IST-Africa 2019 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2019
ISBN: 978-1-905824-63-2

A Review of Security Techniques against Black hole Attacks in Mobile Ad hoc Networks

Ephantus Gichuki MWANGI[1] , Geoffrey Muchiri MUKETHA[2] , Gabriel Kamau NDUNGU[2]
[1]*Kirinyaga University, P.O Box 43-10300, Kerugoya, Kenya*
Tel: +254 0723814846, Email: egmkuc@gmail.com
[2] *Murang'a University of Technology, P.O Box 75-10200, Murang'a, Kenya*
Tel: +254 0713108597, Email: gimuchiri@gmail.com, kamau.gabriel@gmail.com

Abstract: Mobile ad hoc network (MANET) is a special type of a wireless network formed by nodes that communicate without any fixed infrastructure or centralised management. Nodes in MANET act as a router and a host. These nodes are free to join and leave the network. Routes are established by use of special routing protocols. Mobility of nodes makes the network topology dynamic at any given time. These unique features together with unsecured boundaries make the security of MANETs a challenging endeavor. MANETs are prone to attacks such black hole among others. Sometimes the black hole nodes cooperate forming cooperative black hole attack that drop or redirecting data packets. This paper reviews various security techniques and routing protocols against black hole attacks and establishes their limitations. The identified knowledge gaps will be used as a foundation for the development of a resilient security technique against collaborative black hole attacks.

Keywords: Mobile Ad hoc Networks, Security Technique, Routing protocol, Route Request, Cooperative black hole attack.

1. Introduction

Mobile Ad hoc Network (MANET) is a special type of wireless networks that is decentralized and lacks physical infrastructure. Nodes in MANETs freely join and leave the network at their own will, hence making the network have a dynamic topology. Nodes cooperate to forward data packets from source to destination using routing protocols. Each node in a MANET acts as both a router and a host. A node wishing to communicate with other nodes in MANET establishes a route using special routing protocols [1].

Several routing protocols have been designed to optimize MANETs routing performance [2], [6]. Major issues involved in designing MANETs routing protocol are dynamic network topology, constrained bandwidth, limited battery power, error prone wireless channel, and node mobility. These unique features of MANETs make most of the security solutions designed for wired networks inappropriate for mobile ad hoc networks. The dynamic nature of MANETs makes it difficult to establish secure ad hoc routing protocols [3].

MANETs routing protocols are categorized into three types: reactive routing protocols (on demand), proactive routing protocols (table driven) and hybrid protocols. In reactive routing protocols routes are created on-demand whenever a source node wishes to send data packets to a destination node. This means that only nodes which participate in active route maintain routing information. AODV, DSR and LAR are some of the examples of reactive routing protocols [6]. In proactive protocols, each node maintains complete routing information of the network. Change in the network topology due to nodes mobility leads to automatic updating of routing tables in all the nodes. Examples of proactive routing protocols are DSDV, GSR

and HSR. Hybrid protocols are as a result of blended features of both proactive and reactive routing protocols [4].

1.1 – Background

MANETs communicate using open wireless medium which paves way for an attacker to easily intercept the communication process. The unique characteristics of MANETs make it susceptible to various denial of service routing attacks (such as black hole) which causes packet dropping [7], [5].

During a black hole attack, malicious node masquerades to be genuine by claiming that it has the shortest and freshest route to destination by responding to the Routing Request (RREQ) of a source node with a fake Route Reply (RREP). This makes the source node to select the route with black hole node as an optimal choice for data transmission. Once the black hole node starts receiving the packets from source node instead of forwarding them to the destination it simply discards the packets. In MANETs black hole attack comes under the category of active attacks. [7]. In cooperative black hole attacks more than one malicious node collaborates with each other to launch attacks that are more harmful to the network than any other attacks [8].

The rest of the paper is organized as follows; section2 presents objectives of the study, section 3 presents methodology used, section 4 presents MANETs' security techniques, section 5 describes MANETs routing protocols, section 6 results while section 7 presents conclusion and future work.

2. Objectives

This paper is a review existing security techniques and routing protocols with an aim of establishing their limitations against black hole attacks in MANETs.

3. Methodology

The next section of this paper discussed the existing literature on MANETs' security techniques and routing protocols, broadly under black hole and cooperative black hole attacks. Keyword analysis was used to search relevant journals from IEEE and Elsevier journal databases.

