International Journal of Advanced Science and Technology
Vol.110 (2018), pp.1-12
http://dx.doi.org/10.14257/ijast.2018.110.01

Critical Review of Techniques for Detection and Mitigation of Co-operative Blackhole Attack in MANET

Nitin Khanna[1,*] and Monika Sachdeva[2]

[1]*Department of Computer Science, Lyallpur Khalsa College, Jalandhar, India*
[2]*Department of Computer Science & Engineering, IKGPTU, Kapurthala India*
[1]*nitinkhanna300@gmail.com*, [2]*monasach1975@gmail.com*

Abstract

Mobile Ad-hoc NETwork can be stated as a self configuring network that is infrastructure-less and communication happens in multi-hop manner. This dynamic nature of MANET and lack of infrastructure makes it vulnerable to many types of attacks; both routing and security. Out of all these attacks a variation of packet drop attack known as co-operative Blackhole attack proves to be a bottleneck in MANET. In this paper, we have reviewed many existing solutions that are useful in mitigation and detection of co-operative Blackhole attack. Co-operative Blackhole involves two or more malicious nodes working together to perform packet drop. We have provided a detail on these mechanisms involving the methodology and algorithms followed in the mechanisms, simulation and their conclusive result in brief and their critical review for drawbacks and advantages. A comparison is drawn and finally, the areas are identified in the field of mitigation of co-operative Blackhole attack on which the future research should be focussed.

Keywords*: Mobile Ad-hoc Networks, Co-operative Blackhole Attack, Blackhole Attack, Dynamic Source Routing, Routing Overheads*

1. Introduction

Mobile Ad-hoc Network is a self configuring network [1] which is composed of many mobile nodes that communicates with each other to for communication purpose. These movable nodes communicate with each other in multi-hop [2] fashion without any kind of infrastructure. All the communication is done via wireless links that are formed using any of routing protocol that all the mobile devices have implemented. MANET found its application in military operations, personal area network (PAN) [3], disaster management and many other applications where a fixed infrastructure is not possible to be established. The feature of infrastructure-less framework, multi-hop communication and dynamic nature gives an additional benefit of deployment of this network in cases where normal network cannot be established. The route establishment is done in MANET either reactively, pro-actively or through combination of both types. In pro-active route establishment routes between all the nodes are maintained all the time whether these are needed or not. DSDV [4] is the prime example of pro-active routing protocol. On the other hand, for re-active path establishment, re-active route discovery protocols such as AODV [5], DSR [6], OLSR [7], *etc* are used in which routes are established only when these are required for data transfer. While in the combination of these two types are known as hybrid are proposed such as Zone routing protocol (ZRP) [8] in which for local communication routes are maintained pro-actively and for distant communication routes are established in re-active manner. Each of these types of routing protocol comes with their advantages and disadvantages and is used depending upon the requirements that are desired from the network and needed to be fulfilled.

Received (December 25, 2017), Review Result (January 10, 2018), Accepted (January 11, 2018)

ISSN: 2005-4238 IJAST

However, all the routing methods in MANET and protocol implementations in these methods comes with many issues like overloading of messages with broadcast of control messages, dynamic link establishment, low bandwidth, reliability of data packets, security attacks [9] and relatively low battery capabilities. Out of all these issues, security attack is the issue that is severe and widely researched by the researchers for suitable solutions. Both active and passive form of attacks is possible in MANET. Various active forms of attack involve Blackhole attack [10], co-operative Blackhole attack [11], Grayhole attack [12], wormhole attack [13], Sybil attack [14], DOS [15] and D-DOS attack [9], rushing attack [16], *etc*. While passive form of attack involves tapping of data on an insecure link and eavesdropping. All these attacks hinder the performance of MANET. Here, in this paper, we discuss the powerful techniques for mitigation of one of these attacks, *i.e.*, Co-operative Blackhole attack in MANET. In remaining of paper, we firstly describe the framework of the Co-operative Blackhole attack and its various consequences. After that, we provide in tabular form the methods for elimination of co-operative Blackhole attack in MANET. A brief review of each technique is then provided and after which we provide conclusion of this review paper and future scope.

