Global Scientific JOURNALS

GSJ: Volume 8, Issue 7, July 2020, Online: ISSN 2320-9186

www.globalscientificjournal.com

DETECTION AND PREVENTION SYSTEM AGAINST COLLABORATIVE ATTACKS IN MOBILE ADHOC NETWORKS USING ENHANCED TRUST-BASED AODV PROTOCOL

[1]Dada Omotayo Pascal Email:, [2]DR.Alao O. D. Email: 1 dada.pascal@mapoly.edu.ng, 2 alaool@babcock.edu.ng

12 *Babcock University,Department of Computer Science,School of Computing and Engineering Sciences,*
Ilishan Remo, Ogun State, Nigeria.

ABSTRACT

Because of MANETs' self-arranging nature the Mobile Ad hoc Networks (MANETs) are effectively and ready to give an extraordinary channel to correspondence anyplace, whenever without any incorporated foundation and have a colossal potential in genuine applications like, in the military, salvage and business fields. In any case, due to its dynamic nature of the system they are vulnerable to various sort of attacks, which can hamper smooth working of the system. The standard routing conventions for MANETs don't perform well within the sight of pernicious nodes that purposefully drop packets or data; such malignant conduct is propelled by blackhole nodes. In this exploration, enhanced trust based AODV protocol with the use of sequence number approach was used with NS-3 simulator to cope with the problem of Blackhole attacks in networks. The protocol was used combined with the use of trust to eliminate the corrupt paths. The NS-3 simulation results present that the protocol used was efficient and able to thwart the effect of the blackhole attacks in different scenarios and proves to increase the ratio of successfully delivered data packets significantly.

Keywords: Mobile Ad hoc Network (MANET); Blackhole Attack; AODV, Malicious Nodes; Detection and Prevention System.

Word Count: 182

1. Introduction

Evolvement of the globe to turning into a worldwide town and the development of Mobile Adhoc Networks (MANETs) in a few structures has been incredibly affected by the effect of innovative progression and exceptional transformation in the remote correspondence innovation throughout the years.

Data Technology division continues becoming unabated at a quick pace and organizations continues drawing in an increasingly mind boggling system condition every day. With the unequivocal ascent in dangers presented to individual and friends protection, and threats on systems (and PCs); Network Administrators, IT Vendors and scientists have not yielded their endeavours in guaranteeing that the registering situations are all around verified.

In a remote correspondence organize, correspondence between nodes in the system is constrained by a focal foundation or with no framework, which is called Adhoc Networks (Vu & Soneye 2009). MANETs is an utilization of the Wireless Ad hoc Network (WANET) that interfaces portable nodes to one another (Yasin & Zant, 2018).

In Mobile Adhoc Network (MANET), correspondence or transference of information between the nodes are foundations less. Rather, the nodes cooperate to convey information that can't arrive at one another straightforwardly between themselves. As it were, nodes may fill in as a scaffold between the source node and the goal node when the source and goal nodes are not in a similar inclusion. Henceforth, there is constantly a powerful change in the topology of the system because of node portability (Mirza & Bakshi 2018).

Regardless of the various threats found focused on MANET nodes, next to zero consideration appear to have been given to certain threats including numerous nodes (Razak, Furnell and Brooke 2004). What might be answerable for this could be because of the nearness of security instruments material to wired systems in MANET (Vu & Soneye 2009).

The weakness of MANETs to security dangers are to a great extent because of dynamic topology changes, open correspondence condition, absence of focal foundation for observing and the executives, and no unmistakable resistance system (Jain, Tokekar & Shrivastava 2018).

Security ambushes and threats, for instance, wormhole attack, no availability of Service (DoS), flooding attack, emulate attack, blackhole attack, vain node getting into fiendishness, routing table flood attack, and so forth (Alani 2014), which are gathered into different classes, for instance, Active and Passive ambushes. Internal and External ambushes and the Routing and Packet Forwarding attacks (Yasin and Zant 2018) are a part of the attacks suffered by MANETs.

A portion of these malignant threats can be alluded to as single threat while some are portrayed as threats on numerous nodes (Vu & Soneye 2009). Threats on numerous nodes happen when different aggressors synchronize their endeavors to upset an objective system, prominently known as community oriented threats (Khan, Imran, Abbas & Durad 2016).

Right now, node threats against MANET will be researched and dependent on the attributes of these threats; a location and anticipation framework against these threats will be recommended.

2. Literature Review

Tremendous growth in IT/network sector in recent years can be attributed to its usefulness or relevance in many fields. MANETs' versatility as a result of its high dynamic topology and ability to self organize has made it a famous wireless network in research community (Muhammad Salman et. al, 2019).

So many researchers noticed the threats of collaborative attacks on MANETs. Hence, various researches on prevention and detection approaches are ongoing while some results from researches on preventive mechanisms against collaborative attacks have been proposed (Khan, Usman & Matiullahand, K., 2018).

Khan et. al (2018) worked on a signature-based model to mitigate the effect of a cooperative black hole attack on AODV-based MANETs. The model was implemented using OPNET simulator. The simulation was run on various numbers of malicious nodes i.e., 1, 3, 6, 9, 12 and 18. The benefits of the model proposed are achieved less processing time regarding trusted path selection, better malicious detection rate for higher number of cooperative black hole nodes, and Good throughput & average delay.

Thanuja, Sri, Ram & Umamakeswari (2018) proposed a mechanism to detect and prevent blackhole and wormhole attacks in MANETs based on the behavior of the nodes. The authors combined transmission radiation based and 3-phased approach using time factor.

Dhende, Musale, Shirbahadurkar & Najan (2017) in their exploration displayed a Secure Adhoc on-Demand Distance Vector (SAODV) that identifies dark gap and grayhole nodes relying upon neighbor nodes feeling. SAODV keep up two tables: called Neighbor List (NL) and Opinion List (OL) for all nodes in the system. NL contains ids of neighbor nodes and OL is utilized to arrange nodes relying upon their exercises in the system. At the point when the source node gets an answer to a course demand it communicates a conclusion message to neighbors mentioning their feelings about the node that claims that it has the briefest way. In the event that all nodes reacted with NO message, at that point this node is a blackhole node; if a few nodes reacted with YES message and the rest with NO message then this node is a dim gap node; else, it is a typical node. On the off chance that a dark node is recognized, a notice alert is communicated to the system. This model shows high overhead in the apportioned space for OL tables and in the traded conclusion messages.

Dorri 2017, in his exploration took a shot at a table-based way to deal with relieve the helpful dark gap threat in MANETs. Information control bundle was utilized to confirm all the nodes in the chose way and stretched out DRI table was utilized to distinguish and dispose of the malevolent dark opening nodes. The consequence of it

Khan, Imran, Abbas & Durad, (2016) built up a framework for identifying and preventing malicious nodes by conveying some extraordinary nodes called Detection and Prevention System (DPS) nodes in the MANETs, which screens the conduct of different nodes consistently. A DPS node communicates a message pronouncing a node as a wormhole nodeif the node is found to have a suspicious conduct. NS2 reproductions demonstrated that the proposed DPS extensively diminishes the quantity of bundles dropped by the pernicious nodes with low bogus positive rate (Khan et al 2016).

Arathy & Sminesh, (2016) proposed a strategy detect a non-cooperative blackhole attacks; the detection of multiple black hole (D-MBH) scheme is proposed to send a fake RREQ message to request an additional route with non-existent target address. The D-MBH scheme computes a threshold of average destination sequence number and creates a list of black hole nodes. The authors further worked on the detection of collaborative black hole (D-CBH) scheme. The difference between D-MBH and D-CBH is that the D-CBH scheme further extracts next hop information from RREP and also creates a list of collaborative black hole nodes. The paper only presents analysis and the results showed that the proposed scheme performed better than existing scheme in terms of routing overhead and computational overhead.

The exploration work by Deshmukh, Chatur & Bhople (2016) displayed a model that exclusively relies upon legitimacy bit set in Route Reply. The model accepted that the aggressor node is ignorant of legitimacy bit that ought to be sent after sending the RREP. At the point when the source node gets RREP it checks the legitimacy bit on the off chance that it is set to one, at that point it utilizes that way and in the event that not, at that point it thinks about the RREP from a blackhole node and disposes of it. The constraint of this model is the ridiculous supposition in the sense that an assailant who needs to upset a system will utilize a similar convention and investigate the system before the attack.

Khobragade & Padiya (2016) proposed a security enhancing mechanism centred on an effective discovery and avoidance method for wormhole attack named “Wormhole Attack Prevention and Detection using Authentication-Based Delay Per Hop Technique”. detection of attacks in this proposed method is done by counting number of hops and delay of every node in different routes existing in network. The network was simulated in Network Simulator 2.

Chitra and Priya, 2016 proposed a technique that discovers an alternative route to the destination node because a malicious node can be in the shortest route. The implementation of the secure route discovery protocol is performed using NS2 and by modifying AODV routing protocol.

Cai, Li and Chong (2016) in their research work came up with two schemes to prevent collaborative black hole attacks, namely: Self-Checking Scheme (SCS) and Enhanced SCS (ESCS). The three main steps used in SCS are update & maintain neighbourhood topology, liar checking, and consistency checking. In the first step, the authors utilized Hello message exchange method by to accomplish neighbourhood topology table maintenance. In lair checking step, a node executes liar checking before updating reports to its two-hop neighbours when it receives a Hello message. If a node cheats other nodes with false message that is asymmetric to the destination cache of other nodes, it will be listed into liar list and the lying-count increases. Once the lying-count is higher than a predefined threshold, the node will be put in a black list. In consistency checking step, each node executes consistency checking to make sure that received RREP message is consistent to neighbourhood topology. The ESCS improves SCS by periodically sending Hello message to two-hop neighbours. As a result, collaborative black hole nodes can be found. ESCS outperformed SCS according to the simulation results in terms of better PDR and throughput but routing overhead and end-to-end delay increases.

Arya and Singh (2015), proposed a trusted AODV to detect and avoid collaborative attacks by wormhole and blackhole. Nodes were classified into three types regarding the trust level, i.e., unreliable (ur), reliable (r) and most reliable (mr). An extra trust table was maintained for each node to record the trust value of its neighbours. The trust value of a node can be calculated as T = tanh (R1 + R2), where tanh() is a hyperbolic tangent function. Variable R1 is the ratio of packets forwarded to supposed number of packets to be forwarded, and variable R2 is the ratio of packets received from a node sent by others to total packets received. When an incoming node joins the network, its trust level is set to unreliable and the three threshold values are defined to determine its trust level, which are T_{ur}, T_r and T_{mr}. The threshold value are decided and set in simulation setting. Results showed that the trusted AODV provides higher PDR, throughput and remaining energy when compared to the wormhole AODV scheme. However, collaborative malicious nodes are capable of sending fake packets so that the trusted AODV will be compromised due to false trust value.

