97.97	97.74
4	99.88	98.42	97.18	97.04
5	94.88	99.47	98.44	95.43
6	99.88	98.68	99.06	96.91
Average	99.88	98.84	97.94	97.76

Figure 10: Table 2 :

3

Simulation Experiment	Scenario 1 End-to-End Delay (Sec)	Scenario 2 End-to-End Delay (Sec)	Scenario 3 End-to-End Delay (Sec)	Scenario 4 End-to-End Delay (Sec)
1	0.3332	0.3544	0.3612	0.3822
2	0.3372	0.3623	0.3734	0.3798
3	0.3417	0.3571	0.3699	0.3875
4	0.3526	0.3649	0.3711	0.3894
5	0.3522	0.3583	0.3687	0.3912
6	0.3529	0.3682	0.3706	0.3785
Average	0.35	0.3609	0.3691	0.3848

Figure 11: Table 3 :

4

Simulation Experiment	Scenario 1 Routing Overhead	Scenario 2 Routing Overhead	Scenario 3 Routing Overhead	Scenario 4 Routing Overhead
1	3.974	4.135	4.238	5.433
2	3.958	4.142	4.243	5.451
3	3.965	4.137	4.268	5.449
4	3.979	4.139	4.255	5.452
5	3.948	4.161	4.273	5.537
6	3.964	4.153	4.249	5.573
Average	3.965	4.145	4.254	5.549

Figure 12: Table 4 :

5

Simulation Experiment	Scenario 1 Nodes' Final Energy	Scenario 2 Nodes' Final Energy	Scenario 3 Nodes' Final Energy	Scenario 4 Nodes' Final Energy
1	49.256	65.78	68.34	73.47
2	49.434	66.39	69.18	74.39
3	49.389	64.99	68.76	73.58
4	49.167	65.64	69.23	73.82
5	49.336	66.47	68.65	74.14
6	49.249	65.68	68.52	74.26
Average	49.356	65.82	68.78	73.94

Figure 13: Table 5 :

[Sen et al. ()] 'A mechanism for detection of Co-operative Black hole attack in Mobile Ad-hoc networks'. J Sen , S Koilakonda , A Ukil . *Second International Conference on Intelligent Systems, Modeling and Simulation*, 2011. IEEE. p. .

[Rutvij et al. ()] 'A Novel Solution for Gray hole Attack in AODV Based MANETs'. H Rutvij , J Jhaveri , P Sankita , C D Jinwala . *Proc. of Third International Conference on Advances in Communication, Network and Computing*, (of Third International Conference on Advances in Communication, Network and Computing) 2012. Springer. p. .

[Thachil and Shet ()] 'A trust-based approach for AODV protocol to mitigate Black hole attack in MANET'. F Thachil , K C Shet . *International Conference on Computing Sciences*, 2012. IEEE. p. .

[Abdelshafy and King ()] M A Abdelshafy , P J B King . *Resisting Blackhole Attacks on MANETs', 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2016. IEEE. p. .

[Sagar et al. ()] 'AODV-Based Secure Routing Against Blackhole Attack in MANET'. R D Sagar , P N Chatur , B B Nikhil . *IEEE International Conference on Recent Trends in Electronics Information Communication Technology*, 2016. IEEE. p. .

[Gupta et al. ()] 'BAAP: Blackhole Attack Avoidance Protocol for Wireless Network'. S Gupta , S Kar , S Dhararaja . *International Conference on Computer & Communication Technology (ICCCT)*, 2011. IEEE. p. .

[Bhosle et al.] 'Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET'. A A Bhosle , T P Thosar , S Mehatre . *International Journal of Computer Science, Engineering and Applications (IJCSEA)* 2012 (1) p. .

[Dumne and Manjaramkar ()] 'Cooperative Bait Detection Scheme to prevent Collaborative Blackhole or Gray hole Attacks by Malicious Nodes in MANETs'. P R Dumne , A Manjaramkar . *5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)*, 2016. IEEE. p. .

[Emimajuliet and Thirilogasundari ()] 'Defending Collaborative Attacks in MANETs Using Modified Cooperative Bait Detection Scheme'. P Emimajuliet , V Thirilogasundari . *International Conference On Information Communication And Embedded System (ICICES)*, 2016. p. .

[Mwangi et al. ()] 'Design and Implementation of Resilient Cooperative Bait Detection Technique to Curb Cooperative Black Hole Attacks in MANETs Using DSR Protocol'. E G Mwangi , G M Muketha , G N Kamau . 10.5923/j.ijnc.20201001.01.2020. *International Journal of Networks and Communications* 2020. 10 (1) p. .