4. MANETs Security Techniques

In [9], Mistry et al. proposed a security technique in which a source node after receiving the first RREP waits for particular time interval and stores all the RREP's received during that interval. The source node analyzes all the RREP's and ignores all the RREP's having a very high sequence number. In this technique, it is observed that there was an increase in the average end to end delay. Further, a heuristic approach was used in deciding the time interval for a node to wait.

Su et al. [10] proposed an anti-black hole technique that uses intrusion detection system (IDS) nodes for the detection of black hole nodes. In this technique, every IDS node estimates the suspicious value of a node based on the difference between the numbers of RREQ's and RREP's forwarded by a node. If the suspicious value of a node goes beyond the threshold value, then the IDS node broadcasts a block message to all nodes on the network in order to work together in mitigating the black hole node. Once a node receives the block message from the IDS, it places the malicious node into its blacklist. In this technique, it is noted that extra nodes have to be placed in the network and every IDS has to sniff the RREQ and RREP's of all nodes, this may be an extra overhead for a MANET with many nodes.

Sen et al. [3] proposed a technique in which a node (IN) generating the RREP has to send the Data Route Information (DRI) entry of its next hop (NHN). The source node then sends FREQ request to the NHN. Further, NHN node replies FREP with DRI entry of IN. The source node cross checks the entries of IN and NHN and if they match then the node is genuine, else IN is malicious. It is observed from this technique that the FREQ and FREP extra control packets are required which increases routing overhead.

Gupta et al. [11] proposed a technique which uses Ad hoc On-Demand Multipath Distance Vector (OMDV) to provide multiple paths during routes discovery process. The intermediate nodes in the network have multiple paths which lead to the destination node. However, the source node selects only one path among them. Each node in the network maintains a legitimacy of all nodes that are under its neighborhood. In this technique, nodes try to avoid paths that pass through nodes with legitimacy value less than threshold. This helps in identifying the nodes behaving maliciously, hence avoiding them. This method works fine with one black hole node but dealing with cooperatives black hole nodes would be a tedious undertaking.

In [12], Saha et al. presented a Two-Level Secure Re-routing (TSR), a novel routing architecture for MANETs which attack resilient. TSR employs a two-level approach that uses Local Supervision (LS) and Congestion Window Surveillance (CWS) modules to detect network attacks at the transport layer. TSR then responds to these attacks using the Alternate Route Finder (ARF) module that executes re-routing at the network layer. Simulation analysis showed that TSR is resilient against a variety of insider attacks as well as protocol-compliant attacks. This architecture can also be used in controlling black hole nodes as they are a variant of DoS attacks. However, LS and CWS modules introduce routing overhead during data transmission.

In [13], Bhosle proposed a technique based on watchdog and pathrater mechanism. In this technique, each node maintains two tables: pending packet table and node rating table. Every node stores packet forwarded in the pending packet table and overhears its neighbors. If the neighboring node sends the packet in the forward direction, then the value of the packet forwarded in node rating table is incremented. Further, if the packet is dropped, then that value is decremented. If the value of dropped packets in the node rating table goes beyond a threshold value, then that node is considered to be malicious. This technique requires extra memory space to store multiple tables. Further, extra time is incurred for frequently monitoring of the two tables. This technique suffers from routing overhead due to the two tables introduced.

Thachil [14] presented a technique in which every node performs overhearing of neighboring nodes and calculates their trust value. Each node keeps a copy of a packet in the cache before forwarding it and then overhears the packets forwarded by the neighboring node. If a packet forwarded by the neighboring node matches with the packet in the cache then the sending node believes that the neighboring node is genuine; otherwise its trust value is decremented. Each node maintains a trust value that is updated dynamically and if the trust value of a node goes beyond threshold that node is considered to be malicious. In this technique, it is observed that routing overhead at a node level increases due to the fact that a node has to keep copies of packets in its cache and overhear all its neighbors.

In [15], Bindra et al. proposed a security technique using AODV protocol that detect and remove black hole and gray hole attacks. The technique maintains an extended data routing information (EDRI) table at each node in addition to the routing table of AODV protocol. The EDRI table is an extension of DRI Table and is able to identify cooperative black nodes in MANETs. Further, it can discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. Limitation of this technique is that malicious nodes have to be in sequence while acting in cooperation for them to be discovered by the

algorithm. Additionally, routing overhead is experienced due to many packets introduced in the EDRI table. Further, the algorithm needs to be optimized for efficient usage.