Sharma, Bhuriya & Singh (2015) in their paper dealt with limiting the impact of threats in MANET utilizing the idea of cryptographic directing calculation. The cryptographic method depends on Rivest-Shamir-Adleman(RSA) and Data Encryption Standard (DES) Algorithms.

Improved Secure Trusted AODV (ESTA) convention was proposed to alleviate the security issues identified with the dark gap threats in MANETs by Singh & Singh (2015). A hilter kilter key was utilized right now guarantee security over the system. Likewise, a trust-based component is utilized to choose numerous ways for the conveyance of parcels over the system. Two tables associated with the course choice are: Link-Table, which stores RREQ data got from a few neighbour nodes, and Link-information, which is a unique control bundle utilized by a middle of the road node that is a piece of the chose way. The fundamental disadvantage of the proposed approach is the overhead associated with putting away data in two distinct tables (Ali, Khan & Quaid 2015).

Aware and Bhandari (2014) utilized hash function to maintain data integrity for preventing black hole attack in their research. The hash value (SHA-TWO) of the message is computed when the message reached the destination node. If the hash values are same between the source and destination node, route is regarded as a secure. Else, the destination node broadcasts data packet error message to source node and the route marked in routing table, which will not be used any more. Simulation results showed the proposed method is superior to standard AODV in terms of higher throughput, PDR, and lower end-to-end delay.

Gong and Bhargava (2013) in their research work discussed possible collaboration among various attackers and how various signal processing and neural learning can help in the detection and mitigation of such attacks in a MANET. The research conducted proved that wireless networks are affected more compared to wired networks in a collaborative attack and so a model was proposed to ensure the minimization of the attack by immunizing the mobile ad hoc networks.

Dhurandher, Woungang, Mathur & Khurana (2013) proposed the gratuitous AODV (GAODV) algorithm by using gratuitous RREP packet. In AODV protocol, an intermediate node with a route to destination node sends RREP packet to source node after which GAODV scheme unicasts a gratuitous RREP packet to the destination node. The authors took advantage of the gratuitous RREP packet to detect malicious nodes by applying it as a CONFIRM packet. In GAODV protocol, source node unicasts the CHCKCFRM packet to destination node and blackhole node is detected because malicious node fails to send the CONFIRM packet (so that the destination node never generate CHCKC packet). Simulation results by Dhurandher et al (2013), showed that the GAODV protocol outperforms standard AODV in higher data delivery ratio but leads to longer end to end delay.

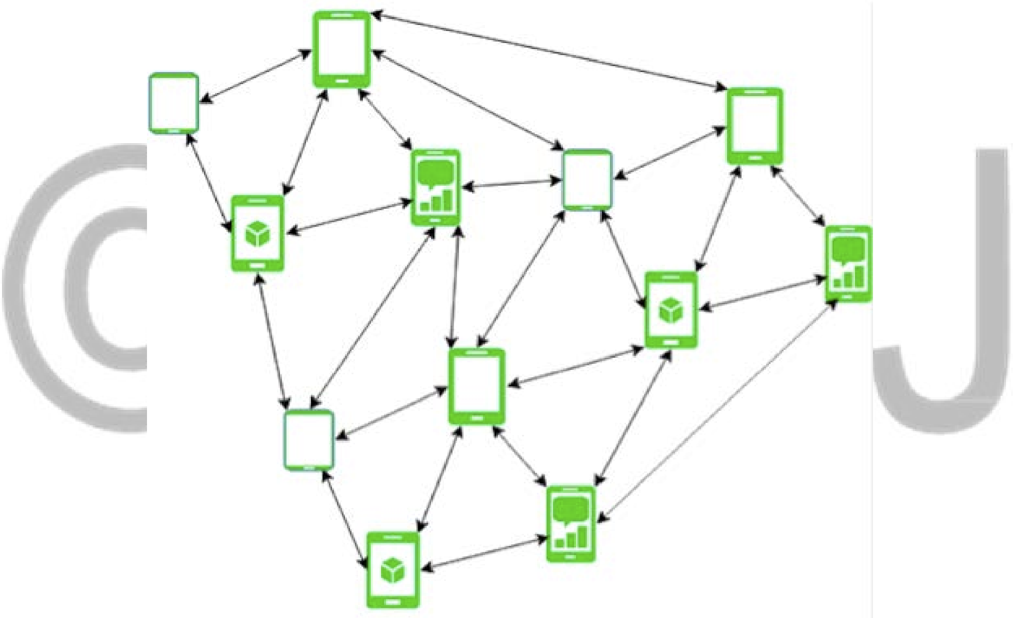


Figure 1: Mobile Ad hoc Networks' Sample. Source: geeksforgeeks.org, 2019.

a. **Some Characteristics of MANETs**

In a remote specially appointed system, an assortment of cell phones (known as 'nodes') with remote system; interfaces to frame a transitory system without the help of a brought together organization.

A portion of the trademark highlights of MANETs are (Goyal & Arora 2017):

i) **Computational Force:** Manet nodes have restricted computational force and this makes it hard or difficult to send complex directing conventions and encryption calculations for security.

ii) **Dynamic organize topologies:** The nodes in MANETs can move openly through any available path. Henceforth, the system's topology changes as often as possible and haphazardly at erratic occasions and essentially comprises of bidirectional connections.

iii) **Low data transmission:** MANETs have lower limit and shorter transmission stretch out than fixed establishment frameworks. The throughput of remote correspondence is lesser than wired counterpart in perspective on the effect of the diverse access, obscuring, uproar, and block conditions.

iv) **Battery power:** The nodes or hosts work on little modest vitality implies (called batteries). Consequently, vitality preservation is the most significant criteria or parameter for thought when planning a streamlining procedure for MANETs.

v) **Decentralized Control:** The working of MANETs relies on the collaboration of taking interest nodes because of inconsistent connections. In this way, it gets hard to actualize a convention with unified position or overseer.

vi) **Unreliable Correspondences:** The unstable channel quality and shared-medium nature of remote associations may realize high pack hardship rate and rerouting precariousness, which is a common marvel that prompts throughput drops in multi-hop frameworks. This derives the security course of action in remote off the cuff frameworks can't rely upon strong correspondence.

b. Security Challenges observed in MANETs

Systems administration works in MANETs, for example, bundles steering and sending are self sorted out and performed by nodes themselves (Rana and Gupta 2013). Thusly, security provisioning in versatile specially appointed systems is testing yet imperative errand. A portion of the objectives to be fulfilled when managing security in versatile impromptu systems are (Aarti 2013):

- **Availability**: This talks about resources accessible to or open by approved clients at reasonable occasions. The two information and administrations go under accessibility; all system administrations ought to consistently be accessible despite the fact that refusal of administration threats happens.
- **Confidentiality:** Confidentiality guarantees the accessibility and availability of all PC resources for just approved gatherings. Data traded between members ought to be shielded from unapproved clients in MANETs.
- **Integrity:** This guarantees just approved clients can get to all benefits or alter the data. Data ought to be unique while being moved to the client to guarantee Integrity.
- **Non-revocation:** This guarantees all message sent or got can't be denied by the sending and accepting gatherings.
- **Authentication:** Authentication implies that the members inside the system's correspondence are completely approved and not phony. Just validated nodes should get to the advantages of MANETs.
- **Authorization:** Authorization implies relegating different access rights like read, compose and both to different sorts of clients. A system administrator, for instance is doled out to perform organize the board assignments.
- **Flexibility to attack:** Various kinds of system functionalities ought to be kept up if various parcels are lost or nodes are undermined.

  Originality: This guarantees a recently grabbed parcel doesn't re-transmit by a malignant node.

c. Applications of MANETS

Application areas are various, and it ranges from little, static systems that are obliged by power sources to enormous scale, versatile and profoundly unique systems.

A portion of the appropriate regions include:

- **Search and Rescue Operations:** Manets are appropriate for correspondence in regions with practically no remote foundation support.
- **Disaster Relief Operations:** Manets is helpful in situations where existing framework is decimated or left inoperable.
- **Law Enforcement:** For secure and quick correspondence during law implementation activities.
- **Military Tactical Operations:** Manets may likewise be sent in Military activities for quick and conceivably momentary foundation of military correspondences and troop arrangements in antagonistic as well as obscure situations.

  Commercial Use: Manets could be progressively proficient in business situations including collective processing outside office conditions, for example, shows, meetings and huge get-togethers.

d. Blackhole Attack

An threat is said to be a blackhole threat when a noxious node is imitating a goal node and a forged course answer message sent to the source node has no powerful course to the goal. The said malignant node will in general produce undesirable rush hour gridlock and disposes of bundles got in the system (Weerasinghe 2007). The vindictive host presents itself as having the most brief way to the host being mimicked (goal node), making it simpler for the message being transmitted to be captured. Noxious node does this by holding up till it gets responses from close by nodes so as to detect the most secure course (Tamilselvan & Sankaranarayanan 2008).

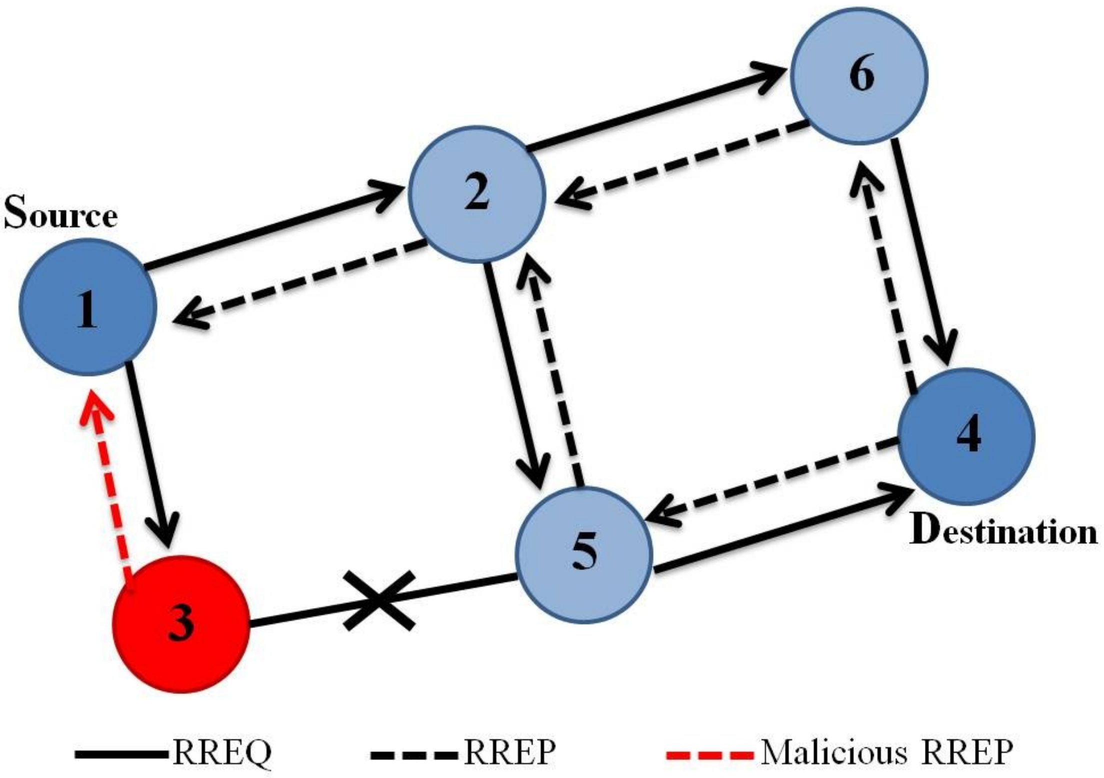


Figure 2: Single Black hole attack. Source: Tseng, Chou & Chao, 2011

The blackhole node captures the parcels originating from the source nodes and quietly drops it, which prompts colossal loss of bundles, and makes an end deferral to move the information bundles through the system. Figure 2.10 shows a model system topology where AODV convention is utilized as a steering convention.