2. Co-operative Blackhole Attack

Co-operative Blackhole attack is a devastating variation of Blackhole attack in which two or more malicious nodes collude or co-operate together to perform the packet drop action. We elaborate the co-operative Blackhole attack by illustrating through a scenario involving two co-operative malicious Blackhole nodes. In co-operative Blackhole attack one of the two co-operative nodes acts as forwarding node that forwards the packet to its co-operating node and appear as a legitimate node to the previous hop that might be using detection mechanism for standard Blackhole attack. The other node involved in the co-operation performs the packet dropping action without getting caught by any other legit node in the network that only uses the detection mechanism for standard Blackhole or grayhole attack. So, there is need of advanced mechanism for detection and isolation of group of co-operative Blackhole nodes. If there are more than two nodes involved in the co-operation, then one of the nodes that receive the packet first will forward to one of the other node involved in co-operation and that node on receiving the packet from its partner will not forward it any further. The role of forwarding node and sinkhole is not static and can be interchanged depending upon the fact that which node receives the packet first.

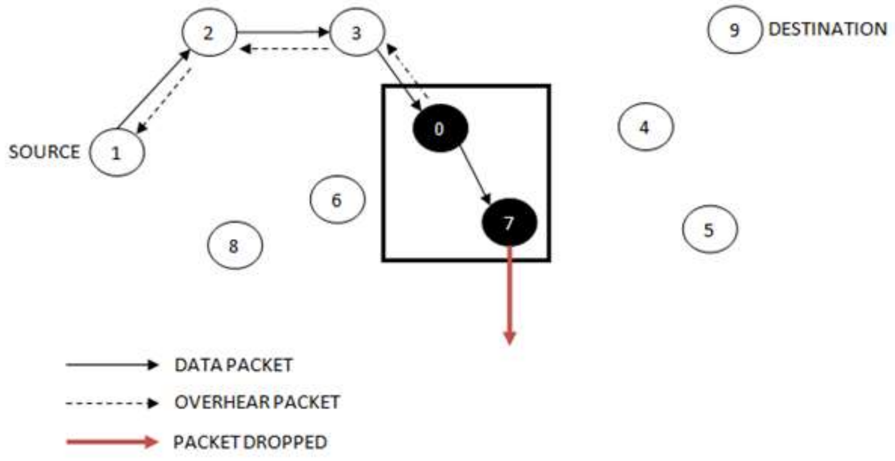

Figure 1. Illustration of Co-operative Blackhole Attack

In the above figure, node 0 and 7 are acting as Collaborative Blackhole nodes, in which at this point, node 0 is acting as forwarding node while node 7 is acting as sinkhole for dropping the data packet. Firstly, on receiving RREQ packet from node 3 for destination node 9, the node 0 involved in co-operative attack sends a fake RREP packet with high destination sequence number creating an illusion that it has the freshest route to the destination. After node 1 which is the source node sends the data packet through the path involving these Blackhole nodes, the node 0 on receiving the data packet forwards it to the node 7 and node 7 drops the packet. However, in these proceedings, node 0 presents itself as legitimate node that is forwarding the packet to next hop and thus prevents its detection by overhearing of previous hop.

3. Counter-measures for Co-operative Blackhole Attack

There are many mechanisms developed by researchers to counter the effects of co-operative Blackhole attacks in MANET and we have comprehensively reviewed 48 research papers published in the past decade in reputed and esteemed journals. Out of these, we have briefly reviewed research mechanisms of 9 research papers that provide a comprehensive overview of research in the past decade. The mitigation of co-operative Blackhole attack can be done either re-actively or proactively. In reactive manner, the detection procedure is initiated after a certain event or when the packet delivery ratio drops to a certain level. While on the other hand, in proactive mechanism initiates the detection procedure before much damage is done in the network communication. Some of the important counter-measures for mitigation of co-operative Blackhole attack are listed in the following table along with their simulator, result, type and drawbacks:-

Table 1. Comparison of Blackhole Mitigation Mechanisms

Scheme	Simulator	Type	Approach/Metric	Result	Drawbacks
EMLTrust [17]	N/A	Pro-active	Machine learning	89% detection rate	Obsolete Modelling, overheads and involvement of third party
Modified AODV [19]	N/A	Pro-active	Enhancement of routing protocol	92-99 % PDR	False positive, longer path formation
Threshold Based Intrusion Detection [20]	GloMoSim, Testbed	Re-active	Entry based Approach	Detection rate is 91%	No dissemination of detection, security overheads
Anomaly Based IDS using Windowing [22]	NS-2	Re-active	Cross layer collaborations	93% accuracy in detection rate	No dissemination of detection, computation overheads
Co-Operative Mechanism [23]	NS-2	Pro-active	Fake route discovery	92% accuracy in detection rate	Applicable only to DSR base routing protocol
D-CBH [24]	N/A	Pro-active	Fake route discovery	12% lesser Routing Overheads	No dissemination of detection, cannot detect Grayhole attack