Ukey [16] proposed a 1-2ACK technique for preventing routing attacks in MANETs. In this technique, all the nodes that form a path for transmitting packets are grouped into sets of three adjacent nodes. When a node sends a packet, it waits for an acknowledgement ACK1 from the Rnode (right node) of its own set and ACK2 from Rnode of the next set. If a node does not receive both of the acknowledgements from both sets, then there exists a malicious node. In this technique, the need for extra control packets introduces routing overhead as well as end to end delays.

In [17], Hiremani & Jadhao proposed a security technique to remove cooperative black hole attacks by using modified extended data routing information (MEDRI) table at each node with the routing table of AODV protocol. Simulation results show that this technique is capable of detecting both consecutive and nonconsecutive cooperative black hole attack. The MEDRI table has the capability of recording and maintaining a history of the previous malicious nodes. This history is used for future discovery of secure paths from source to destination. However, this technique suffers from routing overhead and end to end delay due to the introduction of data packets in the MEDRI table.

Gaikwad & Ragha [18] proposed a technique which uses cooperative cluster agents (CCAs) to detect and avoid cooperative black hole attacks in MANETs. In this technique, DRI and SRT-RRT tables are used as input to CCAs. Simulation results show that the technique successfully detected black hole and cooperative black hole nodes in MANETs. Further, the technique identified secure routing path from source to destination by avoiding the black hole nodes. The new technique was compared with the standard AODV protocol and proved to be more superior in terms of throughput, packet delivery ratio and end to end delays. However, this technique experiences routing overhead due to the introduction of DRI and SRT-RRT tables. Additionally, packet delivery ratio and throughput need to be further improved to hit the optimum level.

In [19], Dumne and Manjaramkar proposed a hybrid defense architecture known as Cooperative Bait Detection Scheme (CBDS) based upon DSR mechanism. This scheme uses proactive and reactive defense architectures to detect malicious nodes that launch collaborative black hole attacks. Simulation results show that CBDS using AODV performs better than DSR protocol and CBDS using DSR in terms of throughput and packet delivery ratio. From the above results, CBDS using AODV was considered as a better alternative because it reduced routing overhead. However, the new technique didn't perform better than CBDS using AODV in terms of throughput and packet delivery ratio. This gives room for enhancement of the new technique in order to improve performance efficiency. Further, introduction of reverse tracing technique led to the introduction of end to end delay in data transmission.

Emimajuliet & Thirilogasundari [20] proposed a Modified Cooperative Bait Detection Scheme (MCBDS) for defending collaborative attacks caused by black hole and jellyfish. Simulation results indicated that MCBDS along with DSDV protocol performs better than the DSR and 2ACK scheme. However, this scheme suffers from routing overhead compared to DSR protocol. A hybrid technique needs to be explored which would be a combination of MCBDS with other techniques in order to effectively secure routing of packets.

Abdelshafy and King [6] introduced black hole resisting mechanism (BRM) on AODV routing algorithm to detect and avoid black hole attack in MANET. During the simulation experiment, AODV and BRM AODV routing algorithms were subjected to black hole attacks in order to study their performance. Simulation results showed that BRM-AODV was superior in all network performance metrics over AODV and SAODV routing protocols. The proposed mechanism detected black hole nodes easily regardless of the number of malicious nodes. Further, the results of study showed that BRM can effectively increase the

performance of AODV routing algorithms in MANETs. However, BRM AODV was not able to detect collaborative black hole attacks. Additionally, performance metrics such as packet delivery ratio, throughput and routing overhead need to be enhanced in the new mechanism in order to increase network performance.

5. MANETs Routing Protocols

In [21] Sreenath at al. proposed an algorithm using Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP). The algorithm focused on improving the security of MANETs against multicast attacks. The proposed algorithm was implemented and tested using GloMoSim (2.03). Further, performance analysis through a simulation showed improvement in packet delivery ratio in presence of black hole attack, with marginal rise in average end to end delay and normalized routing overhead. Additionally, simulation showed that this technique works well for flooding attacks even when the identity of the malicious nodes is unknown. This mechanism does not use any additional network bandwidth during data transmission. However, this mechanism was only intended for multicast routing protocols. There is a need to extend this study by developing a solution for proactive protocols through the change of implementation techniques.