[Bindra ()] *Detection and Removal of Cooperative Blackhole and Gray hole Attacks in MANETs*, G S Bindra . 2012. IEEE. 3 p. .

[Hiremani and Jadhao ()] *Eliminating Cooperative Blackhole and Gray hole Attacks Using Modified EDRI Table in MANET*, V A Hiremani , M M Jadhao . 10.1109/ICGCE.2013.6823571. 2013. IEEE. p. .

[Sukanesh et al. ()] *Energy Efficient Malicious Node Detection Scheme in Wireless Networks*, R Sukanesh , E Edsor , M Aarthylakshmi . 2016. IEEE. p. .

[Bheemalingaiah et al. ()] 'Energy-aware Clustered based Multipath Routing in Mobile Ad-hoc Networks'. M Bheemalingaiah , , M M Naidu , D S Rao . *International Journal of Communications* 2017. 2 (5) p. . (Network and System Sciences)

[Allard ()] 'Evaluation of the energy consumption in MANET'. G P Allard . *Adhoc-Now* 2006. p. .

[Gaikwad and Ragha ()] V Gaikwad , L Ragha . *Security Agents for Detecting and Avoiding Cooperative Blackhole Attacks in MANET', International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, 2015. IEEE. p. .

[Guo and Malakooti ()] Z Guo , B Malakooti . 10.1109/WASA.2007.151. *Energy-Aware Proactive MANET Routing with Prediction on Energy Consumption, International Conference on Wireless Algorithms, Systems and Applications', IEEE*, 2007. p. .

[Ukey et al. ()] 'I-2ACK: Preventing Routing Misbehavior in Mobile Ad-hoc Networks'. A S A Ukey , M Chawla , V P Singh . *International Journal of Computer Applications* 2013. 62 (12) p. .

[Mistry et al. ()] *Improving AODV Protocol against Blackhole Attacks', International Multiconference of Engineers and Computer Scientists*, N Mistry , D C Jinwala , M Zaveri . 2010. 2 p. .

[Rango et al. ()] 'Link-Stability and Energy-aware Routing Protocol in Distributed Wireless Networks'. F Rango , F Guerriero , P Fazio . *Journal of IEEE Transaction on Parallel and Distributed Systems* 2012. p. .

[Toh ()] 'Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad-hoc Networks, Communication Magazine'. C K Toh . *10th International Conference on Practical Applications of Agents and Multi-Agent Systems*, 2001. p. .

[Soufiene et al. ()] 'Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks: Proposals and Challenges'. D Soufiene , N Farid , Z Zonghua . *IEEE Communications Surveys & Tutorials* 2011. 13 (4) p. .

[Mwangi et al.] 'Optimized Trust-Based DSR Protocol to Curb Cooperative Blackhole Attacks in MANETs Using NS-3'. E G Mwangi , G M Muketha , G N Kamau . 10.5923/j.ijnc.20201001.02.2020. *International Journal of Networks and Communications* 10 (1) p. .

[Cao et al. ()] 'Performance evaluation of energy-efficient Ad-hoc routing protocols'. L Cao , T Dahlberg , Y Wang . *Proc. IPCCC*, (IPCCC) 2007. IEEE. p. .

[Boukerche ()] *Routing protocols in Ad-hoc networks: a survey of Computer Networks*, A Boukerche . 2011. 55 p. .

[Jeenat and Tasnuva] *Securing AOMDV Protocol in Mobile Ad-hoc Network with Elliptic Curve Cryptography*, S Jeenat , A Tasnuva . (International Conference on)

[Dorri et al. ()] 'Security Challenges in Mobile Ad-hoc Networks: A Survey'. A Dorri , S R Kamel , E Kheyrkhah . 10.5121/ijcses.2015.6102. *International Journal of Computer Science & Engineering Survey (IJCSES)* 2015. 6 (1) p. .

[Shabbir ()] 'Security: 'A Core Issue in Mobile Ad-hoc Networks'. A Shabbir . 10.4236/jcc.2015.312005. `http://dx.doi.org/10.4236/jcc.2015.312005` *Journal of Computer and Communications* 2015. 3 (3) p. .

[Su et al. ()] M-Y Su , K-L Chiang , W-C Liao . 10.1109/ISPA.2010.74. *Mitigation of Black-Hole Nodes in Mobile Ad-hoc Networks', International Symposium on Parallel and Distributed Processing with Applications*, 2010. IEEE. p. .

[Saha ()] *Two-level Secure Re-routing (TSR) in Mobile Ad-hoc Networks*, H N Saha . 10.1109/MNCApps.2012.31. 2012. IEEE. p. .