TRACEROUTE [29]	MATLAB	Re-active	Reverse tracing and timeouts	92 % accuracy in detection	Cryptographic overheads, relatively lower PDR
EDRI [31]	OPNET	Re-active	Routing table based Approach	97% accuracy in detection rate	True negatives
LSAM [32]	NS-2	Re-active	Sequence Number based Approach	PDR rises to 96-99%	Routing overheads, true negatives
NACK [33]	NS-2	Pro-active	2-hop acknowledgement and reverse tracing	Maintains PDR of greater than 80%	Not effective in case of 3 or more co-operative nodes, acknowledgement overhead
CBDS [35]	Qualnet	Re-active	Fake route discovery and co-operation among nodes	PDR lies in the range of 94-95%	Overheads, non-dissemination of detection

3.1. EMLTrust

EMLTrust is a machine learning based reputation system that safeguards against various routing attack. Firstly, machine learning is devised that is based on a given time series of variables through which the future prediction is made based on current behaviour. Models are made offline to guard against malicious behaviour which is then uploaded into the network nodes to facilitate them to predict the nature of other nodes in the network. Using these models, fair nodes identify malicious behaviour and isolate them. At regular interval of time, each node in network share information and feedback about other nodes in the network. To stop malicious nodes from forging the wrong feedback about a fair node, transaction ID between those two nodes need to be crosschecked that cannot be forged and can be easily verified by a third party trusted server. In this way, a reputation system is developed and updated at regular interval of time for mitigation of malicious behaviour even in the form of co-operation among illegitimate nodes. EMLTrust mechanism is compared with naive and TVM Trustguard [18] against parameters like false positive rate, true negative rate and bandwidth overhead. This mechanism provide high degree of accuracy due valid exchange of feedback in presence of third party and quick effect in mitigation of malicious attacks as the attack models are uploaded offline. However, the offline modelling can become obsolete and requires periodic maintenance that requires the entire network to be stopped and restarted again after fresh uploading. Also due to the introduction of third party server increases the overhead and may create a situation of compromise.

3.2. Modified AODV

Modified AODV mechanism is made by adding new packets to the route discovery procedure of standard AODV routing protocol. In this mechanism, during the route discovery phase, whenever any node needs to find path to a particular destination node, it will initiate the procedure of route discovery by broadcasting the RREQ packet to its entire neighbour. Whenever any intermediate node has a fresh path to the desired destination, then it will reply with a RTRPLY packet and VERIFY packet to destination.

On receiving RTRPLY packet, source verifies the authenticity and reliability of path by sending a CHECKVRF packet to the destination through the path suggested by RTRPLY packet. On receiving CHECKVRF packet, destination checks whether it receives VERIFY packet for the same. If it does, it will send FINALREPLY packet to the source. On receiving that packet source ensures that path formed is authentic and will do future communication with destination through this path. If the FINALREPLY packet is not received by source within specified time limit, the generator of RTRRPLY packet is marked malicious. This method is compared with standard AODV and DSDV routing protocol on the basis of PDR, throughput, End-to-End delay and routing overhead. This method provides reliability of path and use of AODV routing protocol as base will lower the network overhead. However, this mechanism prolongs the path formation process and the accuracy may diminish in case of false positive due to intrinsic nature of MANET.