Jhaveri [22] proposed a modified RAODV (MR-AODV) protocol, an enhancement of R-AODV protocol. This protocol was subjected to varying network size, mobility, traffic load and malicious attacks through a simulation process. Simulation results showed that MR-AODV isolates black hole nodes during route discovery phase just as R-AODV and sets up a secure route for data transmission. The study shows that MR-AODV protocol is superior to RAODV protocol used as benchmark hence a better solution for MANETs against black hole attacks. However, MR-AODV protocol need further enhancement to improve network efficiency in terms of packet delivery ratio as the number of malicious nodes increases. Further, the MR-AODV protocol needs to be enhanced in order to mitigate cooperative black hole attacks.

Gupta and Woungang [23] proposed a trust-based security protocol (TSP) against PRoPHET (PBH scheme) routing protocol for opportunistic networks (Oppnets). The aim of the study was to compare the effectiveness of the two protocols. Simulation results showed that the PBH scheme leads to higher wastage of network resources while the TSP contributes in reduction of network bandwidth usage by avoiding the additional message replicas that would have been transmitted to the black hole nodes. These findings indicate that TSP is a better routing protocol to curb black hole attacks than PBH scheme. However, TSP needs to be enhanced in order to provide the following functions: calculation of the SGV values in case of randomized behavior of malicious nodes, calculation of credits for evaluation of the trust values of nodes and capturing node's relative delivery probability for higher trusted. TSP needs to be enhanced to be able to detect and prevent cooperative black hole attacks.

In [24], Arya et al. recommended a trusted AODV routing algorithm for detecting and avoiding collaborative black hole attacks in MANET. Simulation experiment indicated that in the presence of collaborative black hole attack AODV protocol used more energy than trusted AODV algorithm. Further, it was noted that throughput and packet delivery ration of trusted AODV algorithm was better compared to AODV protocol. This was an indication that trusted AODV routing algorithm is a superior compared to AODV protocol and can do better in protecting MANETs against collaborative black hole attacks.

6. Results

Reviewed literature indicates that routing protocols can be classified into three: reactive routing protocols, proactive routing protocols and hybrid protocols [4]. Reactive routing protocols discover routes on demand and do route maintenance when a route fails due to link

breakage. In proactive protocol, each node maintains a routing table and contains the information about the network topology. When network changes occur, routing tables are updated periodically. Hybrid protocols are a combination of the features of both reactive and proactive protocols.

Dynamic Destination Sequenced Distance Vector (DSDV) is proactive routing protocol that is created with the help of Bellmen Ford algorithm. DSDV protocol adds sequence numbers to the routing table maintained at each node [27]. These tables hold a list of all the destinations nodes and number of hops made by each node. The routing tables are update instantly once alterations occur in the MANET.

AODV is an enhancement of DSDV protocol; however it is a reactive protocol rather than proactive protocol. AODV works on distance vector routing algorithm to discover the shortest route to the destination node. This protocol uses destination sequence numbers to certify the route freshness, and the operation is performed loop free.

DSR protocol is a reactive routing protocol and works like standard AODV routing protocol. It establishes routes on demand basis and does not maintain routing tables; it is based on source routing. This protocol provides two mechanisms: route discovery and route maintenance which work with each other to provide discovery and maintenance of routes in the network. Further, MR-AODV and Enhanced Modified AODV protocols which are both enhancements of standard AODV protocol are reactive routing protocols.

Trust-based Security Protocol (TSP) uses a trust value to determine nodes participation in the message passing process. The destination node calculates the trust value for each hop in the message vector which is finally distributed to nodes that have participated in the delivery process. Trust values for every node are recorded in the trust table. Using trust values, malicious nodes can be quickly identified since trust values will never increase due to the fact that these nodes do not participate in the routing operation [24].

Reviewed literature indicates that several security techniques exist against black hole attacks in MANETs. A mechanism that integrated Modified EDRI Table and NACK algorithm was implemented to overcome cooperative black hole attacks. The mechanism was implemented in three steps and succeeded in detecting cooperative and nonconsecutive black hole attacks but with some level of routing overhead and end to end delays [17]. The MEDRI table was used to record and maintain history of all the previous malicious nodes. This information was used as future reference for secure transmission and route discovery respectively.