Assume Source node "1" has information to be moved to the goal node "4", source node starts a course demand by communicating RREQ parcel to all the neighbouring nodes. The malevolent node "3" manufactures a RREP answer packet containing a mock goal address, less magnitude of jumps and littlest succession value to beguile the origin node. The origin node sends bundle by means of the course embedded in the manufactured RREP message to the goal node. Bundles that are gotten by the vindictive nodes are dropped subsequently not permitting correspondence between the sender and beneficiary.

The blackhole threats can be separated into single or agreeable blackhole threats dependent on the quantity of assailant nodes. (Figure 2.10) shows a case of a solitary blackhole node (just a single aggressor node is dynamic) while in a community oriented or agreeable blackhole threat (Figure 2.11), a gathering of assailant nodes cooperate (Joshi 2016) to corrupt the system unwavering quality (Yasin & Zant 2018).

Collective blackhole threat includes more than one node in propelling the threat. Creation of RREP bundle by all the noxious nodes with shared comprehension and participation (Rana and Gupta 2015) is approaching in a collective threat.

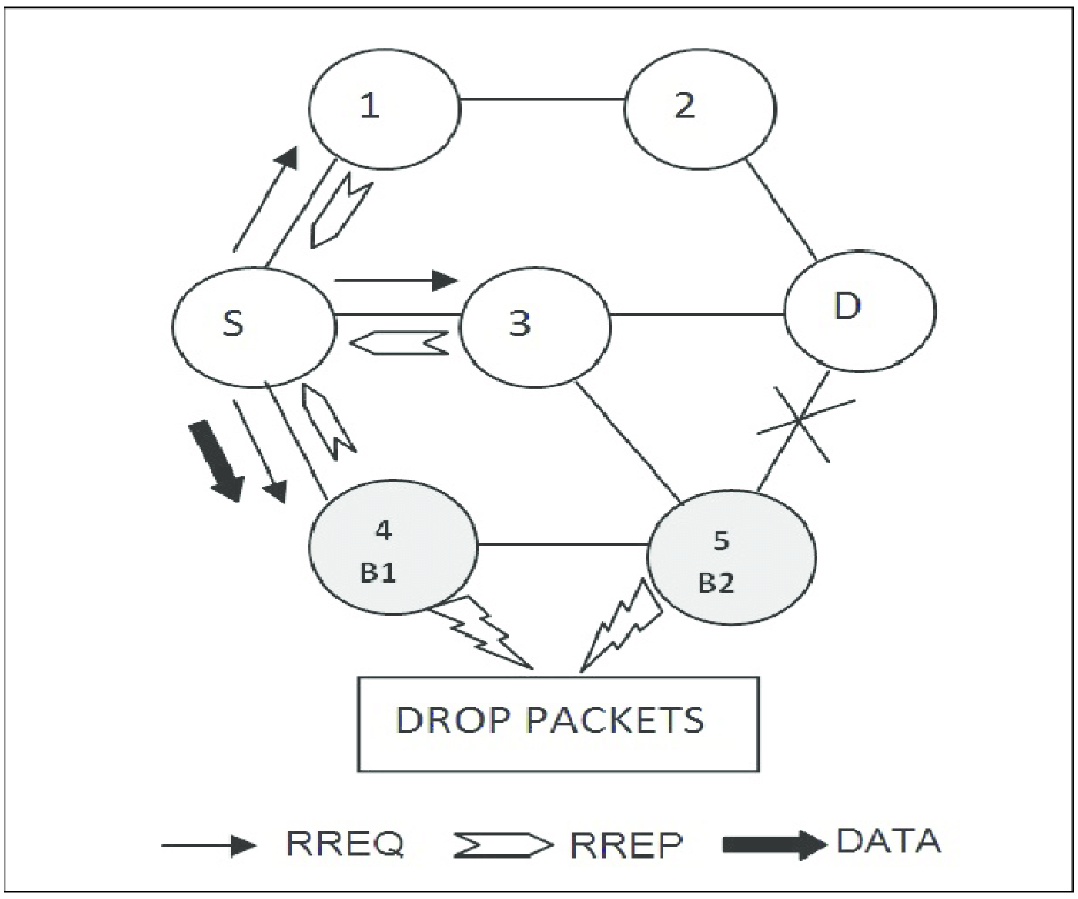


Figure 3: Collaborative Blackhole Attack. Source: Arathy & Sminesh, 2016)

Figure 2.11 is a case of a community threat propelled by vindictive nodes "B1" and "B2". The malignant nodes "B1" and "B2" by shared agreement capture the **Route Request** information and respond back to the source node. Hence, Collaborative dark opening threats are more serious than single dark gap threats and can prompt enormous packet misfortune.

3. Research Method

This work proposed a model and algorithm based on trust, adapted from Khan et al., 2018 to mitigate collaborative blackhole attacks in the MANETs routing protocol based on AODV. The proposed algorithm uses the sequence number and a trust score to classify the blackhole nodes during network communication. Route Discovery Request (RREQ) messages are also known as control packets sent by the source node along with the Route ID (RID) as the destination sequence number (DSN) of the destination node over the MANET at regular intervals and the Route Discovery Reply (RREP) message in the RREQ response to the source node after the RID match. The destination node generates a RREP.

The algorithm's pseudo code is given below:

Algorithm 1: The algorithm is written in the form of pseudo code underneath:

Algorithm 1: Signature-based Black Hole Detection

```
Input: [RREQ, RREP, Min_Seq_No, Max_Seq_No, Destination (D)]

Yield: [Accept RREQ/RREP, Reject RREQ/RREP]
```

A: Route Discovery Phase

Every node to look for extreme goal, **Destination**, among all the neighbouring hosts, utilizes course revelation stage. At the point when a source node in MANET wish to send information bundles to any goal node inside the system, it first checks whether there is any update course present in the routing table.

On the off chance that dependable course is discovered, at that point information parcels are moved through it; else start the course revelation process.

in the event that next-bounce != D && Loop free at that point

Source node, S communicate RREQ parcel to all the neighboring nodes with RID and proceeds till goal isn't investigated.

```
else

on the off chance that Min_Seq_No≤Node_Seq_No≤Max_Seq_No, at that point
```

```
Acknowledge the RREQ
Goal D is come to
else
Reject the RREQ
end if
end if
```

B: Route Reply Phase

In the store of the immediate/halfway nodes, recover the courses from course reserves.

Include these courses in the course record and afterward create the course answer bundles in a specific order.

```
if the route(s) is(are) found then
     Maintain a list of all discovered routes as List of Routes (LR).
else
     Destination host, D is not reachable due to high mobility of host and network
     partitioning;
end if
```

In Mobile Adhoc Networks-based, all hosts are allotted a sequence value ranging from minimum to maximum. The principle responsible for the proposed algorithm is to take advantage of these sequence number allotted to the node.

Assuming:

```
Min_Seq_No = the minimum sequence number,
Max_Seq_No = the maximum sequence number and
Source-Seq-No = the sequence number of the node that can be either source or destination
node.
```

If the packet sent is an RREQ packet, the Source-Seq-No represents the source sequence number. However, if the packet received is RREP, then the Source-Seq-No represents the sequence number of the destination node.

Any host that forwards a **Route Request** is valid if the sequence value of that host is greater than or equal to minimum and less than or equal to maximum sequence number (control of the proposed algorithm) allowed in the MANETs. Moreover, if the sequence value is greater than or less than the expected figure then the RREQ is termed invalid, and the host considered as malicious.

Likewise, the host that responds with a **Route Reply** packet is termed a malicious node if its sequence number does not fall between the minimum and maximum sequence value specified.

minimum and maximum sequence numbers defined.