3.3. Threshold Based Intrusion Detection System

In this mechanism, the intrusion of all types of Blackhole attacking nodes is detected by having a look on the behaviour of other nodes in the network and when any deviation from normal behaviour is detected, that node is marked and isolated. Each node in the network acts promiscuously and keeps an eye on the forwarding pattern of all its neighbouring nodes. secAODV is used as base routing protocol and all the packets of secAODV are monitored for forwarding. Using secAODV provides security features like digital signature and confidentiality that detects any kind of modification in data instantly. The datagram packets are assumed for data transmission. Each node after sending datagram makes an entry dgram_in for the next hop and if the next hop does not forwards the same datagram or modifies the datagram the no dgram_out will match with the entry for dgram_in and the node will note that next hop has not forwarded the packet and is not fair. If such behaviour reaches a certain pre-defined threshold then the node will mark its next hop on a particular destination as Blackhole. This mechanism is validated for true positive, false negative, throughput and response time against standard AODV and secAODV in simulator GloMoSim. This mechanism will take full advantage of promiscuous mode that has higher degree of accuracy in Blackhole detection. Also with a well established threshold the chances of false positive is minimized. However, larger overhead is caused due to added security patterns using secAODV. Also, there is no facility of isolating the malicious attacking node from the network and dissemination of information to other fair nodes.

3.4. Anomaly Based IDS using Windowing

This mechanism is a cross-layer collaboration anomaly based detection mechanism in which routing and data link layer both collaborates for parameter estimation that is further utilized to detection of any intrusion. Firstly, Data_FWD and DAT_RECV parameters are obtained from network layer and CTS_RECV and RTS_SND are collected from data link layer. On the basis of these parameters probabilities of collision, probability of forwarding of data and probability of mobility of a node is calculated by every node in the network for every other node in the network. Using these probabilities, the probability of a node to drop a certain data packet sent by a node is calculated. A certain threshold is defined and if probability of dropping of data packet reaches that threshold the attacking node is identified and marked. This estimation is done in event based windows that are interval during which the behaviour of nodes are judged and any anomaly is identified using threshold value. This mechanism is implemented and tested in NS-2 simulator and performance is measured on the basis of parameters like True negative rate, false positive rate at different mobility speed and density of nodes. The cross-layer feature provides much reliable information as the exchange of information happened between two layers of the same node and thus it will be highly reliable. Event based windowing removes the limitation of time based windowing in which time interval is chosen arbitrarily. However, it is difficult to model the events for windowing and also it will cause high computation load for calculation of large amount of probabilities and parameters. There is also no facility of dissemination of co-operative Blackhole detection among fair nodes in the network.

3.5. Co-Operative Mechanism

This mechanism involves the basic nature of DSR routing protocol for detection of sinkholes, like Blackhole and co-operative Blackhole. It uses three types of packet, *i.e.*, SAP SDP and SNP for identification of existence of attack, detection of attack and notification to other nodes in the network respectively. Firstly, a bogus RREQ is generated by any node that wants to pro-actively detection of sinkhole in the network with a defined destination. When the originator of the RREQ receives the bogus RREQ with greater sequence number it gets an indication of existence of sinkhole on the path and as the entire set of nodes in the path is stored in the RREQ and RREP packets it is easy to analyze each and every node. After getting a sinkhole indicator the source node sends a SAP packet for detection of malicious node. With the help of SAP, the common part of the bogus sinkhole path is identified and which is later on used when SDP packet is sent. When any node in the network receives SDP packet not generated by sinkhole will compare the sequence number of bogus RREQ and SDP packet and if the sequence numbers match, the node will eventually discover that the last node in the bogus RREQ packet is the sinkhole and will mark that node. After that finally SNP packet is disseminated in the entire network to isolate the sinkhole. This mechanism is highly accurate and its pro-active nature will increase the data packet delivery ratio. However, use of DSR as base routing protocol increases the load of control packets.

3.6. D-CBH

D-CBH mechanism is used for detection of collaborative Blackhole attack which uses D-MBH (detection of Multiple BlackkHole), an algorithm that detects single Blackhole. Firstly, a node invokes D-MBH algorithm which involves broadcasting of fake RREQ with a destination that does not exists. All the RREP packets in response to this fake RREQ must be coming from Blackholes and thus will be marked as Blackholes and included in the BH list. From the RREP from Blackholes average destination sequence number is calculated and the list and average of sequence number is passed to newly invoked D-CBH. In this, every RREP packet coming from node in BH list is in BH list will be discarded. If the RREP packet is coming from a node whose next hop is in BH list then it is detected that those two nodes are working in co-operation and hence source of that RREP is included in CBH (Co-operative Blackhole) list. This work is compared with fidelity [25], trust based approach [26][27] and DRI [28] on the basis of routing and computational overheads. This scheme provides a very little amount of computation and routing overhead for detection of attacks. However, this method is not suitable for Grayhole attack detection. Also, there is no co-operation among nodes about dissemination of information about detection of malicious nodes.