Cooperative Cluster Agent (CCA) was used to identify cooperative black hole nodes in MANETs. This mechanism comprises of four steps: attack procedure, analysis, detection mechanism and prevention mechanism. CCA mechanism works with modified AODV protocol and makes use of the data routing information table, cached table and current routing table. To test the effectiveness of CCA mechanism, simulation was done on NS 2.35 installed on Ubuntu 10.04 platform. A number of tests were executed in order to evaluate the performance of CCA mechanism in the presence of cooperative black hole attacks [18, pp. 309]. It was noted that the proposed mechanism detected malicious nodes and effectively mitigated single and cooperative black hole attack compared to the standard AODV protocol.

CBDS scheme based on DSR mechanism uses proactive and reactive defense architecture to detect the malicious nodes that launch collaborative black hole or gray hole attacks. The scheme comprises of three steps: bait, reverse tracing and reactive defense [19, pp.488]. In the bait step, address of the neighbouring node is used as bait ‘RREQ’ packet in order to lure a malicious node to send fake ‘RREP’ packets. The reverse tracing step is used to find the exact position of the malicious nodes.

Finally, the reactive defense strategy is used to identify and blacklist all the malicious nodes in the available routes. This scheme was implemented using network simulator 2.35 installed in Ubuntu 12.04 LTS 64bit. Simulation results showed that CBDS using AODV

performed better than CBDS using DSR and standard DSR protocol respectively in terms of throughput and packet delivery ratio.

Modified Cooperative Bait Detection Scheme is an enhancement of CBDS scheme. This scheme was implemented using network simulator 2.3.5 and a number of simulation parameters were considered [19, pp.5]. Simulation results showed that modified CBDS performed better than DSR, 2ACK used as benchmark scheme in terms of throughput, routing overhead and end to end delay.

7. Benefits of MANETs

Advancement of cellular technology has introduced small, portable and powerful mobile devices which has led to emergence of MANETs[16]. The mobile devices in this context refered to as nodes have been highly embraced globally and especially in African markets. Application of MANETs have attracted a lot of attention especially by industrial players due to their uniqueness[19]. These networks neither requires pre-established infrastructure nor a power grid. MANETs have been used in areas where wired networks cannot be deployed because of dynamics involved and uniqueness of the area[18],[20].

Mobile Ad hoc Networks have been applied in different domains in our daily life. In African context, their application ranges from emergency situations (such as rescue mission in terror attacks), military operations especially in war torn countries, expeditions (such as mountain climbing), vehicular communication (especially by security companies and tour and travel companies), airport communications among other areas[20].

8. Conclusions

MANETs are emerging technologies especially in developing countries in Africa. Their flexibility and ease of deployement have attracted a lot of attention in industrial application. MANETs application areas in Africa ranges from emergency situations (such as rescue mission), military operations, expenditions (such as mountain climbing), vehicular communication), among other areas. However, MANETs are prone to security threats due to their unique characteristics.

Security is a key feature in any communication system. Guaranteeing security in MANETs is today's biggest challenge. In this paper, we focused on a review of security techniques and routing protocols against black hole and cooperative black hole attacks in MANETs. From the reviewed literature, it is evident that there is a range of routing protocols and techniques developed and simulated using NS2 simulator by various researchers in order to secure MANETs from single and cooperative black hole attacks.

Further, literature show that so far, cooperative black hole attacks are still a major problem in MANETs and research work is still ongoing in an attempt to find a lasting solution to this problem. Security techniques provided against cooperative black hole attacks have suffered efficiency challenges in their design and development which is attributed to network parametric issues such as packet delivery ratio, routing overhead, end to end delay and throughput.

As future work, we intend to develop a resilient security technique based on CBDS in order to detect and avoid cooperative black hole attacks with higher efficiency, improved packet delivery ratio, reduced end to end delays and minimal routing overheads.

References

[1] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Solution for Gray hole Attack in AODV Based MANETs", In Proc. of Third International Conference on Advances in Communication, Network and Computing: Springer, February 2012. pp. 60-67.

[2] A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. B¨ol¨oni, and D. Turgut, "Routing protocols in ad hoc networks: a survey of Computer Networks", 2011, Vol. 55(13) pp. 3032–3080.