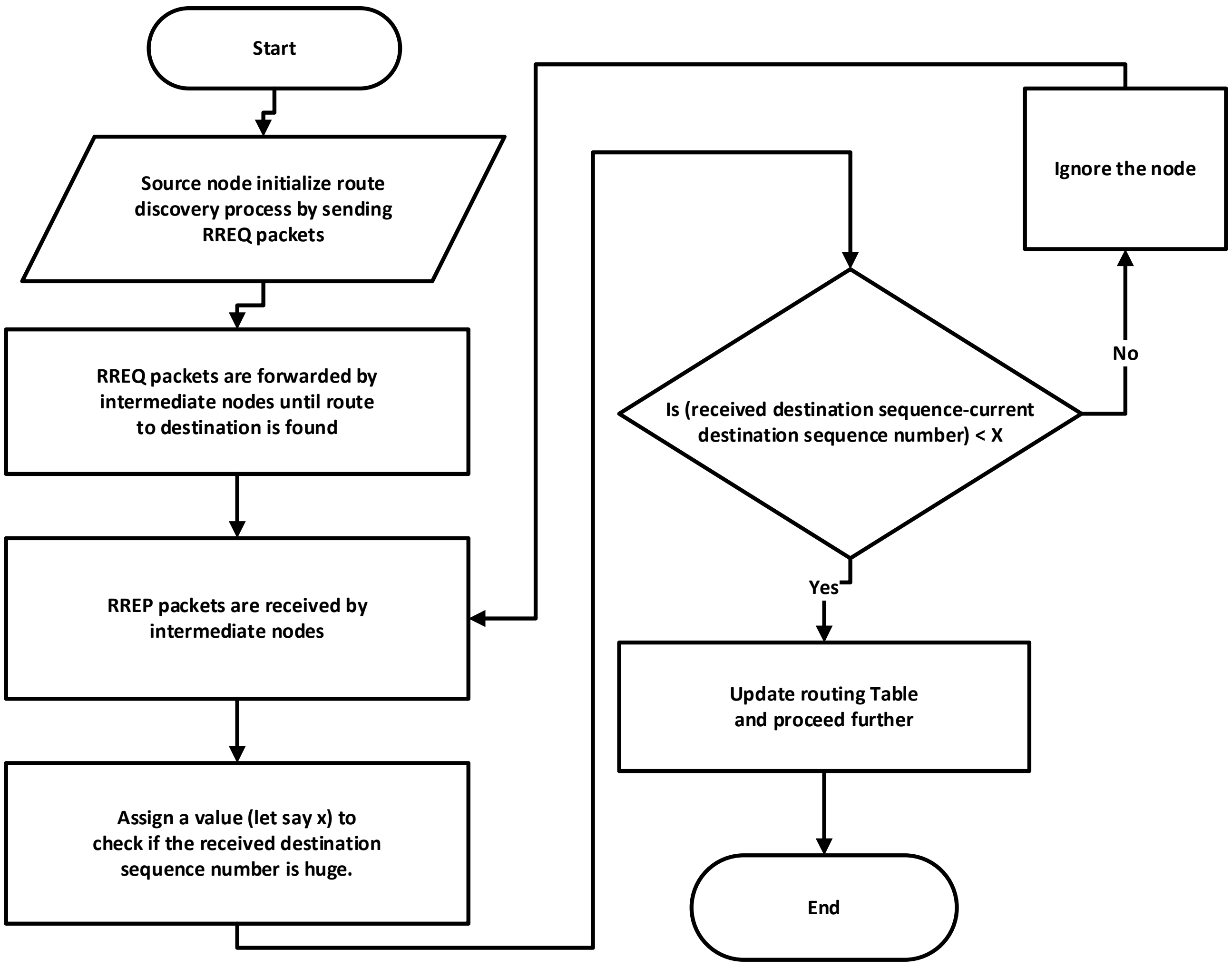

Start
Source node initialize route discovery process by sending RREQ packets
RREQ packets are forwarded by intermediate nodes until route to destination is found
RREP packets are received by intermediate nodes
Assign a value (let say x) to check if the received destination sequence number is huge.
Is (received destination sequence-current destination sequence number) < X
No
Ignore the node
Yes
Update routing Table and proceed further
End

Figure 4: Flow chart of a Detection and Prevention System Against Blackhole Attacks.Source: Khan et al.

Performance Metrics

MANET security attacks can be measured based on various performance metrics. Nonetheless, the critical metrics used in this study to assess the potential for multiple node attacks on MANETs are network throughput, end-to-end delay, packet delivery ratio and malicious detection rate.

Network Throughput: A network's throughput is the average rate of effective message delivery between the source node and the destination node thereof. It is also referred to as the ratio of the amount of data that its destination receives to the time that the last packet reaches destination (Manickam, Baskar, Girija & Manimegalai, 2011; Trang & Xing, 2005). It can be computed as:

$T = \frac{P_r}{C_t} \times \frac{8}{1024}$ ---Computation 1

T means Throughput, P_r indicates the number of packets received at the destination node, and C_t means communication time between source and destination node.

End-to-end delay (E2E): In MANETs, its end-to-end delay can determine the reliability of a routing protocol. The end-to-end delay packet of a stable network is therefore expected to be small / less and measured in milliseconds (ms). It can be computed as follows:

$A_{EtE} = \sum_{i=1}^{n} Rt_i - \frac{St_i}{n}$ --Computation 2

Average Delay from one End to another End A_{EtE}, the time packets was received at host i isRt_i, the time packets was sent at node i is St_i, and n represent the total number of hosts in the network.

Packet Delivery Ratio (PDR): This is the ratio of the total number of data packets the destination host receives to the total number of data packets sent by the source node. PDR is one of the performance metrics used to assess the efficacy and accuracy of the routing protocol of MANET. Packet delivery ratio (PDR) is expected to be high in a network.

It can be computed as follows:

$PDR = \frac{P_r}{P_s}$ ---Computation 3

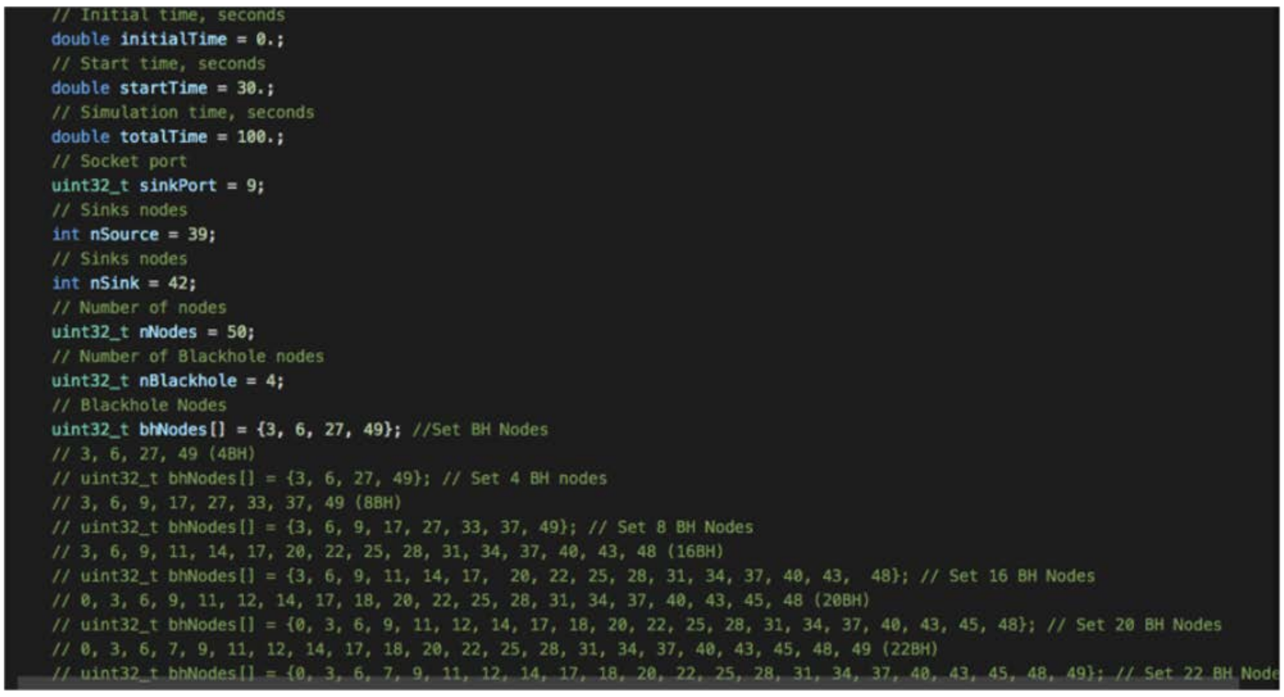
where PDR is Packet Delivery Ratio, the number of packets received at destination node is P_r and the number of packets transmitted from the source node is P_s.

Malicious Detection Rate (MDR): This is the success rate during the AODV routing cycle for detecting malicious (blackhole) nodes.

4. Result and Discussion of Findings

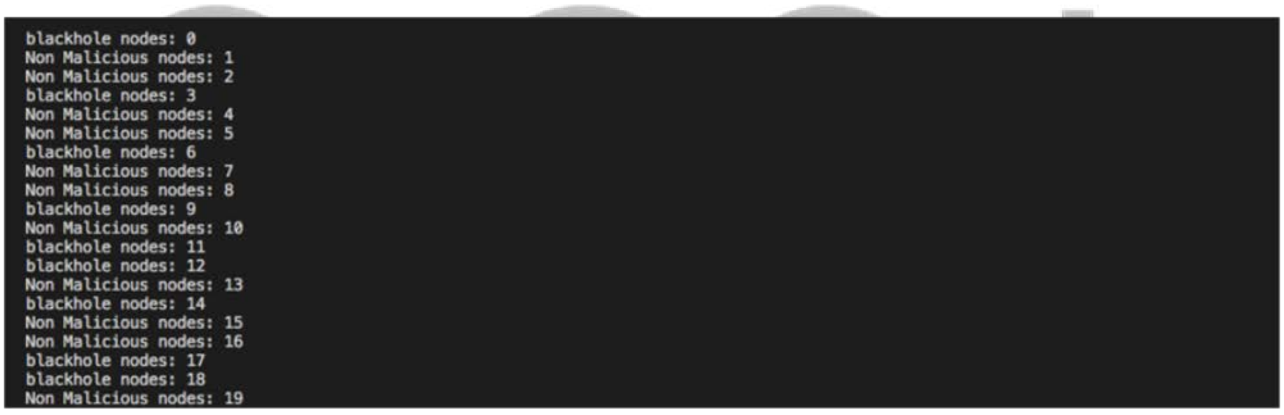
a. This section discusses the results that were obtained from the implementation of the proposed methodology of this research. Screenshots obtained from simulation are given, which were used to explain the functionalities of different interfaces of the System. These functionalities were tested to ensure that the system met its aim. Also, the efficiency of the Trust-based system is quantified by four metrics, i.e. throughput, packet delivery ratio, end-to-end delay and malicious detection rate.

b. **Design implementation:** This solution was implemented using NS3 simulator and set of separate simulation tests were carried out with a total of 50 nodes, varying number of malicious nodes (i.e. 4, 8, 16, 20 and 22) and varying source and destination nodes (Nodes 2 to 4, Nodes 1 to 4 and Nodes 39 to 42).



```
// Initial time, seconds
double initialTime = 0.;
// Start time, seconds
double startTime = 30.;
// Simulation time, seconds
double totalTime = 100.;
// Socket port
uint32_t sinkPort = 9;
// Sinks nodes
int nSource = 39;
// Sinks nodes
int nSink = 42;
// Number of nodes
uint32_t nNodes = 50;
// Number of Blackhole nodes
uint32_t nBlackhole = 4;
// Blackhole Nodes
uint32_t bhNodes[] = {3, 6, 27, 49}; //Set BH Nodes
// 3, 6, 27, 49 (4BH)
// uint32_t bhNodes[] = {3, 6, 27, 49}; // Set 4 BH nodes
// 3, 6, 9, 17, 27, 33, 37, 49 (8BH)
// uint32_t bhNodes[] = {3, 6, 9, 17, 27, 33, 37, 49}; // Set 8 BH Nodes
// 3, 6, 9, 11, 14, 17, 20, 22, 25, 28, 31, 34, 37, 40, 43, 48 (16BH)
// uint32_t bhNodes[] = {3, 6, 9, 11, 14, 17,  20, 22, 25, 28, 31, 34, 37, 40, 43,  48}; // Set 16 BH Nodes
// 0, 3, 6, 9, 11, 12, 14, 17, 18, 20, 22, 25, 28, 31, 34, 37, 40, 43, 45, 48 (20BH)
// uint32_t bhNodes[] = {0, 3, 6, 9, 11, 12, 14, 17, 18, 20, 22, 25, 28, 31, 34, 37, 40, 43, 45, 48}; // Set 20 BH Nodes
// 0, 3, 6, 7, 9, 11, 12, 14, 17, 18, 20, 22, 25, 28, 31, 34, 37, 40, 43, 45, 48, 49 (22BH)
// uint32_t bhNodes[] = {0, 3, 6, 7, 9, 11, 12, 14, 17, 18, 20, 22, 25, 28, 31, 34, 37, 40, 43, 45, 48, 49}; // Set 22 BH Node
```