3.7. TRACEROUTE

TRACEROUTE mechanism provides detection of co-operative Blackhole by using two special types of packet called TRACE and REVERSETRACE. Each node for every data packet it sends, maintains an ACK counter which gets incremented when it sends a data packet to a particular destination and gets decremented when it receives ACK from the destination about sound reaching of data to the destination. If there are any co-operation among any malicious nodes that cannot be identified by single node attack mechanism, the ACK counter will indeed reach a threshold value as the data packet would not reach the destination. This event will trigger the TRACEROUTE mechanism. Implementing this, the source node sends a TRACE packet to the next hop towards that destination and set a timer. It must receive a REVERSETRACE for that packet before expiry of that timer. The next hop forwards the TRACE packet and set the timer and so on. When for any intermediate node, the timer expires; the node marks the next hop as co-operative Blackhole and notifies the source through preceding nodes. Whenever that marked node send a fake RREP in the response of any RREQ, its next hop is also get marked and in this way co-operative Blackhole gets mitigated. The REVERSETRACE cannot be forged as it will come with signature of destination if no node is marked. TRACEROUTE is simulated in NS-2 simulator and compared against W-AODV [30] for paremters like PDR, control load, accuracy and packet drop ratio. This mechanism is very accurate in detection and eliminates many nodes involved in co-operation. However, a large amount of packet gets dropped before TRACEROUTE gets triggered. Also, there is large overhead involved due to acknowledgements and cryptography.

3.8. EDRI

In this mechanism a special routing packet is used along with extended Data Routing Information for detection of co-operative Blackhole attack. Standard DRI table is extended firstly to include Blackhole Node column which is marked 1 along with node ID of the detected node. The new control packet contains three fields, viz, node ID, next hop and random number for security and validation purposes. In the route discovery phase, along with RREP packet the special packet with node ID next hop and random number is sent back to the source of RREQ packet. When Blackhole receives RREQ for a particular destination, it sends special packet with RREP with higher destination sequence number. On receiving the RREP the source sends the special packet to the next hop in that path with a random number. The next hop further sends that packet with a new random number and so on. On receiving that special packet, destination replies to that packet. On receiving the reply each intermediate node checks for the matching random number as the reply special packet and special packet must have same random number for fairness of the next hop. If it differs, then the next hop is marked as malicious and the Blackhole column for that node in EDRI table is set to 1. If not, then both to and from entry is set to 1 for that node. At last the information about the detection of co-operative Blackhole is broadcasted in the network and all the nodes updates their EDRI table entries accordingly. This mechanism is simulated in OPNET simulator and compared against base work [28] for detection of CBH for parameters like packet overhead, delay, throughput, false positive and number of malicious node detection. This mechanism provides detection with least degree of false positive. Also with the application of this mechanism more reliable paths are formed. However, it may have the problem of true negatives where lose of packet or accidental modification may cause a fair node to be treated as malicious.

3.9. LSAM

LSAM is a localized Secure Architecture for MANET that detects both single and co-operative Blackhole attacks in MANET. It involves a special Security Monitoring Node. Firstly, the route between any pair of source and destination is formed, the source sends the data packet to the destination node and in return the destination node send ACK packet back to the source node about reception of data packet in a specified time interval. The shortest path is formed between two nodes according to the weight of the link. All the intermediate hops are continuously monitored for certain time interval for forwarding behaviour and if the packet drop exceeds certain pre-defined threshold value by any intermediate hop, then the sequence number for that node is extracted. If the sequence number comes out to be abnormal then security monitoring node initiates the detection of any Blackhole or co-operative Blackhole attacking node. All the neighbouring nodes maintain node ID and sequence number. Comparison of sequence number for the node in question is done by all the nodes in the same transmission range. If the comparison is found to be abnormal the node in question is marked as malicious. After marking, the security monitoring node sends an ALARM message to notify other security monitoring nodes in the network for notification of identification of co-operative Blackhole nodes. This mechanism is compared in the simulator NS-2 against AODV for parameters like packet delivery ratio, routing overhead, delay, throughput, packet drop ratio and control overhead. The packet delivery ratio is greatly enhanced using this mechanism. Also, the dissemination of malicious node is done instantaneously to alert other fair nodes in the network and using only the special monitoring nodes for this purpose reduces the routing overhead. However, it generates a lot many routing overhead for detection of attack. The rate of true negatives is also a problem in this mechanism.