[3] Jeenat Sultana and Tasnuva Ahmed, “Securing AOMDV Protocol in Mobile Ad hoc Network with Elliptic Curve Cryptography”, International Conference on Electrical, Computer and Communication Engineering (ECCE), @2017, IEEE, pp.539-543.
[4] Sagar R Deshmukh, P N Chatur and Nikhil B Bhople, “AODV-Based Secure Routing Against Black hole Attack in MANET”, IEEE International Conference on Recent Trends in Electronics Information Communication Technology, @2016, IEEE, pp.1960-1964.
[5] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang, “Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges”, IEEE Communications Surveys & Tutorials, 2011.
[6] Abdelshafy M. A. and King P. J. B., “Resisting Black hole Attacks on MANETs”, 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), @IEEE 2016.
[7] Sukanesh R., Edsor E. and Aarthylakshmi. M., “Energy Efficient Malicious Node Detection Scheme in Wireless Networks”, @2016 IEEE, pp. 307-312.
[8] Sen J., Koilakonda S. and Ukil A, “A mechanism for detection of Co-operative Black hole attack in Mobile ad hoc networks”, Second International Conference on Intelligent Systems, Modeling and Simulation, IEEE, 2011.
[9] Mistry N., Jinwala D. C. and Zaveri M., “Improving AODV Protocol against Black hole Attacks”’, International Multiconference of Engineers and Computer Scientists 2010, vol. 2.
[10] Su M-Y., Chiang K-L. & Liao W-C (2010). Mitigation of Black-Hole Nodes in Mobile Ad hoc Networks. International Symposium on Parallel and Distributed Processing with Applications, IEEE, 2010.
[11] Gupta S., Kar S. and Dharmaraja S., “BAAP: Black hole Attack Avoidance Protocol for Wireless Network”, International Conference on Computer & Communication Technology (ICCCT), IEEE, 2011.
[12] Saha H. N., Bhattacharyya D., Bandhyopadhyay A.K. and Banerjee P. K., “Two-level Secure Re-routing (TSR) in Mobile Ad Hoc Networks”, © 2012 IEEE, DOI 10.1109/MNCApps.2012.31, pp. 119-122.
[13] Bhosle A. A., Thosar T. P. and Mehatre S., “Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”, International Journal of Computer Science, Engineering and Applications (IJCSEA), 2012, Vol.2 (1)
[14] Thachil F. and Shet K.C., “A trust based approach for AODV protocol to mitigate Black hole attack in MANET”, International Conference on Computing Sciences, IEEE, 2012.
[15] Bindra G. S., Kapoor A., Narang A. and Agrawal A., “Detection and Removal of Co-operative Black hole and Gray hole Attacks in MANETs”, ©2012 IEEE, pp. 207-212.
[16] Ukey A. S. A., Chawla M. and Singh V. P., “I-2ACK: Preventing Routing Misbehavior in Mobile Ad hoc Networks”, International Journal of Computer Applications (0975 – 8887), 2013, Vol. 62(12).
[17] Hiremani V. A. and Jadhao M. M., “Eliminating Co-operative Black hole and Gray hole Attacks Using Modified EDRI Table in MANET”, ©2013 IEEE, (2013). pp. 944-948.
[18] Gaikwad V. and Ragha L., “Security Agents for Detecting and Avoiding Cooperative Black hole Attacks in MANET”, International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), © 2015 IEEE, pp.306-311.
[19] Dumne P. R. and Manjaramkar A., “Cooperative Bait Detection Scheme to prevent Collaborative Black hole or Gray hole Attacks by Malicious Nodes in MANETs”,5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), ©2016 IEEE, pp. 486-490.
[20] Emimajuliet. P and Thirilogasundari.V, “Defending Collaborative Attacks in MANETs Using Modified Cooperative Bait Detection Scheme”, International Conference On Information Communication And Embedded System (ICICES 2016), ISSN: 978-1-5090-2552-7, 2016.
[21] Sreenath N., Amuthan A., and Selvigirija P., “Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs”, International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, © 2012 IEEE.
[22] Jhaveri R. H., “MR-AODV: A Solution to Mitigate Black hole and Gray hole Attacks in AODV Based MANETs”, 3rd International Conference on Advanced Computing & Communication Technologies. © 2013 IEEE, DOI 10.1109/ACCT.2013.6, pp. 254-260.
[23] Gupta S. and Woungang I.,”Trust-Based Security Protocol against Black hole Attacks in Opportunistic Networks”, 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), ©2013 IEEE, pp. 724-729.
[24] Arya N., singh U. and singh S, “Detecting and Avoiding of Worm Hole Attack and Collaborative Black hole attack on MANET using Trusted AODV Routing Algorithm”, IEEE International Conference on Computer, Communication and Control (IC4-2015), 2015, pp. 205-210.