Figure 5: Screenshot from the Simulation.



```
blackhole nodes: 0
Non Malicious nodes: 1
Non Malicious nodes: 2
blackhole nodes: 3
Non Malicious nodes: 4
Non Malicious nodes: 5
blackhole nodes: 6
Non Malicious nodes: 7
Non Malicious nodes: 8
blackhole nodes: 9
Non Malicious nodes: 10
blackhole nodes: 11
blackhole nodes: 12
Non Malicious nodes: 13
blackhole nodes: 14
Non Malicious nodes: 15
Non Malicious nodes: 16
blackhole nodes: 17
blackhole nodes: 18
Non Malicious nodes: 19
```

Figure 6: An interface showing Blackhole nodes during simulation.

Collaborative black hole attack simulation was performed on the AODV routing protocol and then on the adopted modified AODV protocol as a solution to mitigate the impact of the attack and the comparison.

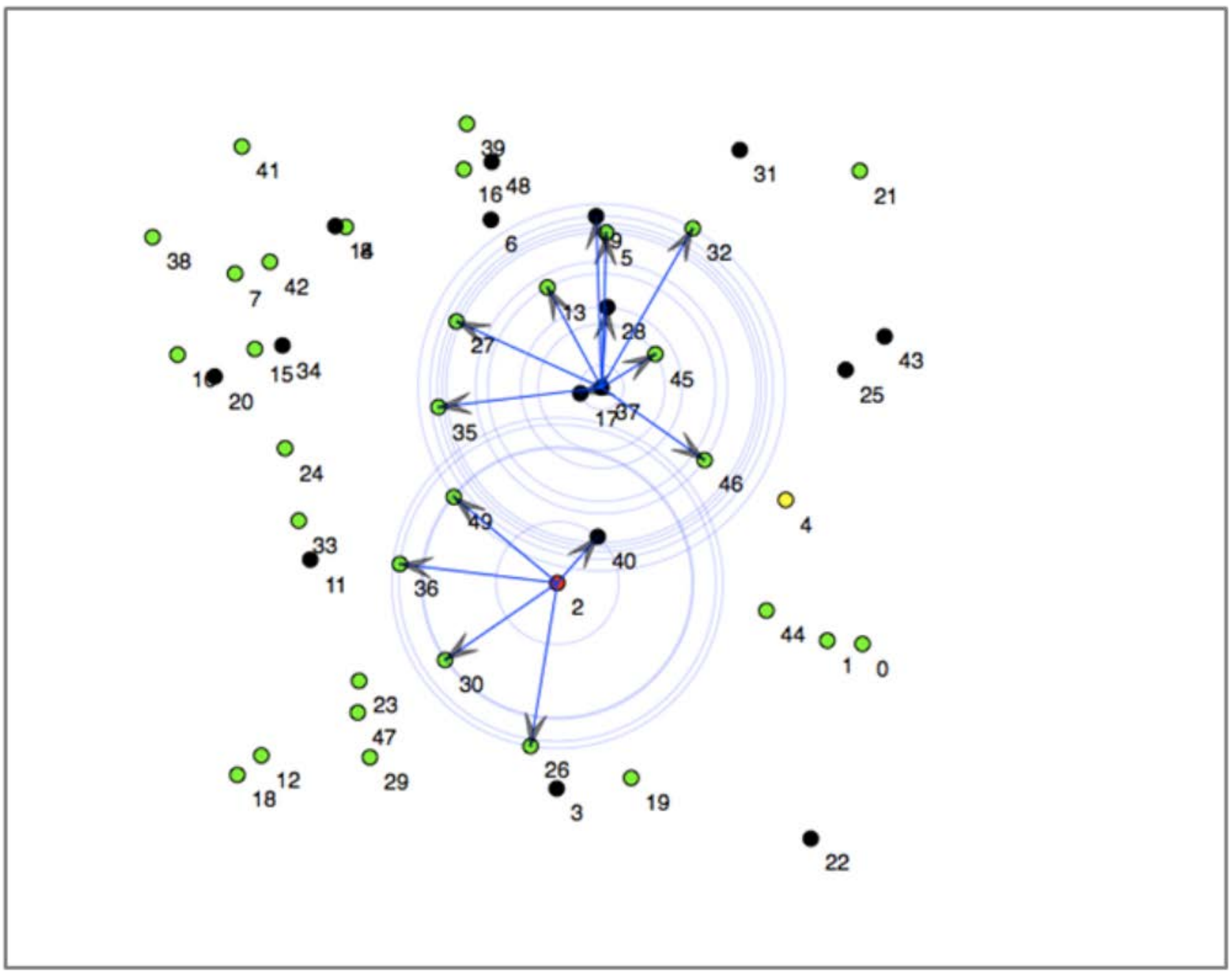
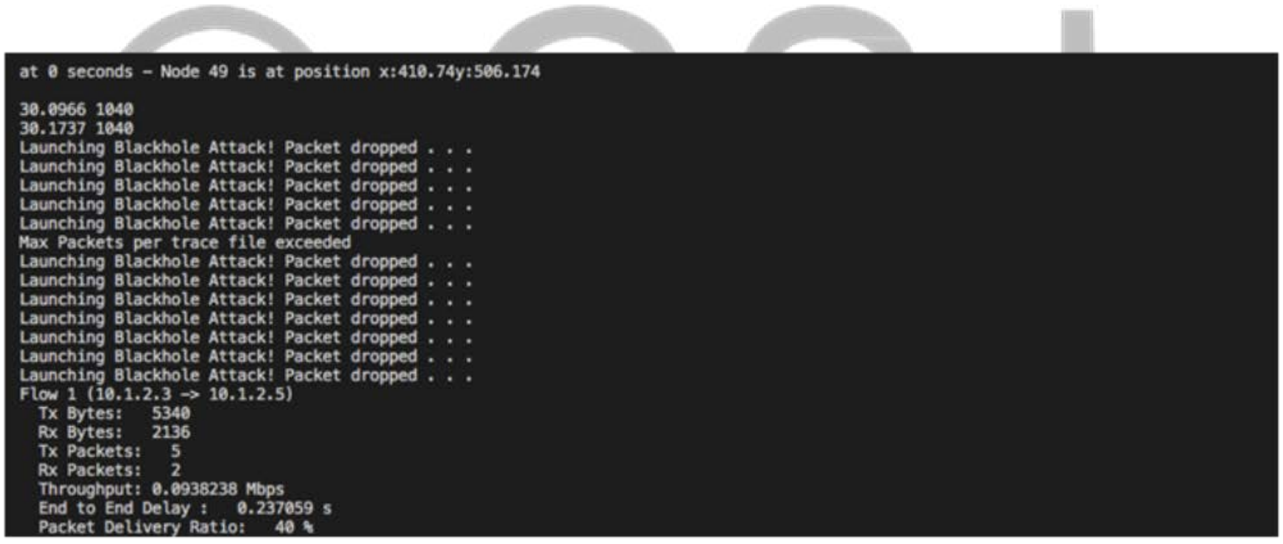


Figure 7: Interface showing Blackhole Attack. Source: NS3 NetAnim

Figure 7 demonstrates the simulation of collaborative black hole on NS3 NetAnim. The black dots represent malicious (blackhole) nodes while the red dot is the source node, the yellow node as the destination node and the green dots as the adjacent nodes during the simulation.

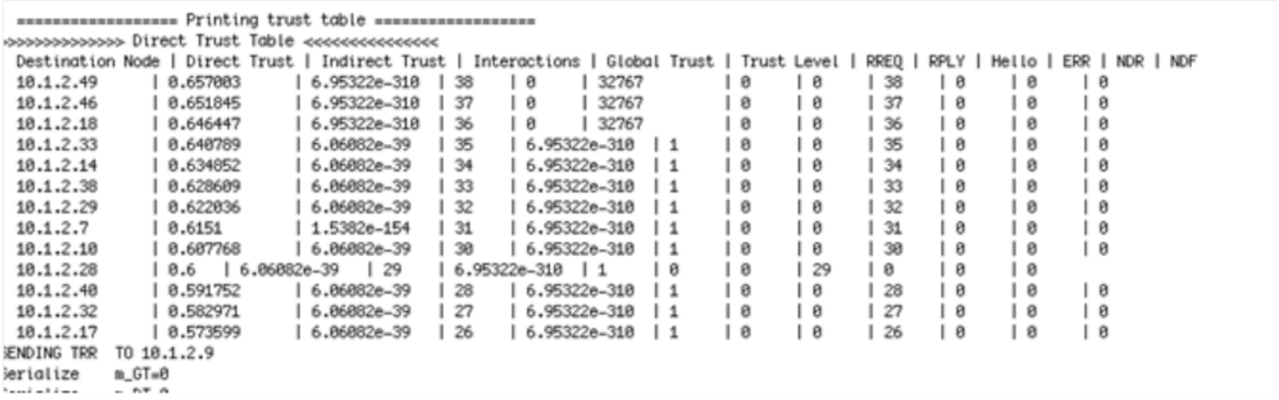


```
at 0 seconds - Node 49 is at position x:410.74y:506.174

30.0966 1040
30.1737 1040
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Max Packets per trace file exceeded
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Flow 1 (10.1.2.3 -> 10.1.2.5)
  Tx Bytes:   5340
  Rx Bytes:   2136
  Tx Packets:   5
  Rx Packets:   2
  Throughput: 0.0938238 Mbps
  End to End Delay :   0.237059 s
  Packet Delivery Ratio:   40 %
```