3.10. NACK

NACK uses a novel ACKnowledgment packet to verify the two-hop node receives the packet from the next hop. When it does receive the packet soundly, it sends NACK to the two hop back node. Each node i maintains a list and time interval before which it must receives NACK from the two-hop node. When a node, i receives the NACK it verifies through the MAC address and LIST. If everything is fine and there is an entry, it will consider the next hop to be fair; otherwise the next hop is marked as malicious. The assumption of use of DSR routing protocol and existence of two routes to the same destination plays a vital role. If there is an attacker in one path, using basics of DSR and NACK co-operation is identified. If the node i verifies hat node i+1 receives the NACK, it will mark both next hop and two-hop node as co-operative Blackhole as they send fake reception of NACK. The timestamp of NACK packet also stored in the list and is utilized for detecting the presence of some malicious co-operation. This work is simulated using NS-2 and compared with 2ACK and DSR [6] for parameters like PDR, false positives and routing overheads. The high rate of packet delivery and low false positives and true negatives makes this concept a vital one. The use of timestamp, lists and acknowledgements leads to high degree of accuracy. However, the routing overhead due to excessive acknowledgements hampers the throughput of the network. Also, this mechanism is useful only in detection and elimination of co-operative Blackhole attacks that includes only two nodes but fails to detect if there is co-operation of more than two Blackhole nodes.

3.11. CBDS

Co-operative Blackhole Detection Scheme detects both grayhole and co-operative Blackhole through a reverse tracing technique. In this, firstly a node that wants to detect the presence of co-operative Blackhole stochastically selects a neighbouring node as bait (fake) destination and triggers a route discovery procedure for that bait destination. This scheme only works in conjunction with DSR routing protocol. When a malicious node sends a fake RREP in response to the bait RREQ packet it starts the detection process by making an address list. Address list includes all the intermediate hops that are involved in that RREP packet. From that list a new list is obtained that includes address and Ids of all the intermediate nodes from source of bait RREQ to the node that generates RREP packet. By refining this list, we obtain two sets; one a set of trusted nodes and the other set that includes nodes for which the decision is yet to be taken. The latter set is then consider as original list and further refinement to that list for trusted nodes is performed through co-operation from other fair nodes. At last there will be only one or set of malicious nodes that are performing co-operative Blackhole attack. This work is tested in Qualnet simulator and compared with 2ACK [34], DSR [6] and BFTR [36] for parameters like packet delivery ratio, routing overhead,end-to-end delay and throughput. Using this mechanism will lead to accurate and fast detection of all types of Blackhole attack either Grayhole, single or co-operative. Also, the detection process is pro-active and thus will detect attack in its early stage and hence not much damage would be caused. However, this method can only be used under DSR routing environment that will cause more routing overhead as compared to AODV. There is no economical procedure of notifying other nodes in the network about detection of attacking node.

4. Conclusion and Future Work

MANET due to dynamicity and intrinsic design and implementation creates a loophole through which co-operative Blackhole nodes work together and performs packet dropping action. Many researchers work on mitigation, detection and avoidance of this co-operative attack through their path breaking proposed mechanisms. In this review paper, we have critically evaluated and reviewed the best mechanisms researched and proposed along with their merits and drawbacks. In our reviewing process, we present best published work for mitigation of co-operative Blackhole attack. Some of these works are proactive in nature while others are reactive. In proactive manner, the detection process for co-operation of attacking nodes is started before or along the route establishment. This type of mechanism creates routing overheads. On the other hand, reactive mechanisms initiate the process of detection only when a certain event happens. But these mechanisms degrade the PDR to some extent. We also observe that there is a trade-off between PDR and routing overheads. Most of the mechanisms discussed here share two common shortcomings that involves dissemination of information after detection of attack and detection of co-operation among more than two malicious nodes.