Figure 8: Screenshot from Simulation showing the effect of the Blackhole Nodes

In AODV, trust-based mechanism was introduced with new tables added in the routing tables showing the different trust values of the nodes at different times during the execution.



```
 ================== Printing trust table ==================
>>>>>>>>>>>>>> Direct Trust Table <<<<<<<<<<<<<<<
 Destination Node | Direct Trust | Indirect Trust | Interactions | Global Trust | Trust Level | RREQ | RPLY | Hello | ERR | NDR | NDF
 10.1.2.49        | 0.657003      | 6.95322e-310  | 38     | 0      | 32767          | 0     | 0     | 38    | 0     | 0     | 0
 10.1.2.46        | 0.651845      | 6.95322e-310  | 37     | 0      | 32767          | 0     | 0     | 37    | 0     | 0     | 0
 10.1.2.18        | 0.646447      | 6.95322e-310  | 36     | 0      | 32767          | 0     | 0     | 36    | 0     | 0     | 0
 10.1.2.33        | 0.640789      | 6.06082e-39   | 35     | 6.95322e-310  | 1     | 0     | 0     | 35    | 0     | 0     | 0
 10.1.2.14        | 0.634852      | 6.06082e-39   | 34     | 6.95322e-310  | 1     | 0     | 0     | 34    | 0     | 0     | 0
 10.1.2.38        | 0.628609      | 6.06082e-39   | 33     | 6.95322e-310  | 1     | 0     | 0     | 33    | 0     | 0     | 0
 10.1.2.29        | 0.622036      | 6.06082e-39   | 32     | 6.95322e-310  | 1     | 0     | 0     | 32    | 0     | 0     | 0
 10.1.2.7         | 0.6151        | 1.5382e-154   | 31     | 6.95322e-310  | 1     | 0     | 0     | 31    | 0     | 0     | 0
 10.1.2.10        | 0.607768      | 6.06082e-39   | 30     | 6.95322e-310  | 1     | 0     | 0     | 30    | 0     | 0     | 0
 10.1.2.28        | 0.6   | 6.06082e-39   | 29     | 6.95322e-310  | 1      | 0     | 0     | 29    | 0     | 0     | 0
 10.1.2.40        | 0.591752      | 6.06082e-39   | 28     | 6.95322e-310  | 1     | 0     | 0     | 28    | 0     | 0     | 0
 10.1.2.32        | 0.582971      | 6.06082e-39   | 27     | 6.95322e-310  | 1     | 0     | 0     | 27    | 0     | 0     | 0
 10.1.2.17        | 0.573599      | 6.06082e-39   | 26     | 6.95322e-310  | 1     | 0     | 0     | 26    | 0     | 0     | 0
SENDING TRR  TO 10.1.2.9
Serialize    m_GT=0
```

Table 1: Routing Table during the simulation on Trust based routing protocol. Source: NS-3 Simulator

N2-4	4	8	16	20	22
Throughput (Mbps)	0.248798	0.182539	0.0938238	-0	-0
PDR (%)	100	100	40	0	0
End to End (bps)	0.226972	0.28759	0.237059	0	0
N39-42					
Throughput (Mbps)	0.286616	0.286616	0.286616	0.286616	0.286616
PDR (%)	100	100	100	100	100
End to End (bps)	0.0492016	0.0482864	0.0544466	0.0502864	0.0554813
N1-4					
Throughput (Mbps)	0.286616	0.286616	0.286616	0.286616	0.286616
PDR (%)	100	100	100	100	100
End to End (bps)	0.052247	0.052247	0.052247	0.056247	0.056247
N2-4 (NM)					
Throughput (Mbps)	0.268858	0.268858	0.0152034	0.256518	0.268479
PDR (%)	100	100	40	100	100
End to End (bps)	0.211463	0.156012	2.09381	0.214383	0.228464
MDR (%)	15.1533	15.1533	10.7189	15.8823	15.1747

Table 2: AODV Results from different simulations.

NM: Malicious nodes are present in the simulation with no intention to attack.

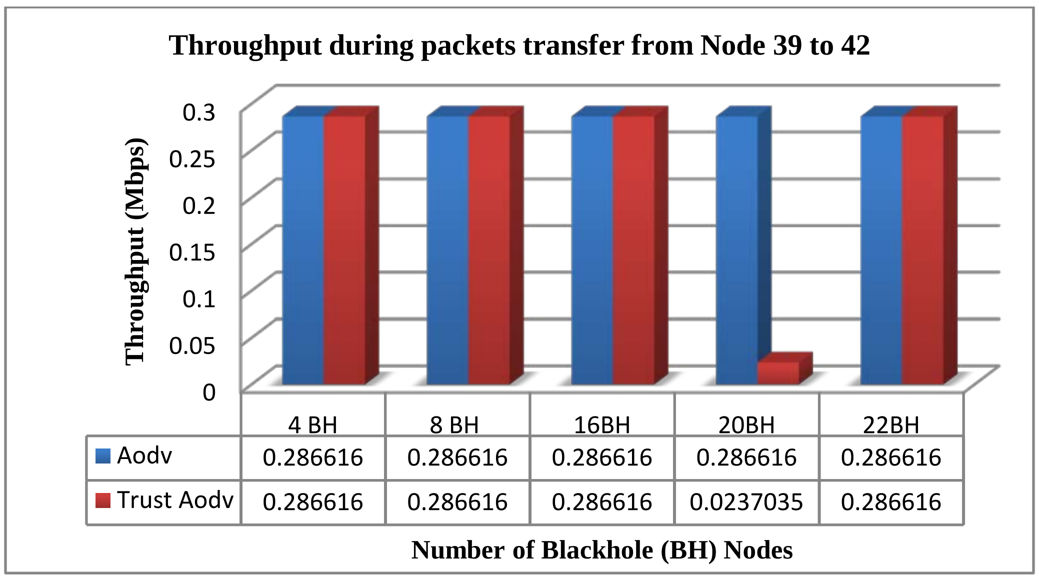
The results obtained from the various simulations on the AODV routing are shown in table 2 above, while table 3 below shows the results based on the proposed trust/signature-based mechanism. No trusted paths were found in table 3, when malicious nodes were active for simulations with 20 and 22 black-hole nodes respectively during packet transfer from source node 2 to destination node 4 during the simulation period of 100s.

N2-4	4	8	16	20	22
Throughput (Mbps)	0.22018	0.165268	0.10037	No result	No result
PDR (%)	100	100	60	No result	No result
End to End (bps)	0.350873	0.310856	0.19622	No result	No result
MDR (%)	3/4 (75)	7/8 (87.5)	14/16 (87.5)	-	-
N39-42					
Throughput (Mbps)	0.286616	0.286616	0.286616	0.0237035	0.286616
PDR (%)	100	100	100	60	100
End to End (bps)	0.0554264	0.0494064	0.0485464	2.96546	0.0485664
MDR (%)	4/4 (100)	8/8 (100)	12/16 (75)	15/20 (75)	20/22 (90.9)
N1-4					
Throughput (Mbps)	0.286616	0.286616	0.286616	0.286616	0.286616
PDR (%)	100	100	100	100	100
End to End (bps)	0.0451236	0.0451236	0.0451236	0.0485464	0.0485464
N2-4 (NM)					
Throughput (Mbps)	0.26815	0.264803	0.265472	0.266927	0.259451
PDR (%)	100	100	100	100	100
End to End (bps)	0.156704	0.192586	0.178199	0.159829	0.171082
MDR (%)	15.1933	15.3854	15.3466	15.263	15.7027

Table 3: Trust AODV Results from different simulations

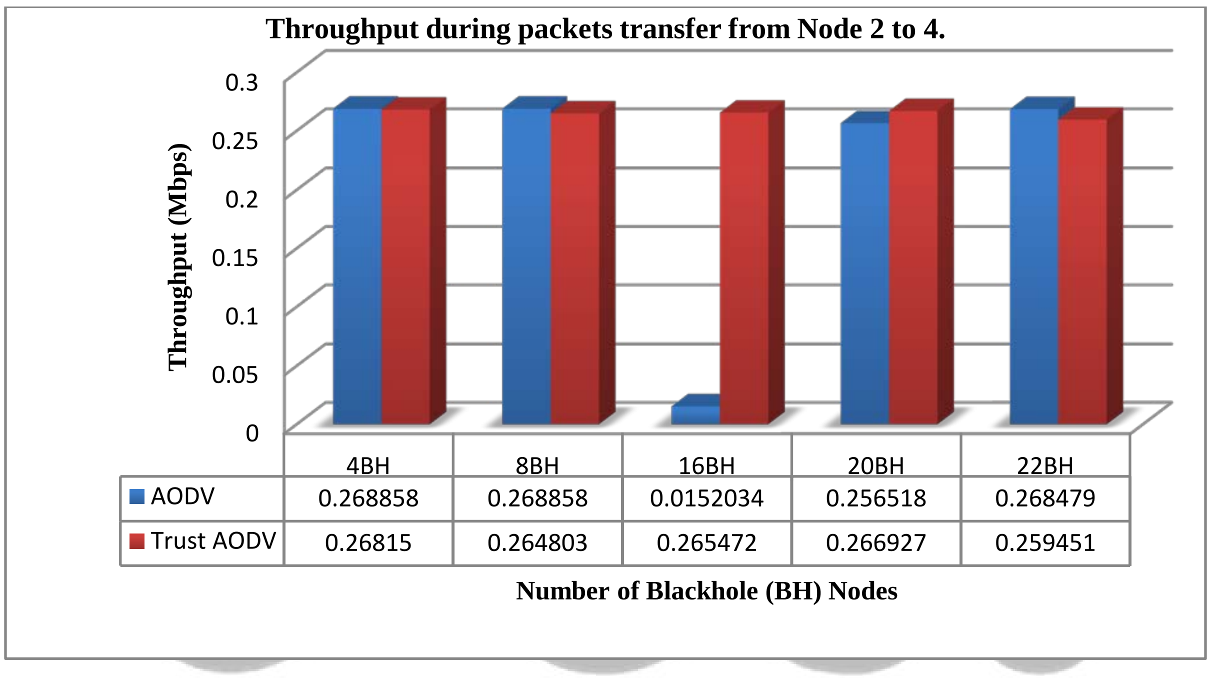
Analysis and discussion

The results of the simulation as illustrated in Figure 9 & 10 show almost identical throughput when using Node 39 as source node and Node 42 as destination node.



	4 BH	8 BH	16BH	20BH	22BH
🟦 Aodv	0.286616	0.286616	0.286616	0.286616	0.286616
🟥 Trust Aodv	0.286616	0.286616	0.286616	0.0237035	0.286616

Figure 9: Throughput during packets transfer from Nodes 39 to 42.