The area of the research in mitigation of co-operative Blackhole attack is still active and has wider scope. The current and future researchers must aim at devising efficient mechanism that finds a suitable the trade-off between PDR and control overhead and forms a proactive mechanism that detects co-operation among three or more Blackhole nodes. This review paper will help the researchers in identifying some of best works on detection and mitigation of co-operative Blackhole attack and realize the importance of these mechanisms in the current situation. For future research, we propose here in this paper after comprehensive reviewing of literature that the researcher should guide their work in the direction of detecting co-operation proactively without much control overhead and the mechanism should be generic enough to work with any base routing protocol. Also, the work must detect co-operation among any number of nodes with higher accuracy.

References

[1] N. Khanna and P. Sharma. “Mitigating Blackhole and Grayhole Attack in MANET using Enhanced AODV with TLTB Mechanism”, International Journal of Future Generation Communication and Networking, vol. 9, issue 8, **(2016)**, pp. 129-140.

[2] N. Khanna and P. Singh, “Mitigating Blackhole and Security attacks in MANET using Enhanced WAODV with Trueness Level and Cryptography”, IJRECE, vol. 3, issue 2, **(2015)**, pp. 146-151.

[3] Z. Thoams Guthrie, “Personal area networks: near-field intra-body communication”, IBM systems Journal, vol. 35, issue 3, **(1996)**, pp. 609-617.

[4] E. M. Royer and C.-K. Toh, “A review of current routing protocols for ad hoc mobile wireless networks”, IEEE personal communications, vol. 6, issue 2, **(1999)**, pp. 46-55.

[5] C. E. Perkins and E. M. Royer, “Ad hoc On Demand Distance Vector Routing”, **(1999)**.

[6] D. B. Johnson and D. A. Maltz, “Dynamic source routing in ad hoc wireless networks”, Mobile computing, **(1996)**, pp. 153-181.

[7] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR)”, No. RFC 3626, **(2003)**.

[8] H. Zygmunt J., M. R. Pearlman and P. Samar, “The zone routing protocol (ZRP) for ad hoc networks”, **(2002)**.

[9] S. William, “Cryptography and network security: principles and practices”, Pearson Education India, **(2006)**.

[10] M. Peng, “Black hole search in computer networks: State-of-the-art, challenges and future directions”, Journal of Parallel and Distributed Computing, vol. 88, **(2016)**, pp. 1-15.

[11] J. Payyappilly Priya and P. A. Ghosh, “Performance Study of AODV Protocol during Collaborative Blackhole Attack in MANET”, International journal for Universal Science & Technology, vol. 1, issue 2, (2015).

[12] H. Jhaveri Rutvij and N. M. Patel, “A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks”, Wireless Networks, vol. 21, issue 8, **(2015)**, pp. 2781-2798.

[13] M. Imran, “Analysis of detection features for wormhole attacks in MANETs”, Procedia Computer Science, vol. 56, **(2015)**, pp. 384-390.

[14] P. Goyal, S. Batra and A. Singh, “A literature review of security attack in mobile ad-hoc networks”, International Journal of Computer Applications, vol. 9, issue 12, **(2010)**, pp. 11-15.

[15] H. J. Rutvij, S. J. Patel and D. C. Jinwala, “DoS attacks in mobile ad hoc networks: A survey”, Advanced Computing & Communication Technologies (ACCT), Second International Conference on. IEEE, **(2012)**.

[16] R. Nandy and D. Barman Roy, “Study of various attacks in MANET and elaborative discussion of rushing attack on DSR with clustering scheme”, International Journal of Advanced Networking and Applications, vol. 3 issue 1, **(2011)**, pp. 1035-1042.

[17] R. Akbani, T. Korkmaz b and G.V. Raju, “EMLTrust: An enhanced Machine Learning based Reputation System for MANETs”, Ad Hoc Networks, Elsevier, Vol. 10, Issue 3, **(2012)**, pp. 435-457.

[18] M. Srivatsa, L. Xiong and L. Liu, “TrustGuard: countering vulnerabilities in reputation management for decentralized overlay networks”, Proceedings of the 14th International Conference on World Wide Web, WWW ’05, ACM, **(2005)**, pp. 422–431.

[19] A.A. Chavan, D. S. Kurul andd P. U. Dere, “Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack”, 7th International Conference on Communication, Computing and Virtualization, Procedia Computer Science, Elsevier, vol. 79, **(2016)**, pp. 835-844.