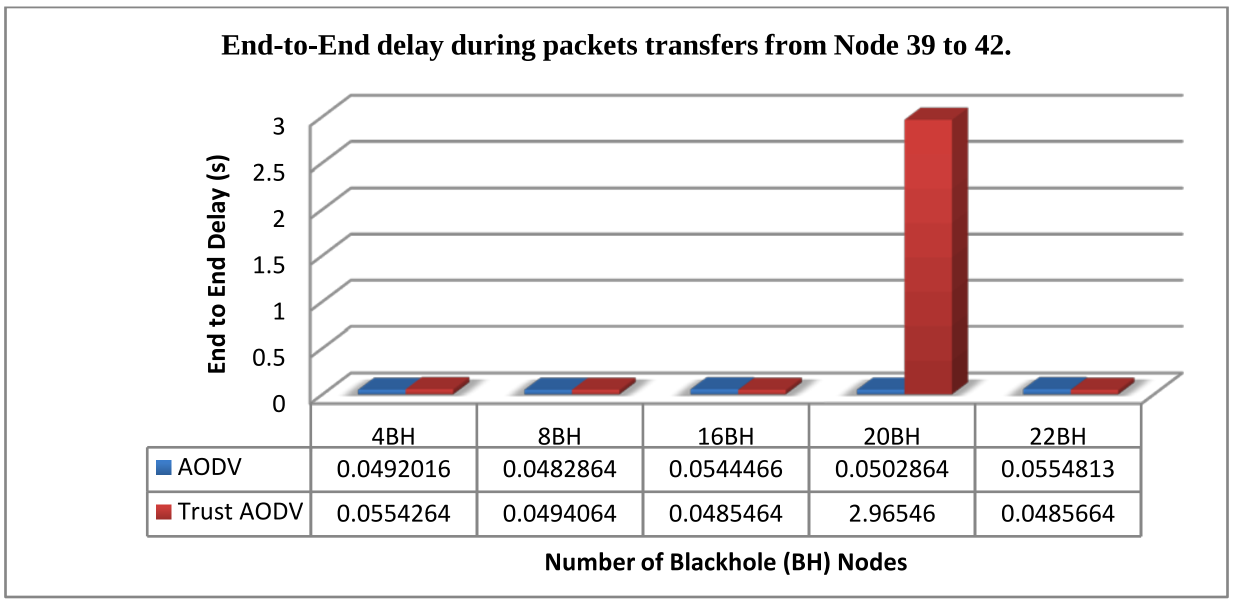


	4BH	8BH	16BH	20BH	22BH
🟦 AODV	0.268858	0.268858	0.0152034	0.256518	0.268479
🟥 Trust AODV	0.26815	0.264803	0.265472	0.266927	0.259451

Figure 10: Throughput during packets transfer from Nodes 2 to 4.

Running the simulation over the same simulating time of 100s, but changing the source node to Node 2 and destination node to Node 4 showed that the method provided a comparatively better performance as the number of blackhole nodes increased in the research.

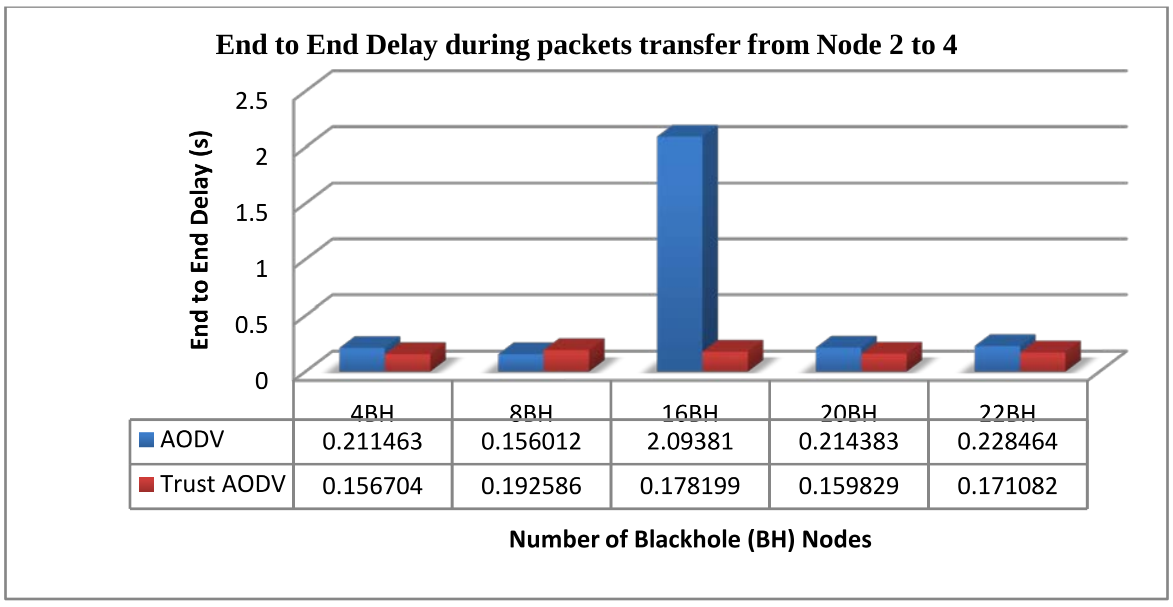
End-to-end delay is the time requires for a packet to reach its destination. Therefore, a good MANET should not have a high end-to-end delay.



	4BH	8BH	16BH	20BH	22BH
🟦 AODV	0.0492016	0.0482864	0.0544466	0.0502864	0.0554813
🟥 Trust AODV	0.0554264	0.0494064	0.0485464	2.96546	0.0485664

Figure 11: End-to-End delay during packets transfers from Nodes 39 to 42.

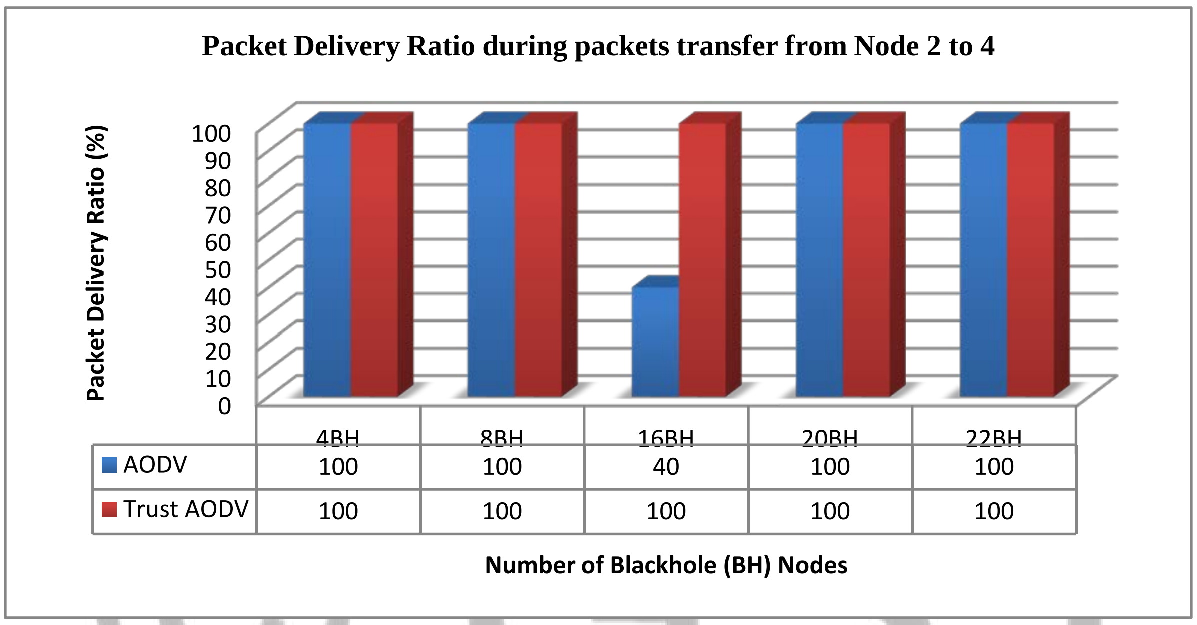
The end-to-end delay of both the AODV and the model is fairly nearly equal in a simulation with fewer blackhole nodes (e.g. 4 or 8) as shown in Figures 11 and 12. However, the mitigation results in a lower end-to-end value, as the number of blackhole nodes within the network increases.



	4BH	8BH	16BH	20BH	22BH
🟦 AODV	0.211463	0.156012	2.09381	0.214383	0.228464
🟥 Trust AODV	0.156704	0.192586	0.178199	0.159829	0.171082

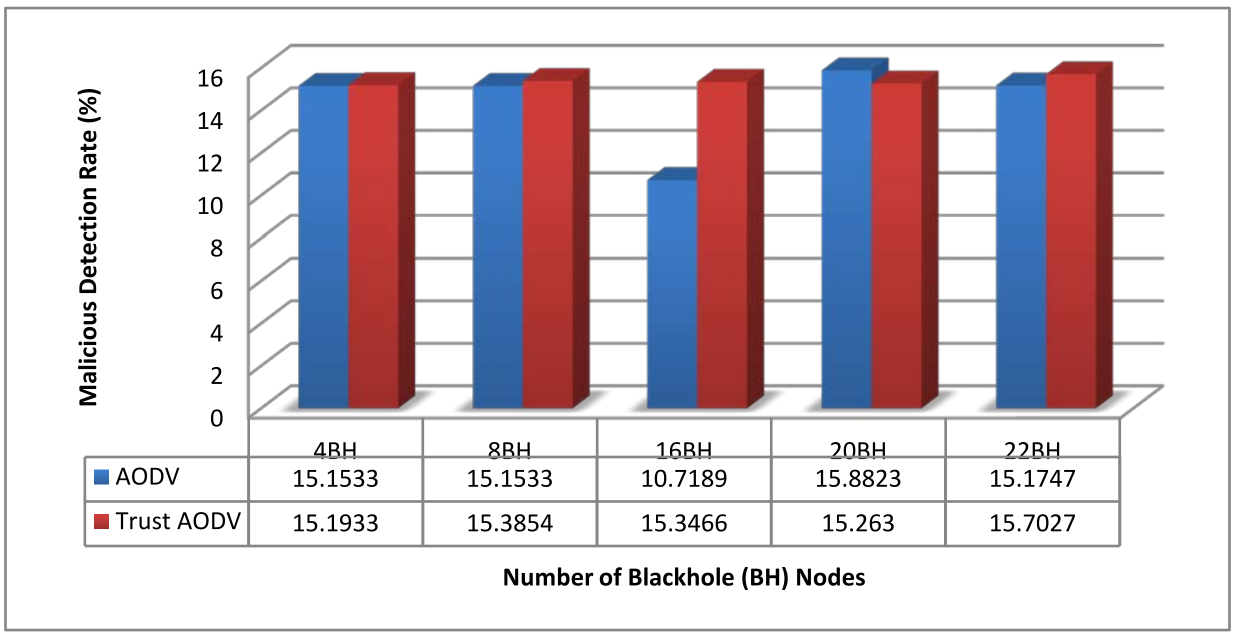
Figure 12: End-to-End Delay during packets transfer from Nodes 2 to 4

Figure 13 indicates the packet delivery ratio of the simulation with Node 2 as the source node and Node 4 as the destination node. Other simulations carried out also show similarity in PDR with the applied system being the most consistent in terms of 100% output.