[20] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha, “Threshold-based intrusion detection in ad hoc networks and secure AODV”, Ad Hoc Networks, Elsevier, vol. 6, Issue 4, **(2008)**, pp. 578-599.

[21] A. Patwardhan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, “Secure Routing and Intrusion Detection in Ad Hoc Networks”, Proceedings of the 3rd International Conference on Pervasive Computing and Communications, IEEE, **(2005)**, pp.191-199.

[22] L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro and R. Magán-Carrión, “A model of data forwarding in MANETs for lightweight detection of malicious packet dropping”, Computer Networks, Elsevier, vol. 87, **(2015)**, pp. 44-58.

[23] G. Kim, Y. Han and S. Kim, “A cooperative-sinkhole detection method for mobile ad hoc networks”, AEU-International Journal of Electronics and Communications, Elsevier, vol. 64, Issue5, **(2010)**, pp. 390-397.

[24] K. S. Arathy and C. N. Sminesh, “A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET”, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, Procedia Technology, Elsevier, vol. 25, **(2016)**, pp. 264-271.

[25] T. Latha and V. Sankaranarayanan, “Prevention of co-operative black hole attack in MANET”, Journal of networks, Elsevier, vol. 3, Issue 5, **(2008)**, pp. 13-20.

[26] S. Biswas, T. Nag and S. Neogy, “Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET”, Applications and Innovations in Mobile Computing (AIMoC), IEEE, **(2014)**, pp. 157-164.

[27] F. Thachil and K. C. Shet, “A trust based approach for AODV protocol to mitigate black hole attack in MANET”, Computing Sciences (ICCS), 2012 International Conference on. IEEE, **(2012)**, pp. 281-285.

[28] J. Sen, S. Koilakonda and A. Ukil, “A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Adhoc Networks”, IEEE Second International Conference on Intelligent Systems, Modeling and Simulation, **(2011)**, pp. 338-343.

[29] N. Khanna, (2016) “Mitigation of Collaborative Blackhole Attack using TRACEROUTE Mechanism with Enhancement in AODV Routing Protocol”, IJFGCN, SERSC Publishers, vol. 9, Issue 1, **(2016)**, pp. 157-166.

[30] T. Varshney, T. Sharma and P. Sharma. “Implementation of watchdog protocol with AODV in mobile ad hoc network”, Communication Systems and Network Technologies (CSNT), Fourth International Conference on. IEEE, **(2014)**, pp. 217-221.

[31] A. Dorri, “An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET”, Wireless Networks, Springer, vol. 23, Issue 6, **(2017)**, pp. 1767-1778.

[32] T. Poongodi and M. Karthikeyan, “Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks”, Wireless Personal Communication, Springer, Vol. 90, Issue 2, **(2016)**, pp.1039-1050.

[33] H.-M. Sun, C.-H. Chen and Y.-F. Ku, “A novel acknowledgment-based approach against collude attacks in MANET”, Expert Systems with Applications, Elsevier, vol. 39, Issue 9, **(2012)**, pp. 7968-7975.

[34] L. Kejun, J. Deng, P. K. Varshney and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in MANETs”, IEEE transactions on mobile computing, vol. 6, Issue 5, **(2007)**.

[35] J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao and C.-F. Lai, “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach”, IEEE Systems Journal, vol. 9, Issue 1, **(2015)**, pp. 65-75.

[36] Y. Xue and K. Nahrstedt, “Providing fault-tolerant ad hoc routing service in adversarial environments”, Wireless Personal Communications, Springer, vol. 29, Issue 3, **(2004)**, pp. 367– 388.

Authors

Nitin Khanna, he received the M.Tech. Degree in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, in 2015, Currently, Currently, he is pursuing Ph.D. in Computer Science & Engineering from IKGPTU, kapurthala, India and working as Assistant Professor in Computer Science department at Lyallpur Khalsa College, India. His area of research is in the field of ad -hoc networks and security mechanisms.

Monika Sachdeva, she has done BTech computer science and engineering from National Institute of Technology NIT, Jalandhar in 1997. She finished her MS software systems from BITS Pilani in 2002. She completed her PhD in Department of Computer Science and Engineering from Guru Nanak Dev University, India. Currently she is working as head, Department of Computer Science & Engineering, IKGPTU, India. Her areas of interest include security measures in ad-hoc and sensor networks.