	4BH	8BH	16BH	20BH	22BH
🟦 AODV	100	100	40	100	100
🟥 Trust AODV	100	100	100	100	100

Figure 13: Packet Delivery Ratio during packets transfer from Nodes 2 to 4



	4BH	8BH	16BH	20BH	22BH
🟦 AODV	15.1533	15.1533	10.7189	15.8823	15.1747
🟥 Trust AODV	15.1933	15.3854	15.3466	15.263	15.7027

Figure 14: Malicious Detection Rate during packets transfer from Node 2 to 4

Malicious Detection Rate represents the success rate of the detection of black hole attacking nodes during the routing process. Different simulation runs were made when the malicious activity of the black hole nodes was disabled for different scenarios using the AODV routing protocol and the newly proposed method as shown in Figure 14.

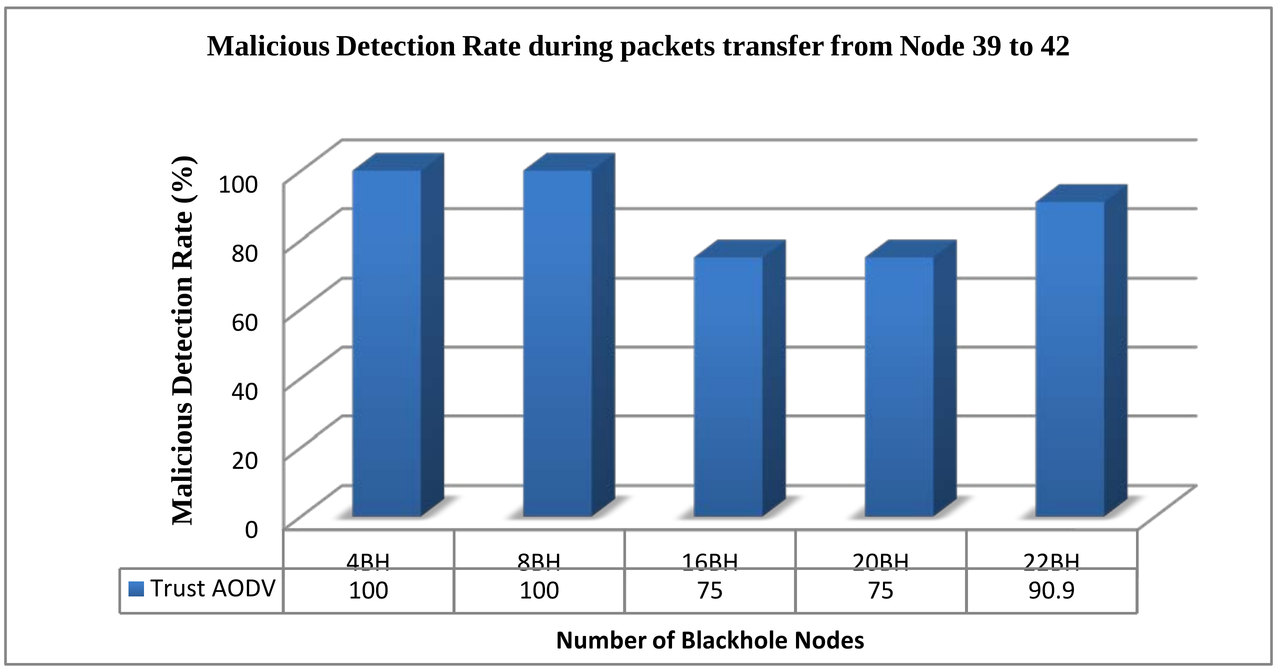


Figure 15: Malicious Detection Rate of the proposed system

During packet transfer from Node 39 to Node 42, the first two simulations of the system were effective in detecting all malicious nodes. However, the detection rate decreased by 25 per cent after the first two simulations, after which the detection rate increased to more than 90 per cent as shown in Figure 15.

5. A. Conclusion

While some methods for mitigating blackhole assaults in MANETs have been introduced, several of the proposed solutions have been capable of detecting single blackhole assaults and are unable to detect and prevent multiple node assaults in the context of AODV-based MANET. The results obtained from the simulation indicated that the goal of this research has been accomplished in terms of collaborative black hole identification and prevention, because the PDR is high and the end-to-end delay is low for most simulation runs. Therefore, based on the results, we may infer that the proposed mechanism is successful in militating against collaborative black hole attacks, as also observed in the 2018 research by Khan et al.

The applied mechanism in this research is beneficial at:

1. Better malevolent detection rate with secure routing for more malicious nodes with collective black hole attacks in MANETs.
2. Achieving less dealing out time for trusted path selection.
3. Good throughput and low end-to-end delay.

B. Summary

This research work represents an essential step towards the successful detection and prevention of collaborative black hole attacks. The adopted trust-based framework in conjunction with the use of sequence number led to the implementation of an effective approach for detecting and preventing multiple malicious node attacks in AODV-based platform MANETs

References

Arathy, K. S. & Sminesh, C. N. (2016). A novel approach for detection of single and collaborative black hole attacks in MANET," *Procedia Technology*, 25(1), 264-271.

Arya, N., Singh, U. & Singh, S. (2015). Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," *in Proceedings of International Conference on Computer Communication and Control (IC4)*, Indore, India, 2015, 1-5.

Aware, A. A. & Bhandari, K. (2014). Prevention of black hole attack on AODV in MANET using hash function," in *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization*, Noida, India,20(5), 1-6.

Cai, R. J., Li, X. J. & Chong, P. H. J. (2016). A novel self-checking ad hoc routing scheme against active black hole attacks," *Security and Communication Networks*, 9 (10), 943-957 .

Chitra, G., & Priya, P. (2016). Movement Based or Neighbor Based Technique for Preventing Wormhole attack in MANET. *Symposium on Colossal Data Analysis and Networking (CDAN).*

Deshmukh, S. R., Chatur, P. N. & Bhople, N. B. (2016). AODV- Based secure routing against blackhole attack in MANET," in Proceedings of *the 1st IEEE International Conference on Recent Trends in Electronics*, *Information and Communication Technology, RTEICT* ,1960–1964 .

Dhende, S., Musale, S., Shirbahadurkar, S. & Najan, A. (2017). SAODV: Black hole and gray hole attack detection protocol in MANETs," in Proceedings of the 2017 *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET*), 2391–2394 .

Dhurandher, S. K. , Woungang, I.; Mathur, R. & Khurana, P. (2013). GAODV: A Modified AODV against single and collaborative Blackhole attacks in MANETs", *IEEE 27th International Conference on AINA Workshops*, 357-362.

Dorri, A. (2017). An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. *Wireless Networks*, *23 (6)*,1767-1778.

Geeksforgeeks (2019). Manet Routing Protocol. https://www.geeksforgeeks.org/manet-routing-protocols.

Gong1, T. & Bhargava, B. (2013). Immunizing mobile ad-hoc networks against collaborative attacks using cooperative immune model. Article published in Wiley Online Library (wileyonlinelibrary.com), Issue: *Security and Communication Networks, 58-68.*

Imperva (2019). https://www.imperva.com/learn/application-security/intrusion-detection-prevention/. Retrieved .

Jain, A.K., Tokekar, V. & Shrivastava S. (2018). Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks. *In Information and Communication Technology, Springer, Singapore, 39-47*.

Khan, F., Imran, H., Abbas, H. & Durad, H. (2016). A Detection and Prevention System against Collaborative Attacks in Mobile Ad hoc Networks. Future Generation Computer Systems. 68. https://doi.org.

Khan, Samiullah, U. F. Khalil, B. & Fahim, K. (2018). Enhanced Detection and Elimination Mechanism from Cooperative Black Hole Threats in MANETs. *International Journal of Advanced Computer Science and Applications (IJACSA), 9(3),* 2018.

Khobragade, S. & Padiya, P. (2016). Detection and prevention of Wormhole Attack Based on Delay Per Hop Technique for Wireless Mobile Ad-hoc Network. 1332-1339. 10.1109.

Manickam, P., Baskar, T.G., Girija, M. & Manimegalai, D.D. (2011). Performance comparisons of routing protocols in mobile ad hoc networks. arXiv preprint arXiv:1103.0658, 2011.

Mirza, S. & Bakshi, S. Z. (2018). Introduction to MANET. *International Research Journal of Engineering and Technology*, 5(1), 17–20.

Razak, S. A.; Furnell S. M. and Brooke P. J. (2004). Attacks against Mobile Ad Hoc Networks Routing Protocols.

Routing in MANETs (2019). https://goo.gl/LdjeVk

Sharma, A., Bhuriya, D. & Singh, U. (2015). Secure data transmission on MANET by hybrid cryptography technique. *IEEE 2015 International Conference on Computer, Communication and Control (IC4),* 10-12 Sept. 2015 pp. 1-5.

Tamilselvan, L. & Sankaranarayanan, V. (2008). Prevention of co-operative blackhole attack in MANET. *Journal of Networks*, *3*,(13-20), 2008.

Thanuja, R., Sri R. E. & Umamakeswari, A. (2018). A Linear Time Approach to detect wormhole tunnels in MANET using 3PAT and Transmission Radious (3PATw). *Procedings of the second International Conference on Inventive System & Control (ICISC),* 837-843.

Trang, N. V. &Xing, X. (2005). Rate-adaptive Multicast in Mobile Adhoc Networks", WiMob'2005, 3(1), 352-360.

Tseng, F., Chou, L. & Chao, H. (2011). A survey of black hole attacks in wireless mobile ad hoc networks" Human-centric Computing and Information Sciences.

Vu, C. H., Soneye & Adeyinka (2009). An Analysis of Collaborative Attacks on Mobile Ad hoc Networks. School of Computing, Blekinge Institute of Technology. Lambert Academic Publishing, Germany ©2010. ISBN: 3838369750 9783838369754

Yasin, A. & Zant, M. A. (2018). Detecting and Isolating BlackHole Attacks in MANET Using Timer Based Baited Technique. Hindawi Wireless Communications and Mobile Computing, Article ID 9812135, 10 pages https://doi.org/10.1155/2018/9812135.

Yun, J., Kim, I., Lim, J. & Seo, S. WODEM: Wormhole Attack Defence Mechanism in Wireless Sensor Networks. ICUCT 2006, LNCS 4412, 200–209.